Resilience Week 2014

Transforming the
Resilience of Cognitive,
Cyber-physical Systems

August 19-21, 2014

Welcome

The International Symposium on Resilient Control Systems originated in 2008, and was initiated to address the research challenges associated with cognitive, cyber-physical threats to this "nervous system" of critical infrastructure. In 2013 the Symposium evolved into separate, co-located symposia under the Resilience Week umbrella. Resilience Week is now a collection of symposia on several related topics—Control Systems, Cyber Systems, Cognitive Systems, and Communications Systems—organized around the theme of resilience. However, to achieve critical infrastructure resilience requires an interdisciplinary approach, and a foundational element of Resilience Week is to facilitate the interdisciplinary dialog. Therefore for this year, you will notice that the sessions were developed to integrate diverse contributors under a common technical challenge, and as well, a National Symposium on Resilient Critical Infrastructure (NSRCI) has been added to the program.

As complement to the existing research and development symposia, NSRCI is intended to facilitate productive discussion of tools, technologies, and policies for improving critical infrastructure resilience. A goal of NSRCI is to engage in a discussion of modeling and decision support tools, methodologies to discover and mitigate the impacts of dependent and interdependent relationships among infrastructure systems, and techniques to assist decision-makers in resource allocation and prioritization both pre- and post-event. NSRCI aims to provide an environment in which universities, national labs and other innovators and problem solvers can interface directly and gather requirements from the "user community."

We trust you will find the NSRCI and this year's Resilience Week to be beneficial in creating a thought provoking, synergistic environment that advances the research agenda and solutions for cognitive, cyber-physical resilience. On behalf of the organizing leadership and sponsors, let me express our appreciation for your participation.

Craig Rieger
Steering Committee Chair

Table of Contents

Resilience Week Sponsors

Organizers

- Idaho National Laboratory
- Temple University
- Florida Institute of Technology
- Ohio State University
- University of Denver
- Colorado State University
- Air Force Research Institute

Technical Sponsors

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

Gold Sponsors

- Argonne National Laboratory
- F5

Silver Sponsors

- Juniper Networks
- Gigamon

Tuesday, August 19 - Special Topics Sessions

	Resilience Models and Measures Track Chair: Marco Carvalho, FIT; Craig Rieger, INL *[Crystal Peak B/C]*	**Mixed Human-Automation Resilience Track** Chairs: Frank Ferrese, NAVSEA; Will Nothwang, ANL *[Mt. Elbert A]*	**Resilient Infrastructure Track** Chairs: David Alderson, NPS; Cherrie Black, INL; Sean McAraw, INL *[Mt. Evans]*
7:00 a.m.	**Coffee and Registration** *[Capitol Pre-Function Area, 38th Floor]*		
8:00 a.m.	**Symposium Opening Plenary** *[Capitol Peak]* Bill Bryan, Deputy Assistant Secretary, Infrastructure Security and Energy Restoration DOE		
8:20 a.m.	**Logistics** *[Capitol Peak]*		
	Keynote Speakers		
8:30 a.m.	Bill Sanders, UIUC	Lynne Parker, UTK	Stephen Flynn, NU
9:15 a.m.	Nancy Leveson, MIT	Chris Wickens, CSU	**Morning Break (9:30 a.m.)**
10:00 a.m.	**Morning Break**		***Invited Speakers***

	Invited Speakers		Stakeholder Perspectives
			Facilitator: Cherrie Black, INL;
			David Alderson, NPS;
			John Madden, State of Alaska;
			Sean McAraw, INL;
			Steven Kuhr, Colorado Springs Util

10:30 a.m.	Control-Cyber Research Perspective Craig Rieger, INL Indrajit Ray, CSU	Cyber-Control Research Perspectives David Garlan, CMU; Nathan Michael, CMU	
11:30 a.m.	**Hosted Lunch with Plenary Speaker** *[Capitol Peak]* Rosemary Wenchel, DHS Deputy Assistant Secretary for Cybersecurity Coordination		
	Invited Speakers		***Lightning Talks***
1:00 p.m.	Cyber-Cognitive Research Perspectives Marco Carvalho, FIT; Nick Multari, PNNL; Michael Assante, NBISE	Cognitive-Control Research Perspectives Anthony Seman, ONR; Mike McCourt, UF; Kaleb McDowell, ARL	J. Phillips, ANL, "Critical Infrastructure Dependencies"; I. Martinez-Moyano, ANL, "Community Resilience and the Role Played by Critical Infrastructure"; L. Genik, DRDC, "Systems Analysis of Community Resilience"; J. Phillips, ANL, "Critical Infrastructure and Regional Resilience"; J. Richards, DHS, "Regional Resiliency Assessment Program Successes and Goals"; R. Bowman, NEU, "Focusing the Lessons of Disaster through the Lens of Resilience: A Case for More Case Studies"; D. Alderson, NPS, "Moving Away from Threat-- Based Analysis"

2:30 p.m.	**Afternoon Break** *[Crystal Peak A]*		
	Facilitated Discussions		***Panel Discussion***

3:00 p.m.	Promising Interdisciplinary Methodologies
	Facilitator: Chairs
		Research Challenges
		Facilitators: Chairs
			Challenges and Opportunities
			Moderator: Stephen Flynn, NU;
			David Brannegan, ANL;
			Connie Lau, HEI;
			John Madden, State of Alaska;
			Brandon Wales, DHS

4:30 p.m.	**Welcome Reception, GridGame Competition and Poster Session** *[Crystal Peak A / Pre-function Area]*		
	A. Rege, Temple U., "Adversary Dynamics and Smart Grid Security: A Multiagent System Approach"; D. Bodeau, MITRE, "Resiliency Techniques for Systems-of-Systems: Extending and Applying the Cyber Resiliency Engineering Framework to the Space Domain"; D. Naidu, ISU, "Nonlinear Model Predictive Control for Regulation of a Class of Nonlinear Singularly Perturbed Discrete-time Systems"; N. Gong, Temple U., "Evaluation of Highly Conditionally Diagnosable (n,k)-star Topology for Applications in Resilient Network on Chip"; Q. Ren, Temple U. "A BDI Multi-agent Approach for Power Restoration"; Xie Feng, China ITSEC, "Using Simulation Platform to Analyze Radio Modem Security in SCADA"		
6:30 p.m.	**Adjourn for Day**		

