**CREDC Summer Symposium**

**June 23rd-28th, 2019**

Information is subject to change

2019 CREDC Summer Symposium Presenter Bio’s and Presentation Abstracts

Monday, June 24th | Q Center, Theater (Main Room) & Ballroom

|  |
| --- |
| **David Lawrence, Technology Development Manager, Duke Energy:**David Lawrence is a Technology Development Manager with Duke Energy working in the Emerging Technology Office for the last 5 years. In this role, he provides leadership on a portfolio of technologies to support the Future Electric Grid. He is a founding technologist in the development of the OpenFMB platform. He is currently working on Electric Grid distributed applications, Microgrids, DC services and metering, and Grid edge analytics. His current focus is Cybersecurity for Grid Edge Devices (IIoT and PKI).Mr. Lawrence has 40 years of experience in the Electric Sector though a broad set of roles with Westinghouse and ABB. He worked in R&D, product development, and IT management for electric metering, transformers, sensors, and switchgear products. His roles included microprocessor embedded systems development, engineering management, global engineering information systems, manufacturing execution (MES) and scheduling systems (ERP), product life-cycle management (PLM), and IT management. A native of Portsmouth, VA., Mr. Lawrence earned a Bachelor of Science degree in Computer Science from Virginia Polytechnic Institute and has been awarded six US Patents.**“Progress in DERs, DAFs, Interoperability, Cybersecurity, and Standards**…**Is it Enough? Top 5 Issues in Grid OT Cybersecurity”**Increased interoperability will introduce additional threats to the Grid. There will be need for cyber security standards to combat this threat that can compromise data integrity. This talk will discuss the ongoing work in this space and highlight the top 5 current issues in GRID OT cyber security. |
| **Joel Robertz, Special Agent, FBI Chicago:**Special Agent Robertz joined the FBI in 1996. Assigned to the FBI’s Chicago Field Office, he investigated a broad range of counterintelligence threats for eleven years. He subsequently supervised squads in the counterintelligence, counterterrorism, and human intelligence programs in Chicago before serving as a unit chief in the Counterespionage Section at FBI Headquarters. His last supervisory assignment included oversight of joint cyber/counterintelligence investigations. He is currently responsible for coordinating operational counterintelligence and cyber outreach initiatives for FBI Chicago.**"FBI’s Cybersecurity mission and what role the FBI would play in a cyberattack against a utility"**The partnerships between the law enforcement and the power utility industry is vital. The partnership will go a long way in developing early awareness and coordinating an effective response to combat cyber threats to utilities. In this talk, we will learn about the strategies, priorities and processes undertaken by FBI officials to combat cyber threats to utilities. |