Wednesday, August 20 - Papers

	Cyber Track Chairs: Marco Carvalho, FIT; Annarita Giani, LANL *[Crystal Peak B/C]*	**Control Track** Chairs: Frank Ferrese, NAVSEA; David Scheidt, JHU APL *[Mt. Elbert A]*	**Cognitive-Communications Track** Chairs: Roger Lew, UI; Jie Wu, Temple *[Grays Peak A/B]*	**Resilient Infrastructure Track** Chairs: David Alderson, NPS; Cherrie Black, INL; Sean McAraw, INL *[Mt. Evans]*
7:30 a.m.	**Coffee and Registration** *[Capitol Pre-Function Area, 38th Floor]*			
8:20 a.m.	**Logistics** *[Capitol Peak]*			
	Keynote Speaker *[Capitol Peak]*			***Invited Speakers***
8:30 a.m.	Michael VanPutte, MOD-2			Connie Lau, HEI, "CEO's View of Resilience"; Brandon Wales, DHS, "Analyzing Infrastructure Interdependencies: Lessons Learned"
9:30 a.m.	**Morning Break** *[Crystal Peak A]*			
	Cyber Security Methodologies	***Power and Energy Systems***	***Human System Interaction and Training***	***Lightning Talks***
10:00 a.m.	N. Evans, ANL, "Multiple OS Rotational Environment: An Implemented Moving Target Defense"	*E. Archibong, ISU, "Time Scale Analysis and Synthesis for Model Predictive Control under Stochastic Environments"	R. Lew, INL, "A Prototyping Environment for Research on Human-Machine Interfaces in Process Control: Use of Microsoft WPF for Microworld and Distributed Control System Development"	N. Mehravari, CMU, "Evaluating and Improving Cyber Resilience Capabilities of the Electricity and Oil & Natural Gas"; J. Phillips, ANL, "Mathematical Disruption and Impact Models for Addressing Regional Resilience"; B. Thomas, ORNL, "Modeling Climate Impacts on Critical Infrastructures"; D. Judi, LANL, "Urban Water System Modeling and Simulation Tools to Evaluate Infrastructure Resilience"; N. Mehravari, CMU, "Improving the Resilience of National Postal and Related Transportation Critical Infrastructure"; K. Stamber, SNL, "Event Response Resource Quantification and Prioritization"; P. Roege, INL, "Metrics for Energy Resilience"; D. Alderson, "A Vritual Environment for Resilient Infrastructure Modeling and Design"
10:30 a.m.	C. Miles, UL, "VirusBattle: State-of-the-Art Malware Analysis for Better Cyber Threat Intelligence	B. Niemoczynski, NAVSEA, "Closed Loop Control of Hysteretic Magnetization"	R. Lanier, Design Interactive, "Aptitude Testing for Selection, Specialization, and Training, of Airport Security X-ray Imaging Operators (X-APT)"	
11:00 a.m.	M. Atighetchi, BBN, "A Framework for Resilient Remote Monitoring"	C. Nwankpa, DU, "Performance Indicator Dependency on Measurement Sets in a DC Multi-Converter Power System"	R. Lew, INL, "A Prototype Computerized Operator Support System"	

11:30 a.m.	**Hosted Lunch with Plenary Speaker** *[Capitol Peak]* Kevin Moore, Dean of Engineering and Computational Sciences, CSM			
	Cyber Security and Control Systems *[Mt. Elbert A]*		***Keynote Speaker*** *[Capitol Peak]*	
1:00 p.m.	R. Hink, ORNL, "Machine Learning for Power System Disturbance and Cyber-attack Discrimination"		Jalal Mapar, HSARPA RSD	
1:30 p.m.	C. Patterson, Virginia Tech, "Isolating Trust in an Industrial Control System-on-Chip Architecture"			
2:00 p.m.	W. Abbas, Vanderbilt U., "Resilient Consensus Protocol in the Presence of Trusted Nodes"		***Facilitated Discussion*** *[Capitol Peak]* Workforce Development Facilitator: David Alderson, NPS	
2:30 p.m.	**Afternoon Break** *[Crystal Peak A]*			
	Evaluation and Analysis of Defense Systems	***Perturbed Systems and Nonlinear Control***	***Resilience Measurement***	***Lightning Talks***
3:00 p.m.	*G. Martins, Vanderbilt U., "Performance Evaluation of an Authentication Mechanism in Time-Triggered Networked Control Systems"	D. Naidu, ISU, "Time Scale Analysis and Synthesis for Unmanned Aerial Vehicles(UAVs)"	S. Duff, Design Interactive, "The Diagnosis and Measurement of Team Resilience in Sociotechnical Systems"	D. Christiansen, INL, "Virtual Simulation for Cyber and Physical Integration"; R. Bent, LANL, "Optimal Resilient Distribution Grid Design"; R. Hruska, INL, "Knowledge Framework for Critical Infrastructure Dependency Analysis"; S. Tam, ANL, "Applications of Nonlinear Dynamics to Resiliency Analysis"; C. Unis, SNL, "Understanding Complexities in Emergency Management in Order to Mitigate Cascading Consequences"; D. Egli, JHUAPL, "The Value Proposition of Operationalizing Resilience"; J. DiRenzo III, USCG, "Maritime Strategic Surprise: Can An Emphasis on Resilience Be The True Center of Gravity?"; P. Roege, INL, "Resilience: Modeling for Conditions of Uncertainty and Change"
3:30 p.m.	M. Balchanos, Georgia IT, "Metrics-based Analysis and Evaluation Framework for Engineering Resilient Systems"	J. Kollmer, Temple U., "Hovering Synchronization of a Fleet of Quadcopters"	C. Rieger, INL, Resilient Control Systems Practical Metrics Basis for Defining Mission Impact	
4:00 p.m.	Z. Beech, PNNL, "Quantifying Cyber-Resilience Against Resource-Exhaustion Attacks"	D. Naidu, ISU, "Real-Time Algorithm for Nonlinear Systems With Incomplete State Information Using Finite-Horizon Optimal Control Technique"	P. Ostovari, Temple U, "Priority-Based Broadcasting of Sensitive Data in Error-Prone Wireless Networks"	
4:30 p.m.	**Sponsor Reception** *[Wynkoop Brewing Company, 1634 18th Street]*			
7:00 p.m.	**Adjourn for Day**			

Thursday, August 21 - Special Topics Sessions

	Industrial Control System Cyber Security Track Chairs: Subbaram Naidu, ISU; Sean Peisert, LBNL; Miles McQueen, INL *[Crystal Peak B & C]*	**Resilient Infrastructure Solutions User Group Track** Chairs: David Alderson, NPS; Cherrie Black, INL; Sean McAraw, INL *[Capitol Peak B]*
7:30 a.m.	**Coffee and Registration** *[Capitol Pre-Function Area, 38th Floor]*	
8:20 a.m.	**Logistics** *[Capitol Peak A]*	
	Panel Discussion *[Capitol Peak A]*	
8:30 a.m.	Resilient Infrastructure Needs and Capabilities Facilitator: Ron Fisher, INL; Matt Gibson, EPRI; Fred Hintermister, NERC; Kevin Morley, AWWA; John McCray, CSM	
9:30 a.m.	**Morning Break** *[Crystal Peak A]*	
	Keynote Speakers	***Invited Speakers***
10:00 a.m.	David Corman, NSF	Current Tools: Domain, Impact, Potential Gaps Mike Pozmantier, DHS S&T; Michael King, SNL; David McKinnon, PNNL; John Hummel, ANL; Julia Philips, ANL; Ron Fisher, INL; Ryan Hruska, INL; Craig Miles, INL
10:45 a.m.	Zach Tudor, DHS S&T	
11:30 a.m.	**Hosted Lunch with Plenary Speaker** *[Capitol Peak A]* Samara Moore, Chief Cyber Security Officer for the Office of the Under Secretary for Science and Energy, DOE	
	Keynote Speaker	***Invited Speakers***
1:00 p.m.	Robert Laddaga, DARPA	Current Tools: Domain, Impact, Potential Gaps Tim McPherson, LANL; Russell Bent, LANL; David Judi, LANL; Ben Thomas, ORNL; Steve Fernandez, ORNL
	Overviewing Questions for Panel/Facilitated Discussion	
2:00 p.m.	Facilitators: Chairs	Facilitators: David Alderson, NPS Ron Fisher, INL
2:30 p.m.	**Afternoon Break** *[Crystal Peak A]*	
	Panel Discussion	***Facilitated Discussion***
3:00 p.m.	ICS Security Facilitators: Chairs Track Keynote Speakers	Recognized Gaps and Needs Prioritization Facilitators: David Alderson, NPS; Ron Fisher, INL
4:30 p.m.	***Closing Thoughts*** *[Capitol Peak A]*	
4:40 p.m.	**Adjourn**	

Friday, August 22 - Tours

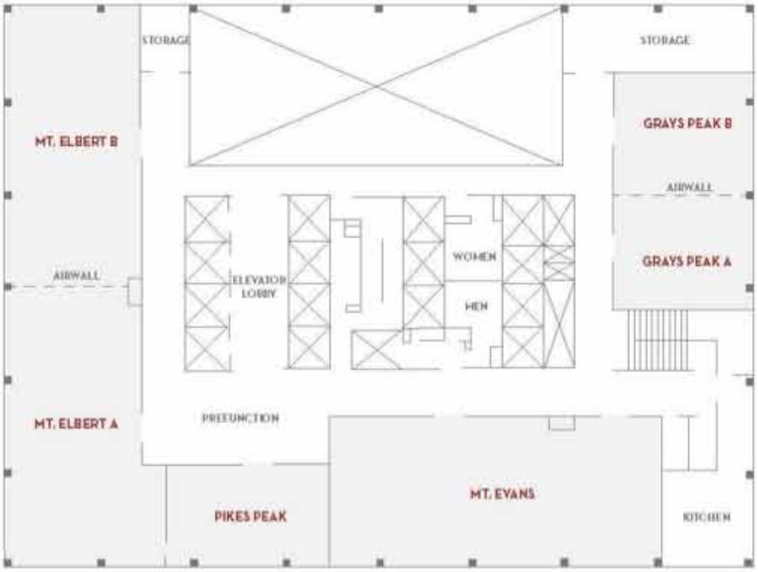
	Tours
9:00 a.m.	***Congregate for Tours*** *[Grand Hyatt Entry]*
9:30 a.m.	***The Money Museum at the Federal Reserve Bank of Kansas City - Denver Branch***
11:00 a.m.	***Historical Tour of the Colorado State Capital***
12:00 p.m.	**Tour Completion**

Venue Map

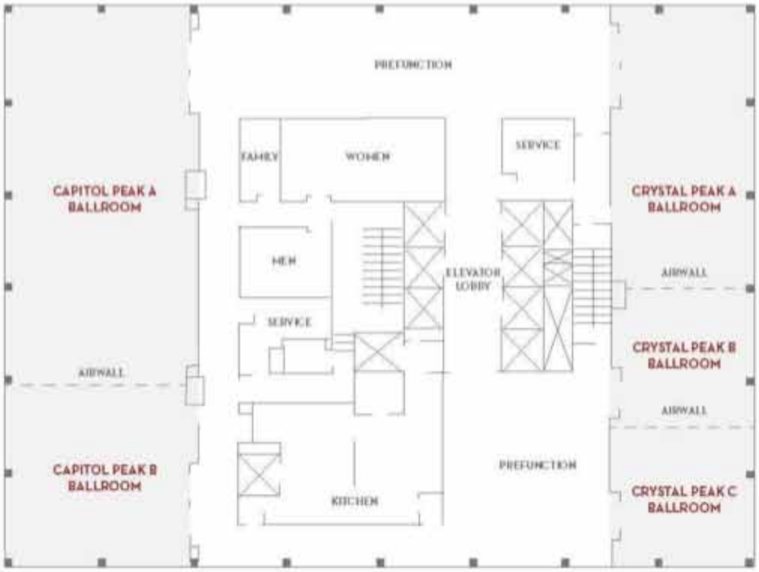
FLOOR PLAN

Atrium Tower

Grand Hyatt Conference Center–2nd Floor



Pinnacle Club–38th Floor



Resilience Week Plenary Speakers

Tuesday, August 19

William N. Bryan, U.S. Department of Energy

Symposium opening welcome address

William Bryan is the Deputy Assistant Secretary for Infrastructure Security and Energy Restoration in the U.S. Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE). The office of Infrastructure Security and Energy Restoration (ISER) works with the National Security Staff, other U.S. government agencies, and international partners to enhance the security and resiliency of critical energy infrastructure and facilitate the reconstruction and recovery of damaged or disrupted energy systems.

Bryan leads DOE's efforts in the coordination and collaboration of energy sector-related reliability and resiliency activities between the energy industry and the federal government. He also leads the office in support of the electricity, oil, and natural gas industries in the development and implementation of infrastructure protection strategies and methodologies both at home and abroad.

Rosemary Wenchel, DHS Deputy Assistant Secretary for Cybersecurity Coordination

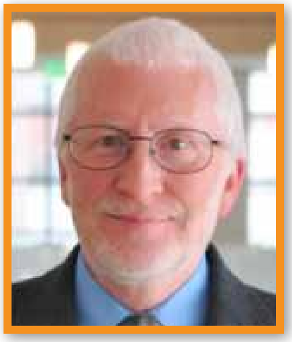
"Cyber/Physical Resilience in Critical Infrastructure"

A seasoned information operations director at the Defense Department, Rosemary Wenchel is the deputy assistant secretary for cybersecurity coordination in the Department of Homeland Security's National Protection and Programs Directorate. She coordinates joint cybersecurity initiatives among DHS, DoD and the National Security Agency while overseeing operations at the DHS-DoD Joint Coordination Element located at Fort Meade, MD, where NSA and the military cyber command are headquartered. Wenchel also works with DHS's Science and Technology Directorate to ensure the department's cybersecurity research and development efforts are coordinated with policy and operations.

Abstract

There is a need for critical infrastructure resilience and security in our increasingly cyber-physical society. This talk will cover the DHS perspective on resilience in Critical Infrastructure, related advances in cybersecurity, initiatives to increase information sharing and an update on the current status of cyber insurance.

Wednesday, August 20



Kevin Moore, Colorado School of Mines

"A dynamic network perspective on resilient control"

Kevin L. Moore is the Dean of the College of Engineering and Computational Sciences at the Colorado School of Mines. He received his B.S. and M.S. degrees in electrical engineering from Louisiana State University and the University of Southern California, respectively. He received his Ph.D. in electrical engineering, with an emphasis in control theory, from Texas A&M University in 1989. His research interests include iterative learning control, autonomous systems and robotics, and applications of control to industrial and mechatronic systems, including the cooperative control of networked systems. He is the author of the research monograph Iterative Learning Control for Deterministic Systems, co-author of the book Sensing, Modeling, and Control of Gas Metal Arc Welding, and co-author of the research monograph Iterative Learning Control: Robustness and Monotonic Convergence for Interval Systems.