|  |
| --- |
|  **Venkatesh Venkataramanan is a fourth year Ph.D. student in the School of Electrical Engineering and Computer Science at Washington State University** co-advised by Prof. Anurag Srivastava and Prof. Adam Hahn. He completed his Masters in electrical Engineering from Washington State University. His interests are in cyber-physical system analysis, and resilient microgrid design and operation.  **Aolin Ding is a third year Ph. D. student in the Department of Electrical and Computer Engineering at Rutgers University** advised by Prof. Saman Zonouz. His research interests are in cyber-physical security problems such as firmware security, intrusion detection and runtime verification of safety-critical components in energy delivery systems (EDS).**“CyPhyR – A real time cyber-physical analysis tool for resilient microgrid operation and planning.”**This talk presents a tool to study the cyber-physical resiliency of the microgrid, in particular the effect of cyber events on the microgrid's resiliency for planning phase and operation phase. The microgrid resiliency is formulated based on graph theoretic metrics and power system constraints. A Common Vulnerability Scoring System (CVSS) based metrics was developed to analyze possible cyber events. Cyber Asset Impact Potential (CAIP) is used in the planning phase, and Cyber Impact Severity Score (CISS) is introduced in the operation phase to study the system vulnerability. The information from these two phases is provided to the operator to make informed and proactive decisions to ensure the resilient operation of the microgrid. |
| **Sachin Shetty, Associate Professor, Old Dominion University | CREDC:**Sachin Shetty is an Associate Professor in the Virginia Modeling, Analysis and Simulation Center at Old Dominion University. He holds a joint appointment with the Department of Modeling, Simulation and Visualization Engineering and the Center for Cybersecurity Education and Research. Sachin Shetty received his PhD in Modeling and Simulation from the Old Dominion University in 2007. His research interests lie at the intersection of computer networking, network security and machine learning. His laboratory conducts cloud and mobile security research and has received over $10 million in funding from National Science Foundation, Air Office of Scientific Research, Air Force Research Lab, Office of Naval Research, Department of Homeland Security, and Boeing. He is a co-principal investigator on the DoD Cyber Security Center of Excellence, the Department of Homeland Security National Center of Excellence, the Critical Infrastructure Resilience Institute (CIRI), and Department of Energy, Cyber Resilient Energy Delivery Consortium (CREDC).**"Buffer Overflow in ICS - Attacks and Countermeasures" Presentation & DEMO**Buffer overflow vulnerabilities have been exploited in Industrial Control Systems (ICS) that allow attacker to inject malicious data or modify software execution. The vulnerability involves a program attempting to write data beyond the boundaries of pre-allocated fixed buffer length. Examples of buffer overflow vulnerabilities in ICS products, include remote code execution on ICS hosts, password buffer overflow in Web Human-Machine Interface (HMI) Web server, multiple buffer overflows in network packet parsing application, overflows in application that accept command line and process control arguments over the network. We will provide a hands-on experience in learning how buffer-overflow vulnerability is exploited to alter the flow control of a program and execute arbitrary code fragments. Attendees will be provided a program with a buffer-overflow vulnerability. They will learn how to exploit the vulnerability to gain root privileged access on the target system. The attendees will also learn about protection schemes to mitigate the impact of buffer overflow attacks. |

Tuesday, June 25th | Q Center, Theater (Main Room) & Ballroom

|  |
| --- |
| **Ryan Speers, Managing Partner, River Loop Security**Ryan is a managing partner of River Loop Security and has assessed a wide range of embedded devices, finding vulnerabilities by physical attacks, network access, firmware reversing, and other techniques. He has led design of remediation’s or new systems, frequently focusing on their cryptographic protocols and protections. Ryan is also known for his research on the security of radio protocols, including IEEE 802.15.4/ZigBee and maintenance of the KillerBee framework frequently used to assess these protocols.Ryan also leads efforts at Pilot Security in providing a state-of-the-art automated security assessment platform for embedded firmwares.He has published peer-reviewed articles at USENIX WOOT (Packets in Packets: In-Band Signaling Attacks for Modern Radios), HICSS (wireless tools), Workshop on Embedded System Security (USB as a “network” attack surface for embedded systems), and MILCOM. Additionally, he has presented at the ShmooCon, ToorCon Seattle, DefCon Wireless Village, and Troopers information security conferences. Ryan also is the inventor on a number of patents related to key management and encryption at scale.Ryan has worked as a security researcher and developer with the US Government, a fraud detection company, a university, and a VC-backed start-up enterprise security and encryption company. He holds a Computer Science degree from Dartmouth College and various other trainings.**"Assessing IEEE 802.15.4/ZigBee Attack Surface with KillerBee"**Industrial devices increasingly connect via gateways or as native IIoT devices, many of which are built on ZigBee (or other protocols atop IEEE 802.15.4). The security of these networks can’t be found via IP network scanning or mobile application assessment, yet they present upstream risks into traditional networks or via the data used in mobile apps.KillerBee continues to be the primary tool for manufacturers and penetration testers to use to assess these networks. We will discuss the various options someone has to assess their networks using KillerBee and provide a ‘quick start’ orientation to the tool to make it easy for people to successfully get started. |
| **Dominic Saebeler, Director of Cybersecurity and Risk Management, Illinois Commerce Commission**Dominic Saebeler is the Director of the Illinois Commerce Commission’s Office of Cybersecurity and Risk Management where he focuses on cybersecurity awareness, best practice adoption and assessment of the effectiveness and capabilities of utility security strategy and preparedness. In addition to working with utility industry stakeholders, Dominic researches, writes and speaks about cybersecurity, business impact and regulatory policy while promoting cross sector training, exercises and information sharing and collaboration. Dominic is an Illinois attorney whose almost 30- year career includes a variety of roles that focus on the intersection of technology, security, law and business.**"The emerging role of the Illinois Commerce Commission in working with utilities to address cyber threats"**The ICC is one of 50 Public Utility Commissions (PUC) across the country responsible for ensuring cost effective, safe and reliable delivery of utility services by regulated entities. With escalating threats of cyber intrusion and disruption, PUCs across the country are actively determining the best approach toward assessing how utilities are optimally securing their operations. This presentation will cover what Illinois and several other state PUCs are doing and considering moving forward. |