Abstract

Many important systems can be modeled as a collection of integrating agents that exchange material, energy, or information with each other according to some protocol and interconnection topology. When that exchange is governed by differential equations we refer to such a system as a dynamic network. Of particular interest is the situation that arises when there is a tight integration of physical system dynamics, sensors and actuators, and computing infrastructure, resulting in what has come to be called a cyberphysical system. Such systems can be viewed as a dynamic network not only at the level of the physical process but also at the level of the sensing, communication, and control system, giving rise to the interpretation of complex systems as being networks controlled by networks. In this talk we consider how this interpretation can be applied to the analysis and design of system resilience – the ability for a system to return to normal operation as soon as possible after a disruption. Our approach is to model the resilient control problem as the problem of disturbance or noise attenuation in consensus networks. To motivate our approach we first note that a number of physically-relevant systems exist (e.g., the power grid) that can be modeled as a dynamic network. For such processes, we show how controller networks can be designed to reject two kinds of disturbances or attacks: sudden, time-limited disruptions and continuous-time disruptions. We also discuss how network topology can impact the ability to reject disturbances. We conclude by considering the extension of these ideas to more general problems related to sustainability.

Thursday, August 21

Samara Moore, White House National Security Staff

"Blurred lines: managing security and resilience in convergent world"

Samara Moore is the Senior Policy Advisor for the Under Secretary for Science and Energy, within the Department of Energy. Moore is responsible for the cyber policy and oversight for the programs within the Office of the Under Secretary, and has a leadership role in DOE's efforts to support security and resilience for the Energy sector. In June 2014, she returned to DOE from the White House National Security Council Staff, where she worked as the Director for Cybersecurity Critical Infrastructure Protection to coordinate across the federal government and partner with the private sector on efforts to strengthen cybersecurity for all critical infrastructure sectors.

Abstract

Innovation in technology continues to provide opportunities for increased reliability, safety, and efficiency. Organizations are modernizing their infrastructure, automating processes, becoming more connected, and increasingly leveraging telecommunications - as a result, understanding and managing cyber risk is KEY to ensuring secure and resilient infrastructure. Today organizations are experiencing convergence in multiple areas, including: information and operation technology (IT/OT), the role of vendors and external partners, and engaging corporate governance in addressing cyber risks. Mrs. Moore will highlight policy, operational, and cultural considerations for managing cyber risks and ensuring resilience in our changing world.

Semi-Plenary Speakers

Tuesday, August 19

William H. Sanders, University of Illinois at Urbana-Champaign

"Making sound design decisions using quantitative security metrics"

William H. Sanders is a Donald Biggar Willett Professor of Engineering, the Interim Head of the Department of Electrical and Computer Engineering, and the Director of the Coordinated Science Laboratory (www.csl.illinois.edu) at the University of Illinois at Urbana-Champaign. He is a professor in the Department of Electrical and Computer Engineering and Affiliate Professor in the Department of Computer Science. He is a Fellow of the IEEE and the ACM, a past Chair of the IEEE Technical Committee on Fault-Tolerant Computing, and past Vice-Chair of the IFIP Working Group 10.4 on Dependable Computing. He was the founding Director of the Information Trust Institute (www.iti.illinois.edu) at Illinois. He is currently the Director and PI of the DOE/DHS Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) Center (www.tcipg.org), which is at the forefront of national efforts to make the U.S. power grid smart and resilient.

Abstract

Making sound security decisions when designing, operating, and maintaining a complex system, such as the power grid cyber infrastructure, is a challenging task. Analysts need to be able to understand and predict how different factors affect the overall system security. To provide insight on system security and aid decision-makers, we propose the ADversary VIew Security Evaluation (ADVISE) method to quantitatively evaluate the strength of a system's security. Our approach is to create an executable state-based security model of a system. This talk describes the system and adversary characterization data that are collected as input for the executable model. It also describes the simulation algorithms for adversary attack behavior and the computation for the probability that an attack attempt is successful. A power grid distribution-side case study illustrates how to analyze system security using the ADVISE method. A tool is currently under development to facilitate automatic model generation and simulation.

Nancy Leveson, Massachusetts Institute of Technology

"A paradigm change in the way we engineer for safety and security"

Nancy Leveson is Professor of Aeronautics and Astronautics and also Professor of Engineering Systems at MIT. She is an elected member of the National Academy of Engineering (NAE). Leveson conducts research on the topics of system safety, software safety, software and system engineering, and human-computer interaction. In 1999, she received the ACM Allen Newell Award for outstanding computer science research and in 1995 the AIAA Information Systems Award for "developing the field of software safety and for promoting responsible software and system engineering practices where life and property are at stake." In 2005 she received the ACM Sigsoft Outstanding Research Award. She has published over 200 research papers and is author of two books, "Safeware: System Safety and Computers" published in 1995 by Addison-Wesley and "Engineering a Safer World" published in 2012 by MIT Press. She consults extensively in many industries on the ways to prevent accidents.

Abstract

Is resilience simply the latest buzzword that will be replaced in a few years with the latest magic solution to everything that ails us? Certainly, a tremendous amount of hype and promises have been associated with this term as well as straw man arguments. In this talk I will describe what is possible and not possible and how we make progress in ensuring safety and security by making a paradigm change in the way we engineer for safety and security without resorting to wishful thinking.

Lynne Parker, University of Tennessee, Knoxville

"Towards natural and reliable peer-to-peer human-robot teams"

Lynne Parker is Professor and Associate Head in the Department of Electrical Engineering and Computer Science at the University of Tennessee, Knoxville, where she directs the research of the Distributed Intelligence Laboratory. Additionally, she holds an appointment as Adjunct Distinguished Research and Development Staff Member at Oak Ridge National Laboratory (ORNL), where she worked as a full time researcher for several years. Parker received her Ph.D. degree from the Massachusetts Institute of Technology (MIT), performing her research in MIT's Artificial Intelligence Laboratory, with a minor in brain and cognitive science. She conducts research in the areas of distributed robotics, human-robot interaction, sensor networks, and machine learning, and has published over 145 articles in these areas. For this research, Parker was awarded the PECASE (U.S. Presidential Early Career Award for Scientists and Engineers) in 2000.

Abstract

In peer-to-peer human-robot teaming, a primary objective is to create a style of cooperation between robot(s) and human(s) that is reminiscent of well-practiced human-only teams. In these human-only teams, the individuals have trained together, and understand intuitively how to interact with each other on the current task without the need for explicit commands or conversations. Achieving such peer-to-peer teams requires technical advances in many areas, including fault-tolerance in multi-robot teams, as well as implicit communication amongst team members. Advances in intelligent approaches to fault tolerance will enable these teams to be reliable, while advances in implicit communication methodologies will help these teams feel more natural to human teammates. This talk will explore the technical challenges of achieving natural and reliable peer-to-peer human-robot teams.

Chris Wickens, Alion Science

"Black swans & lumberjacks: the role of complacency, automation bias and cognitive tunneling in human interaction with highly reliable automation"

Chris Wickens received his Bachelor degree in Physical Science from Harvard University in 1967 and his PhD in experimental psychology from University of Michigan in 1973. He served in the US Navy from 1969-1974. He was a Professor in Psychology and Aviation at the University of Illinois from 1973-2005. In this capacity he served as both head of the Aviation Human Factors Laboratory and as Associate Director of the Institute of Aviation. He has subsequently worked as a senior scientist at Alion Science and Technology, and as a visiting professor of Psychology at Colorado State University. Wickens has published extensively on issues of human attention in complex systems, and their relevance to safety (particularly in aviation), and has authored two textbooks on Human Factors and Engineering Psychology.

Abstract

In airspace and other industries, system efficiency is increasingly accomplished by a high degree of highly reliable automation. However resilient systems in safety critical industries must keep an operator in the loop in order to respond on the rare occasions when automation fails. A major paradox is that the higher the degree and reliability of automation, the greater the problems of human failure response on those very rare, but inevitable, occasions when automation does fail. These very rare occasions are a class of phenomena that Taleb describes as "black swans", and the tradeoff of automation support for routine performance, and human response for unexpected failure performance is known as the lumberjack phenomenon: the higher they are, the harder they fall.

Underlying the poor failure response with higher degree and reliability of automation is the loss of situation awareness, which can be decomposed as a loss of capability for (1) noticing failures (2) understanding or diagnosing failures and (3) predicting the implications of failure for safety management. We briefly describe three major shortcomings or biases identified in human-automation interaction research underlying each of these: respectively change blindness, the automation bias, and cognitive tunneling. Possible ways of mitigating these can be achieved through training (turning black swans to gray swans), flexible automation, and displays.

Stephen Flynn, Northeastern University

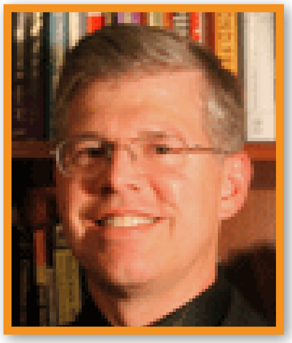
"Understanding the resilience imperative: lessons learned from Superstorm Sandy"

Stephen Flynn has conducted research and informed policymaking on transportation security and infrastructure and community resilience issues for over two decades. He is currently leading a project funded by the Alfred P. Sloan Foundation, "After Superstorm Sandy: Bolstering the Resilience of Metro-New York's Infrastructure." He is the author of numerous books, chapters, and articles on homeland security. Prior to September 11, 2001, he served as an expert advisor to U.S. Commission on National Security (Hart-Rudman Commission), and following the 9/11 attacks he was the principal advisor to the Congressional Port Security Caucus. He holds a M.A.L.D. and Ph.D. from the Fletcher School of Law and Diplomacy at Tufts University and a BS from the US Coast Guard Academy.

Abstract

Escalating societal losses associated with unexpected events such as terrorism, natural disasters, and the mounting risk associated with cyber-attacks on physical infrastructure are focusing attention on new approaches to reducing damages and mitigating consequences. Whereas the dominant approach in recent years has been to invest in efforts that identify and reduce threats, there is now a growing interest on emphasizing building greater societal resilience. For example, in February 2012, the Obama administration released an executive order (EO-13636) and presidential policy directive (PPD-21) that focus national attention on improving critical infrastructure and cyber resilience. This keynote presentation will identify how lessons learned from Superstorm Sandy should inform what can be done to advance critical infrastructure resilience.

Wednesday, August 20



Michael VanPutte, MOD-2 Systems, LLC

"Resilient system, or a pyrrhic victory?"

Michael VanPutte is the Chief Scientist of MOD-2 Systems, LLC where he leads multi-disciplinary research and consulting projects involving conflict in cyberspace. He has over twenty-five years successfully building and leading research and operational projects. VanPutte was a government Program Manager at the Defense Advanced Research Projects Agency (DARPA) from 2006 – 2010 where he created and manger numerous cyber programs including the National Cyber Range, Dynamic Quarantine of Worms, and the Cyber Genome Program as well as numerous studies and research initiatives focused on revolutionizing cyber security and cyber scientific experimentation. He received a BS from The Ohio State University, an MS in Computer Science from the University of Missouri - Columbia, and a Ph.D. in Computer Science from the Naval Postgraduate School.

Abstract

Cyber incidents have become everyday occurrences as cyber threats have become more technical and complex. The community has responded by researching and developing systems that are resilient to both benign and malicious events. However, to develop robust resilient cyber solutions that can be deployed in operational environments we need to think of the problem holistically. Developers and decision makers must understand not only how an adversary thinks to defeat resilient systems, but also how an adversary may use our cyber reliance against us. This is not about understanding specific threats, or gathering intelligence on specific individuals or groups, but understanding that attackers think differently than defenders, and developers and decision makers must understand these differences.

VanPutte has first-hand experience in this area. While assigned to the Joint Task Force - Computer Network Operations, and Joint Task Force - Global Network Operations, predecessor of US Cyber Command, Lieutenant Colonel VanPutte was responsible for the Department of Defense enterprise defensive and offensive cyber operations. Subsequently, VanPutte was at DARPA where he created the vision to revolutionize the nation's cyber experiment and operations technologies, including creating and running the National Cyber Range, Dynamic Quarantine of Worms, and Cyber Genome programs.

This contrarian, and a bit controversial talk will address eight key issues cyber resilient researchers, developers, or decision makers need to understand, including "security buzzwords and myths", "how defenders make attackers more resilient and encourage attacks", and "the most malicious people may never touch your network."

Jalal Mapar, Department of Homeland Security, Resilient Systems Division

"The Role of Science and Technology in Enabling Resilience"

Jalal Mapar serves as the Director of the Resilient Systems Division (RSD) at the DHS Science and Technology Directorate (S&T). RSD's mission is to rapidly develop and deliver innovative solutions that enhance the resilience of individuals, communities, and systems by enabling the Whole Community to prevent and protect against threats, mitigate hazards, effectively respond to disasters, and expedite recovery. Mapar has been recognized by DHS S&T for his leadership in developing and transitioning technologies to customers across DHS and establishing collaborations with several universities, national labs, U.S. and international government agencies. He is a member of the JSDE Executive Board, Panelist/Session Organizer/Chair at IEEE, ION, JNC, TCIP, and other conferences, and a frequent speaker on DHS related science and technology topics.

Abstract

Resilience, Resilience, Resilience!

What does it mean and how broad is it: critical infrastructure, disaster management, community, individual? Are we resilient and how do we know we are resilient? How do we measure resilience? Can technology help achieve resilience?

These are some of the questions that we are considering and use as a foundation for developing science and technology capabilities to help enable resilience. The broad mission presents a challenge and requires a clear approach that is manageable, cost effective, and provides near term and long term results for experimentation and evaluation leading to deployment. This presentation will provide an overview of DHS Science and Technology's Resilient Systems Division, areas where Research and Development (R&D) is being conducted to enhance the resilience of the Critical Infrastructure, and areas where future R&D is needed to enhance the resilience mission.

Thursday, August 21

David Corman, Boeing

"Recent trends in security for cyber physical systems – can the physical element in CPS security help us"

Dr. David Corman is lead Program Director for the Cyber Physical Systems program at the National Science Foundation. Corman has a broad range of research interests spanning many technologies fundamental to CPS application areas including transportation, energy, medical devices, and manufacturing. He has extensive industrial experience in the development, design, and manufacture of CPS systems including manned and unmanned systems. Corman received a Ph.D. degree in electrical engineering from the University of Maryland.