|  |
| --- |
| **Joe Polen, Executive Director, Security Controls and Engagement Management, MISO**In this new role as of May 13th, Joe will champion the administration of MISO’s control framework. He will work closely with IT and service line leadership to identify risks to the business and drive process solutions for effective risk identification and management. Joe will be responsible for establishing a governance framework to achieve continuous security and capability maturity improvement and engage with internal and external stakeholders.Joe’s nearly 25 years serving in high-level IT and security roles in the energy sector will certainly bolster MISO’s strategic vision and support our goal to be a leader in our industry. He joins us from Avangrid (formerly Iberdrola Renewables) in Portland, Oregon, where he had over 20 years of experience in challenging IT and security roles, most recently serving as the Director of Security & NERC Compliance. He oversaw the strategic development, operations and management of corporate physical, information, personnel and cybersecurity policy, as well as business continuity initiatives. He was responsible for NERC compliance and chaired the internal stakeholder workgroups assigned with NERC-CIP regulatory compliance.Joe has an Associate of Arts in electrical engineering from I.T.T. Technical Institute, a Bachelor of Science in business management from Concordia University, a Masters of Business Administration from George Fox University. He received an Executive Global Leadership Certificate from the IMD Business School in Switzerland. He holds several certifications, including the Certified Information Systems Security Professional (CISSP)-(ISC)2 and the Certified Compliance and Ethics Professional (CCEP).**“Exploring an RTO’s Approach to Cybersecurity”**MISO is a not-for-profit member-based organization that ensures reliable, least-cost delivery of electricity across all or parts of 15 U.S. states and one Canadian province. In cooperation with stakeholders, MISO manages approximately 65,000 miles of high-voltage transmission and 200,000 megawatts of power-generating resources across its footprint.The Security team will continually mature our capabilities to integrate security processes across MISO’s Service Lines and implement risk-based controls to ensure sustained reliable operations. These efforts will prepare MISO for the future and establish MISO as a Security Center of Excellence for our members.Joe will discuss MISO’s Security organization, including our programs on cyber security, threat intelligence and hunting, physical security, and information protection. |
| **Tim Yardley, Principal Research Scientist and Associate Director, Information Trust Institute, University of Illinois | CREDC****RADICS DEMO**A substantial and prolonged disruption of electric power would have profound economic and human costs for the United States. From a defense perspective, a major power outage could hamper military mobilization and logistics and impair the capability to project force. The goal of the **Rapid Attack Detection, Isolation and Characterization Systems (RADICS)** program is to enable black start recovery of the power grid amidst a cyber-attack on the U.S. energy sector’s critical infrastructure. RADICS research is developing technology that cybersecurity personnel, power engineers, and first responders can utilize to accelerate restoration of cyber-impacted electrical systems. |

|  |
| --- |
| **Consultant Panel:****Moderator: Dominic Saebeler, Director of Cybersecurity and Risk Management, Illinois Commerce Commission:** Utilities are relying on both internal resources and third party advisors, auditors and vendors to counsel, assist and provide critical feedback toward attaining a secure environment. A panel of consultants who work with utilities will share a peek behind the curtain and some selective insight on various approaches being taken within the industry. Please see our panelists bios below: * **James Sample, Principal, Americas Advisory Services, Ernst & Young:**

Jamey is the *America’s Energy Sector Cybersecurity Leader* with over 20 years of experience in establishing and operating enterprise security risk management programs. Most recently, Jamey served as the Chief Information Security Officer (CISO) at Pacific Gas & Electric (PG&E). He was accountable for the governance, oversight, and support of PG&E's enterprise security and critical infrastructure protection program. He was responsible for overall achievement and compliance with regulatory requirements and identifying, assessing, and prioritizing cybersecurity risk.* **Bradley Singletary, Senior Manager, Deloitte & Touche:**