Abstract

Cyber-physical systems are subject to threats stemming from increasing reliance on computer and communication technologies. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, public safety, and health at risk.

Cyber Physical Systems are fundamentally different than enterprise network systems. Securing them imposes a new set of challenges that must be addressed. These challenges arise from the non-reversible nature of the interactions of CPS with the physical world; the scale of deployment; the federated nature of several infrastructures; the deep embedding and long projected lifetimes of CPS components; the interaction of CPS with users at different scales, degrees of control, and expertise levels; the economic and policy constraints under which such systems must often operate; and sensing and collection of information related to a large spectrum of everyday human activities. In addition, CPS will generally not have a "system administrator" to resolve security issues, and there may be significant operational challenges in updating system security software. The interaction of the system with the physical world, however, offers some opportunity that can be leveraged by the security approach.

This talk will address CPS security challenges, present a perspective on recent trends in solutions, and discuss whether the physical world can be our friend here.

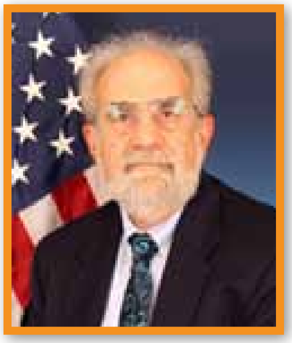
Zachary Tudor, SRI International

"How much resilience do we need, and how do we get it?"

Zach Tudor, a Program Director in the Computer Science Laboratory at SRI International, serves as a management and technical resource for operational and research and development cyber security programs for government, intelligence, and commercial projects. He supports DHS's Cyber Security Research and Development Center (CSRDC) on projects including the Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC) consortium, and the Industrial Control System Joint Working Group (ICSJWG) R&D working group. Tudor is the past Co-Chair of the Institute for Information Infrastructure Protection (I3P), is a member of the Nuclear Cyber Security Working Group, and represents SRI in the International Information Integrity Institute (I-4), a world forum for senior information security professionals.

Abstract

Based on the "new" realization that we will never be able to stop all cyber attacks, resilience is currently favored as a system development and attack mitigation approach. Resilience implies an ability to degrade gradually and predictably, and recover effectively and rapidly. The key problems in this approach are determining what resilience means in different domains and different applications. Meanwhile, the progenitors of resilience: high assurance, fault tolerance, and redundancy; now find themselves competing for prominence and relevance. In view of competing priorities, unclear requirements, and limited resources, how can we identify and deliver the right amount of resilience for our needs?



Robert Laddaga, DARPA

"Active perception and cyber security"

Robert Laddaga joined DARPA in October 2013. His research interests include resilient computing systems and artificial intelligence (AI). He joined DARPA from Vanderbilt University, where he was a research professor in the Electrical Engineering and Computer Science Department of the School of Engineering. He was also a member of the Institute for Software Integrated Systems (ISIS) at Vanderbilt. Laddaga holds a Doctor of Philosophy degree from Stanford University, a Master of Science degree in Philosophy from the University of South Carolina, and a Bachelor of Science degree in Mathematics from the University of South Carolina. He has published nearly 40 peer-reviewed computer science papers and co-authored or edited four books.

Abstract

The talk presents a theory about perception that highlights multiple uses of feedback, including feedback from results of action to perceptual interpretation, and feedback from interpretation to low level control of sensors and signal processing. It further discusses the application of this theory to cyber defense, and Intrusion Detection and Response specifically. The talk also discusses the relationship between Active Perception and defensive maneuver in cyberspace.

Track Descriptions

Tuesday, August 19

Resilience Models and Measures

The Resilient Models and Measures track will focus on the presentation and discussion of new theories, techniques and practices for the design and evaluation of resilient systems. The definition of effective and representative models and metrics is an important element for the design, control, and evaluation of practical resilience techniques. The track will include a number of invited presentations that will provide an interdisciplinary perspective to the problem.

Mixed Human-Automation Resilience

This track considers situations where humans must interact with automation or autonomy and its impacts on resilience. Many times, there are problems that are best solved by allowing for a collaboration between human intelligence and computational intelligence. However, it is often much more difficult to predict the performance of the human, which may change from day to day, or from human to human. The benefits gained by allowing humans and computers to collaborate is too great to ignore. However, it makes the job of understanding the resilience of the system more difficult. The methods of interaction between humans and autonomy are still emerging as well. These two issues make Mixed Human / Automation Resilience a topic of current study.

Resilient Infrastructure

Creating and sustaining resilient critical infrastructure is a diverse and complex mission. Critical infrastructure systems in the United States consist of a diversity of interdependent networks, varied operating and ownership models, systems in both the physical world and cyberspace, and stakeholders from multi-jurisdictional levels. Methods to improve critical infrastructure resilience are advancing, but much more can be done. Large-scale disasters have revealed that decision makers often struggle to identify or determine key components and interdependency relationships in infrastructure systems, optimal resource allocation to increase resilience or reduce risk, and optimal response plans. The Resilient Critical Infrastructure Symposium seeks to bridge the gaps among local, city and state entities, infrastructure owner-operators, federal agencies, and researchers to advance a productive discussion of tools, technologies, and policies for improving critical infrastructure resilience.

Wednesday, August 20

Some sessions will be multidisciplinary across tracks.

Resilient Cyber Systems

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

Resilient Control Systems

The major purpose of this symposium is to extend and endorse particular concepts that will generate novel research and codify resilience in next generation control system designs. Engineering systems are increasingly subjected to disturbances which are not generally predictable at design time. These disturbances can be man-made or naturally occurring, and they can be physical or cyber in nature. A multi-disciplinary approach for designing controls for these systems is envisioned that provides the intrinsic state awareness and intelligence that give the overall system an increased level of resilience.

Resilient Cognitive-Communication Systems

Cognitive

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

Communication

Many commercial and government applications require reliable and secure communications for effective operations. These communications are often challenged in contested environments – whether from hostile states in an anti-access area denial scenario, degraded infrastructure following a man-made or natural disaster, or ¬nite spectrum pressure that restrict agility. The symposium will highlight how incorporation of resiliency in communications systems can support a wide range of applications given uncertainty in the communication environment.

Resilient Critical Infrastructure

Creating and sustaining resilient critical infrastructure is a diverse and complex mission. Critical infrastructure systems in the United States consist of a diversity of interdependent networks, varied operating and ownership models, systems in both the physical world and cyberspace, and stakeholders from multi-jurisdictional levels. Methods to improve critical infrastructure resilience are advancing, but much more can be done. Large-scale disasters have revealed that decision makers often struggle to identify or determine key components and interdependency relationships in infrastructure systems, optimal resource allocation to increase resilience or reduce risk, and optimal response plans. The Resilient Critical Infrastructure Symposium seeks to bridge the gaps among local, city and state entities, infrastructure owner-operators, federal agencies, and researchers to advance a productive discussion of tools, technologies, and policies for improving critical infrastructure resilience.

Thursday, August 21

Industrial Control System Cyber Security

"….It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties…" – Executive order from President of United States, Feb. 12, 2013. Across the world, it is clear that critical infrastructure is susceptible to computer and network attacks against the Industrial Control Systems (ICSs) that operate the water, power, gas, and transport systems. The track on industrial control system cyber security provides insight into origins, problems, issues, challenges, innovations and best practices for the computer and network security issues relating to ICSs.

Cyber-Physical Resilience: Infrastructure Needs and Capabilities User Group Session Planning

This track is intended to provide a perspective on the cyber-physical resilience needs and capabilities for critical infrastructure. The track will start with an industry panel to discuss infrastructure needs, focusing on water and power. This will be followed by two sessions where cyber-physical resilience "programs" and "tools" will then be overviewed. The track will conclude with a government panel to discuss gaps and priorities. Program overviews will provide the vision and mission of the program, current cyber-physical resilience tools being funded, and those planned. Presentations will also reflect on opportunities for engagement. Tool presentations will include reference to the domain(s) benefited, the capabilities of the tool to benefit resilience, the impact (users) of the tool and future plans. For more information on the programs and tools, see Appendix.

Special Events and Additional Information

The Money Museum at the Federal Reserve Bank of Kansas City - Denver Branch

Tour Start Time: 9:30 am

The Money Museum at the Federal Reserve Bank of Kansas City—Denver Branch is a unique experience offering a free, up-close look of the nation's financial system in action.

As the nation's central bank, the Federal Reserve is a vital part of what makes the economy work. At the Money Museum, you can learn more about the Fed through interactive exhibits that explore banking, how people pay for things and how monetary policy decisions impact your family's bottom line. You'll also be able to take a peek at $30 million.

Historical Tour of the Colorado State Capitol

Tour Start Time: 11:00 am

Historical tours begin on the first floor and consist of early Colorado history, Capitol construction, several stained glass windows, Women's Gold Tapestry, Presidential portraits, and a stop outside the Senate and House of Representatives chambers.

Resilience Week Organizers

Organizing Committee

- Jodi Grgich, Idaho National Laboratory
- Vivek Agarwal, Idaho national Laboratory
- Dina Fragkedaki, DU2SRI, University of Denver
- Chandrasekhar Potluri, Mercedes-Benz Technology
- Indrajit Ray, Colorado State University
- Matt Rutherford, DU2SRI, University of Denver
- Michelle Cozzi, General Dynamics Information Technology

Steering Committee

- Ron Boring, Idaho National Laboratory
- Marco Carvalho, Florida Institute of Technology
- Frank Ferrese, Temple University
- Milos Manic, University of Idaho
- Craig Rieger, Idaho National Laboratory

Appendix

1. Program Abstracts

1.1 Mike Pozmantier, HSARPA. Technology to Practice

The Department of Homeland Security Science and Technology Directorate has White House support to assist in transitioning cyber security technologies developed through federally funded research and development (R&D) into broader utilization. The Transition to Practice (TTP) program was identified by the Federal Networking and Information Technology R&D (NITRD) program of the White House as one of a set of interrelated priorities for the United States Government (USG) – and established DHS as the lead for this interagency initiative. The goal of this effort is to: (1) identify mature technologies that address an existing or imminent cyber security gaps in public or private systems that impact national security, (2) identify and fund necessary incremental improvements, and (3) increase utilization through partnerships, product development efforts and marketing strategies. Efforts focus on identified technologies that have a reasonably high probability of successful transition within a two-year timeframe, and which would have notable impact on the cybersecurity of our nation's networks or systems. This is a very ambitious endeavor with enormous potential for positive impact.

1.2 John Hummel, ANL. Argonne's Critical Infrastructure Protection and Resiliency Assessment Programs

Argonne's programs in critical infrastructure protection and resilience provide an integrated view of the interconnections between infrastructures, the cyber realm, the environment, and society. These programs are helping to make the Nation's regions and communities more protected and resilient to many hazards, such as natural disasters, manmade events, aging infrastructure and climate change.

1.3 Ron Fisher, INL. Holistic Approach to Resilient Systems and Control Architectures

Idaho National Laboratory's program is focused on advancing the critical infrastructure protection and resilience mission by solving the challenges associated with the integration of physical and cyber security, life line sector resilience, infrastructure fragility, and environmental impacts. The DHS Program office is leveraging INLs long history of scientific expertise, engineering discipline and unique infrastructure assets to develop a suite of capabilities that enable a more holistic risk management approach that includes physical security, cyber security, infrastructure operations and an enhanced understanding of infrastructure dependencies and interdependencies. Together, these capabilities address the daily challenges faced by our homeland security, law enforcement and military stakeholders.

1.4 Tim McPherson, LANL. Energy and Infrastructure Analysis

The Energy and Infrastructure Analysis Group at Los Alamos National Laboratory (LANL) has developed a suite of advanced modeling and analysis tools to estimate potential impacts of disruptive events—natural or manmade—on population, infrastructure, and economy in an affected area. These analyses provide detailed, quantified information on the physical, operational, and economic behavior of energy networks and water and transportation systems. DSA-4 can provide analysis results quickly during a crisis, and also perform studies of anticipated scenarios before they happen. Analysis results can be extended to inform disaster planning and recovery operations across infrastructure networks and to assess asset resilience in the face of disaster. These analyses help decision makers understand infrastructure protection, mitigation, response, and recovery options. LANL has supported infrastructure protection for 20 years with advanced research and development of new modeling and simulation techniques, operational support, and infrastructure data acquisition.

1.5 Ben Thomas, ORNL. ORNL Critical Infrastructure Network Disruption Modeling Program

The objective of ORNL's Critical Infrastructure Disruption Models is to provide data and analysis of situational awareness by integrating several web streaming services to create not only a national, but also an international visualization Common Operational Picture (COP). These models, whose results are continuously streamed to the responder community includes several tools. The most versatile web streaming tool is Visualizing Energy Resources Dynamically on Earth (VERDE). Similar to Google Earth®, VERDE contains several layers, and analysis modeling components to advocate almost instantaneous spatial awareness, not only throughout the national power grid, but also among other critical infrastructure networks. VERDE combines current infrastructure and forecast disruption models with predictive, look ahead models to improve response and repair time, to enhance the decision process, to foster improved customer-utility relationships. The Department of Homeland Security (DHS) HEAT tool combines climate change adaptation, complex forecasting and modeling to support more accurate hazard forecasts, and population estimates via the LandScan Database. This Tool set determines threats related to extreme weather events, to analyze potential critical infrastructures impacts, to assess alternative adaptive risk management, and to reduce risks and costs associated with critical infrastructure protection. Current capabilities include: real-time electric grid status and weather data for all-hazards, and anticipatory models to forecast cascading failures. The Enhanced Data Layer program develops datasets, through remote measurement and observations, to characterize complex facilities. The final product is a shareable-open source Electric Energy infrastructure geospatial vector data layer for use by infrastructure modelers.

2. Tool Abstracts

2.1 Michael A. King, SNL. WeaselBoard: Zero-Day Detection for PLCs

WeaselBoard captures traffic between the modules of programmable logic controllers (PLCs). By monitoring backplane traffic, WeaselBoard detects changes to process control settings, sensor values, module configuration information, firmware updates, and process control program (logic) updates. WeaselBoard detects 0-day attacks with minimum intrusion and footprint.