Bradley Singletary is a Senior Manager within Deloitte & Touche LLP’s Power and Utilities cyber risk practice who helps utilities prepare and defend their physical processes and operations against cyber threats.  Brad actively leads critical infrastructure protection programs for utilities and has ICS/OT experience spanning electric, nuclear, gas and telecom sectors.   Brad has over 17 years in the workforce with 12 deployed with utilities cybersecurity projects. Brad holds a masters in AI and Computer Science from Georgia Tech.  * **Scott Crider, Manager, West Monroe Partners, LLC:**

Scott is a program manager and operational excellence leader with more than 12 years of experience in the field as a cybersecurity practitioner that evaluates critical infrastructure and business development needs, and who demonstrates secure and safe principles and techniques within the Oil & Gas, Nuclear, Bulk Power, Water, and Hygiene, Transportation, Clinical Information Systems, and Pharmaceutical/ Biotechnical industries. He currently serves as Manager in West Monroe Partner’s Cybersecurity practice with a focused understanding of strategic cybersecurity, cyber resilience, and critical infrastructure. |

|  |
| --- |
| **Dmitry Ischenko, Lead Principal Scientist, ABB, Inc.:**Dmitry Ishchenko is a Lead Principal Scientist at ABB US Corporate Research Center in Raleigh, NC, where he currently provides technical leadership and supports strategic corporate technology development in the areas related to cyber-physical security for power grids, microgrid control and protection, renewable integration and utility communications. Dr. Ishchenko is an active member of several IEC and IEEE Working Groups on DER integration and interoperability, and microgrid control functions, has published more than 20 technical papers and holds three patents. Additionally, he has extensive utility, new product development and application engineering experience in power systems.**Al Valdes, Principal research Scientist, Information Trust institute | CREDC:**Alfonso Valdes is a Principal Research Scientist with the Information Trust Institute at the University of Illinois, responsible for a portfolio of diverse research activities, including the Cyber Resilient Energy Delivery Consortium (CREDC); and previously the Trustworthy Cyber Infrastructure for the Power Grid project (TCIPG), and the Illinois Center for a Smarter Electric Grid (ICSEG).Mr. Valdes is the Illinois lead on industry-academic partnerships studying secure inter-operability of electric microgrid assets as well as high-voltage direct current (HVDC) interconnects, and successfully led a previous partnership developing security solutions in time-critical distributed substation protection systems. His research interest focuses on security and resiliency of infrastructure systems, particularly innovative techniques for intrusion detection, as well as security implications of renewable energy integration and smart grid mechanisms. Mr. Valdes regularly participates in infrastructure security roadmapping efforts at the invitation of the Department of Energy (DOE), the Department of Homeland Security (DHS), and the National Institute of Standards and Technology (NIST).Mr. Valdes is active in international collaborations, with KTH (Swedish Royal Institute of Technology) through the University of Illinois INSPIRE program, NWO (Netherlands equivalent of the NSF), and the European Union (as external advisor to the SUCCESS and previously CRISALIS project securing critical infrastructures).Mr. Valdes was formerly a Senior Computer Scientist in the Computer Sciences Laboratory at SRI International, leading several projects in information security for clients such as the Defense Advanced Research Projects Agency (DARPA) and the Advanced Research and Development Activity (ARDA), the Department of Homeland Security, and the Department of Energy. His later research at SRI focused on security of critical infrastructure systems in the Oil and Gas and Electric Sectors He is co-inventor on two patents in cyber-security.Mr. Valdes holds an AB (Mathematics) from the University of California, Berkeley and a MS (Operations Research) from Stanford University.**“Use Cases in Secure Microgrid Interoperability”**Microgrids are emerging as an important element in modern power systems, to maintain resiliency, integrate distributed energy resources, and provide services to area power systems. As microgrids evolve from single systems to microgrid ecosystems, we observe a convergence of microgrid control and communication assets with the Industrial IOT. The presentation will cover advanced detection and control strategies in microgrid ecosystems, including cyber event detection, stability control, and distributed state estimation. We will discuss characteristics of modern microgrid controllers and protection equipment, secure communication within and between microgrids, for example, to maintain power delivery to critical loads. |