2.2 David McKinnon, PNNL. Digital Ants

Digital Ants is a resilient cyber security framework designed to protect large infrastructures in a decentralized manner. At the core of the framework are the Digital Ants Sensors, small single-purpose agents that constantly roam a networked infrastructure. When an agent identifies an anomalous value it leaves a digital pheromone trail, much like a real-world ant leaves a chemical pheromone trail. A single alert is not conclusive because it is based upon only one metric (e.g., CPU usage, file I/O, network I/O). But, when multiple sensors measure several anomalous metrics, the resultant pheromone trails will cause agents to swarm around the node in question. This collective, swarming behavior provides input to higher-level agents. These Digital Ants Sentinel and Sergeant agents then inform human operators of significant issues of concern.

2.3 Russell Bent, LANL. Infrastructure Restoration and Expansion Planning (IREP) Tool

IREP is an optimization analysis tool that helps stakeholders (e.g., utilities, first responders, planning authorities and regulators) create plans for the development of resilient infrastructure systems. IREP can support short-term response planning for infrastructure systems following natural disasters. IREP also supports the design of system expansion plans that improve reliability and resilience of infrastructure systems relative to potential future hazards.

2.4 David Judi, LANL. Water Multiple Infrastructure Simulation Technology (MIST).

MIST is a web-based simulation environment supporting the modeling of critical water infrastructure systems. Water MIST allows users to set-up and run water system resilience studies from multiple devices and systems regardless of local computational resources.

2.5 Julia Phillips and Frederic Petit, ANL. Indicators of Critical Infrastructure and Community Resilience

Several studies have provided a range of perspectives on the role of resilience in policies and programs designed to address natural and man-made threats. A review of those studies reveals that there is strong agreement that the concept of resilience must play a major role in assessing the extent to which various entities—critical infrastructure and key resources, systems, communities, and regions—are prepared to deal with the full range of threats they face. The resilience of each of these components can be integrated through a framework developed to capture holistic community resilience. This presentation will highlight a resilience related indicator for critical infrastructure and discuss preliminary tools developed to capture preparedness of emergency responders and the local community at large. Through the integration of these components a community can better understand its current resilience posture, as well as implement a systematic approach to reduce the consequences of potential threats or hazards.

2.6 Julia Phillips and Frederic Petit, ANL. Mathematical Disruption and Impact Models for Addressing Regional Resilience

Assessing infrastructure resilience requires consideration of many interconnected socioeconomic, ecological, climatic, and technical elements. Sandy and other recent disasters have underscored the need to utilize a combination of mathematical tools and impact models to improve overall understanding of critical infrastructure systems and lay the foundation for enhanced resilience. The objective of this session is to discuss three tools developed by Argonne National Laboratory: EPFast, NGFast, and Restore©. These three models can be used in tandem with each other to provide a more holistic picture of infrastructure resilience. While these models provide insight on a small portion of community or regional resilience, they are an important step in creating a framework to better understand how connected our critical infrastructure systems are and the impacts of disruptions to these systems.

2.7 Ryan Hruska, INL. Cross-cutting Interdependency Analysis Tool Suite

The ability to assess vulnerabilities, resiliency, and identify priorities for protective and support measures for interdependent critical infrastructure systems from an all hazards perspective remains an open and difficult problem at the federal, state and local levels. In order to help address this challenging national need, the INL in collaboration with its mission partners have develop a number of tools to enhance the understanding of dependencies and interdependencies between critical infrastructures and their potential consequences if disrupted. These tools include:

CEA (Consequence Effects and Analysis), PGVT (Power Grid Visualization Tool), CIAS (Critical Infrastructure Assessment and Simulation), and (AHA) All Hazards Knowledge Framework.

2.8 Craig Miles, INL. The Intelligent Cyber Sensor (ICyS)

The ICyS A network security and information solution that utilizes intelligent mechanisms to recognize anomalous network traffic, identify network hosts and dynamically instantiate deceptive virtual honeypots. The design concept is composed of an integrated framework of communication fundamentals derived from Autonomic research and Service Oriented Architecture (SOA). The main system components are implemented as replaceable modules that utilize a common Inter-Process communication standard.

2.9 Steve Fernandez, ORNL. Visualizing Energy Resources Dynamically on Earth (VERDE)

The most versatile web streaming tool is Visualizing Energy Resources Dynamically on Earth (VERDE). Similar to Google Earth®, VERDE contains several layers, and analysis modeling components to advocate almost instantaneous spatial awareness, not only throughout the national power grid, but also among other critical infrastructure networks combines current infrastructure and forecast disruption models with predictive, look ahead models to improve response and repair time, to enhance the decision process, to foster improved customer-utility relationships. VERDE receives physical infrastructure and key resources data from the eighteen critical infrastructure networks, spanning more than 54 integrated foundational and streaming data sources, which are converted to KML, WMS, WFS, and REST formats. Extreme weather events, disruption threats information, status of infrastructure services are streamed and updated, along with social media posts. The culmination of incoming data initiates anticipatory forecasts and models to create informed command decisions.

2.10 Steve Fernandez, ORNL. The Department of Homeland Security Extreme Weather Analysis Tool (HEAT) and Enhanced Data Layer

The Department of Homeland Security (DHS) Climate Change Adaptation Road Map combines climate change adaptation, complex forecasting and modeling to support more accurate hazard forecasts, and population estimates via the LandScan Database. The tool set determines threats related to extreme weather events, analyzes potential critical infrastructures impacts, to assess alternative adaptive risk management, and reduces risks and costs associated with critical infrastructure protection. Current capabilities include: real-time electric grid status and weather data for all-hazard, future models to prevent cascading failures.

The Enhanced Data Layer program develops datasets, through remote measurement and observations, to characterize complex facilities. The deliverable for this project is a shareable-open source Electric Energy infrastructure geospatial vector data layer; developed, characterized, infrastructure, satellite image features. Remote sensed data is converted to topology, through the fusion of image classification, computer vision, and image labeling. Advanced analytics created a maintainable replacement data set for Advanced Grid Modeling by developing a functional equivalent of the HSIP Gold dataset without using either proprietary sources or limited by non-disclosure sources. Areas without open utility data were successfully provided by digitizing published open source Federal Energy Regulatory Commission (FERC) reports that contained unlimited imagery distribution and validation, performed at the national laboratories The limited or unobservable data, such as underground pipelines, were obtained by a culmination of multiple, past laboratory datasets.

Resilience Week
2015
Transforming the Resilience of Cognitive, Cyber-physical Systems
Hosted in Philadelphia, PA
August 18-20, 2015

Resilience Week 2015

The city of Philadelphia has a lot to offer! Within a short distance from the conference location, you will find Fine Arts, several historical sites, casual and fine dining, and plenty of shopping opportunities. Take some time to explore the Liberty Bell, Art Museum, Reading Terminal Market, Academy of Natural Sciences, professional sports arenas, or maybe take a trip to University City or South Philadelphia! There is truly something here for everyone. Visit www.visitphilly.com and www.uwishunu.com for more information.

Resilience Week 2014