Wednesday, June 26th | Q Center, Theater (Main Room) & Ballroom

|  |
| --- |
| **Carol Hawk, PhD., Acting Deputy Assistant Secretary, Cybersecurity for Energy Delivery Systems (CEDS) Cybersecurity, Energy Security, and Emergency Response (CESER) U.S. Department of Energy****CEDS Program Update**The DOE Cybersecurity for Energy Delivery Systems (CEDS) program is working in partnership with the energy sector to advance the vision of resilient energy delivery systems that are designed, installed, operated and maintained to survive a cyber-incident while sustaining critical functions. This presentation will describe the CEDS program, initiatives, approach and opportunities. |
| **Jonathon White, Phd, Manager, Cyber-Physical Systems Security Group, NREL**Jonathan White, Ph.D., is the manager for the Cyber-Physical Systems Security Group within the Energy Security and Resilience Center at the National Renewable Energy Laboratory, which focuses on the identification and mitigation of cyber and physical threats to today’s power grid while providing pathways to a more intrinsically secure and resilient future grid. White leads a team of 15 researchers and analysts who specialize in cybersecurity vulnerability analysis, encryption technologies for distributed energy resources, and advanced modeling and visualization tools to evaluate the security of power-communications networks.Prior to joining NREL, White spent over a decade performing research in wind turbine physical damage monitoring and wind plant control systems at Sandia National Laboratories. He was the chief engineer for the Department of Energy’s first research multi-turbine, wind plant, the Scaled Wind Farm Technology Facility (SWiFT), where he oversaw numerous teams performing wind blade validation, data analysis, wind plant control, and wind plant reliability. During this time, White led a joint Sandia-NREL multi-million dollar effort to forensically identify natural and cyber-physical vulnerabilities after a wind turbine catastrophically failed at the facility. The effort led to the most extensive cyber-physical assessment and consequence-driven mitigations study to date by the U.S. Department of Energy’s Wind Energy Technologies Office on wind energy systems.White earned his doctorate and master’s degrees in mechanical engineering from Purdue University, and he earned his bachelor’s degree in mechanical engineering from The Ohio State University.**“Visualization and Analysis of Grid-Cyber Systems Security”**Increasing penetration of renewable energy, energy storage, controllable loads and electrified transportation on the electric grid are causing a generational change in how the grid is designed and operated. Electric inverters, critical to enabling this transformation, utilize a level of communication and control not previously required. While enabling grid control through communications, these changes are exponentially increasing the cyber vulnerability surface. NREL’s Cyber-Physical Systems Security Group is developing environments that combine emulated communication and power systems with real-physical grid devices to construct virtual grids, utilities, cites or regions to study threats, vulnerabilities, mitigations, analyses and visualizations. An overview will be provided of how this environment, NREL’s Energy Systems Integration Facility and Flatirons Campus are being interconnectedto develop these environments to support future grid cybersecurity research and development efforts. |

|  |
| --- |
| **Dr. Roger Alexander, Lead research Engineer, Schweitzer Engineering Laboratories, Inc.****“TBA”** |
| **Matt Wakefield, Director-Information, Communication & Cyber Security, Electric Power Research Institute (EPRI)**Matt Wakefield is the Director of Information, Communication and Cyber Security (ICCS) at the Electric Power Research Institute (EPRI). The research focus is on enabling advanced applications and data analytics through standards, communication technology, integration architectures and addressing cyber threats to an interconnected system as well as practical demonstrations to enable a modernized grid. He is the facilitator for the EPRI ICCS Executive Committee – to gain insights and strategic input from CIO’s and senior leaders in the IT and Security domains of the electric power industry.Wakefield started his career in 1986 in the United States Navy serving as a Nuclear Power Plant Reactor Operator and Engineering Supervisor in the Submarine Fleet and specializing in reactor operations and electronic instrumentation and controls. He received his Bachelor of Science degree in technology management from the University of Maryland University College.**"OT Security Solutions for the Grid – the EPRI Challenge"**The Electric Power Research Institute (EPRI) coordinated to share OT Security gaps identified by the electric industry with CREDC members as a “Challenge” and request to have CREDC university members propose potential projects to bridge those gaps. This session will present the outcome of those results. |
| **Jana Sebestik, Assistant Director of STEM Curriculum Design, University of Illinois | CREDC**Jana Sebestik is the Assistant Director of STEM Curriculum Design in the Office for Mathematics, Science and Technology Education (MSTE) at the University of Illinois. Before coming to MSTE, Sebestik spent 34 years as a public school classroom teacher and community college mathematics teacher. She currently coordinates education and outreach for the NSF funded GIC Hazard Prediction: From the Solar Wind to Power Systems Impacts Project and the DOE/DHS funded Cyber Resilient Energy Delivery Consortium (CREDC). She helps engineers and research scientists connect their work to educators, consumers, and students. She is the author of curriculum modules in computer science, mathematics, and science including, *The Power of the Wind*, and *Discovering Computer Science & Programming through Scratch* Levels One, Two, and Three. She has presented at national meetings of the National Science Teachers Association (NSTA), the International Society for Technology in Education (ISTE), and the American Society for Engineering Education (ASEE) K-12 Workshops.**The K-12 Connection**Acceptance and support for new technologies and new ideas requires communication and education. When we connect with K-12 teachers and students, we inform and encourage a potential future workforce We also reach families. In this session we will engage in an activity that uses a solar path light to create interest and increase understanding of power grid resiliency. |

Thursday, June 27th | Q Center, Theater (Main Room) & Ballroom

|  |
| --- |
| **Randy Sandone, Executive Director, Critical Infrastructure Resilience Institute (CIRI)** **TBD** |
| **Steve McElwee, Chief Information Security Officer (CISO), PJM Interconnection**Steven McElwee is the Chief Information Security Officer at PJM Interconnection, which ensures the reliability of the high-voltage electric power system serving 65 million people in 13 states and the District of Columbia. He oversees the security risk management program at PJM, including threat and vulnerability management, supply chain cybersecurity, information protection, security monitoring and incident response, as well as IT compliance. He is engaged in a variety of industry, government, and academic collaborative partnerships.He holds a BA in Computer Science from Thomas Edison State College, an MBA from Alvernia University, an MS in Computer Information Systems from Boston University, and a PhD in Information Assurance from Nova Southeastern University. He has published papers on simulated spear phishing education as well as machine learning approaches for intrusion detection. He maintains the CISSP certification and is a member of the IEEE.**“A Strategic Framework for Cyber Resilience"**Electric utilities interact in a complex system of interdependencies. Regional Transmission Organizations (RTOs) help electric utilities pool their transmission capabilities and resources to balance reliability and economics.With the emergence of high-consequence risks to the electric grid, reliability is no longer a sufficient measure of effectiveness. Resilience, the ability to withstand or quickly recover from events that pose operational risks, is becoming increasingly important and affects operations, markets, planning, and security. This presentationintroduces PJM’s approach to resilience, with a focus on the cyber threats to resilience and a strategic framework for addressing them. It presents five high-priority objectives for cybersecurity management. |
| **Amin Hassanzadeh, Cyber Security R & D Principal, Accenture Labs**Dr. Amin Hassanzadeh is a Research Principal at Accenture Cyber Lab, working on cybersecurity research projects in the area of secure Industrial Internet, Trustworthy AI, and Cyber Risk Management. He has earned his PhD in computer engineering from the Department of Computer Science and Engineering at Texas A&M University. His research interests are IoT and Industrial IoT Security, Predictive Analytics in Cyber Security, Privacy Preserving, Wireless Mesh and Sensor Networks, and Intrusion Detection Systems. Dr. Hassanzadeh has designed and developed multiple prototypes on alert correlation in IIoT, proactive risk analysis and remediation, and security event classification. His PhD dissertation was on security function assignment in resource-constrained wireless networks. He has also worked on data correlation methods for intrusion detection systems. |

|  |
| --- |
| **“Proactive Cyber Risk Management in IIoT”**Cyber risk management requires an accurate and holistic identification of the business services, assets and technologies controlling those services and their vulnerabilities, possible impacts on the entire business, and finally remediation options to avoid those impacts. This process is very challenging in industrial environments due to heterogeneous, large scale and geographically dispersed networks and lack of accurate asset inventory and cyber knowledge compare to corporate IT environments. In this research, we will first enumerate the risk management requirements in industrial environments, then propose Agile Security as an approach to tackle the challenges associated with the risk management process. Agile Security methodology and technologies industrialize holistic cyber and business alignment by employing proactive automated cyber risk management. It automatically finds, models, and prioritizes different types of the requirements such as business processes, critical assets, configuration issues, and possible impacts. By simulating virtual adversary attacks, attack paths and cardinal assets, and analyzing impact on business processes, Agile Security analytics engines recommend surgical prioritized actions for gradually reducing business risks and inform external service desk and security operation center on a needed work plan. |
| **Sachin Shetty, Associate Professor, Old Dominion University | CREDC**: see above bio**Bheshaj Krishnappa, Resilience and Risk Program Manager, ReliabilityFirst:**Bheshaj Krishnappa, as a Resilience and Risk Program Manager at ReliabilityFirst, leads all aspects of Cyber/Operational resilience and a strategic, operational and tactical advisor on regional resilience issues. His responsibilities include risk assessment and management of Cyber/Physical security risks to ensure Bulk Power System reliability across the  ReliabilityFirst footprint of 13 U.S. States and Washington D.C.Mr. Krishnappa works with several electric utilities to effectively mitigate risks and advise on best practices. Prior to joining ReliabilityFirst, he has worked for Utility, Software & Services, Manufacturing, Aerospace, Mortgage and Finance companies in consulting and leadership roles. With a vast functional and technical knowledge in Cyber/Physical security, he was instrumental in leading several small to large scale IT and security projects that have enabled businesses to transform and be resilient in delivering their mission.Mr. Krishnappa earned his B.S. in Electrical Engineering from Bangalore University, India and an MBA in Sustainable Business with Renewable Energy concentration from Marylhurst University in Oregon. He actively holds CISSP, CISM, and Carnegie Mellon University’s Executive CISO certifications.**"Cyber Risk Assessment and Cyber Resilience Metrics in Energy Delivery Systems" Presentation & DEMO**Cyber resilience hinges on data driven analytics. Without data driven analytics, the resilience models are not able to characterize the attack surface accurately which leads to incorrect estimation of impact of cyber threat and lack of understanding of resilience of cyber defenses against future threats. In this session, we will present two CREDC projects that involve development of techniques for cyber risk assessment and cyber resilience metrics. In collaboration withAccenture Technology Labs, the CREDC team has developed techniques to conduct prioritized cyber defense remediation plan which is critical for effective risk management in Energy Delivery Systems (EDS). We will present the methodology for identifying the critical attack paths in EDS, balancing the tradeoff between cost and removal of vulnerabilities in critical nodes and evaluating impact on gradual readiness. We will present the results obtained by applying the techniques on a small scale ICS testbed at Accenture. Next, we will present a collaborative effort between CREDC and ReliabilityFirst to develop cyber resilience metrics for bulk power systems. We will present the framework adopted to develop the metrics. Finally, we will provide the demonstration of the work with a cloud-based tool. |

Friday, June 28th | Q Center, Theater (Main Room) & Ballroom

|  |
| --- |
| **Klara Nahrstedt, Professor and CSL Director, University of Illinois | CREDC**Klara Nahrstedt is the Ralph and Catherine Fisher Professor in the Computer Science Department, and Director of Coordinated Science Laboratory in the College of Engineering at the University of Illinois atUrbana-Champaign. Her research interests are directed toward end-to-end Quality of Service (QoS) and resource management in large scale multi-modal distributed systems and networks, and real-time security and privacy in cyber-physical systems. She is the recipient of the IEEE Communication Society Leonard Abraham Award for Research Achievements, University Scholar, Humboldt Award, IEEE Computer Society Technical Achievement Award, ACM SIGMM Technical Achievement Award. Klara Nahrstedt received her Diploma in Mathematics from Humboldt University, Berlin, Germany in 1985. In 1995 she received her PhD from the University of Pennsylvania in the Department of Computer and Information Science. She is ACM Fellow, IEEE Fellow, and Member of the German National Academy of Sciences (Leopoldina Society).**“Anomaly Detection and Causal Reasoning about Attacks on SCADA Networks”**The SCADA (Supervisory Control and Data Acquisition) systems are widely used in critical cyber-physical systems (CPS) such as Smart Grid, Manufacturing and other mission-critical CPS systems. However, SCADA devices and networks are often subject to a wide range of attacks coming from external attackers and/or internal misconfigurations. Traditional intrusion detection systems are deployed to ensure the security of SCADA systems, but they often focus on monitoring only one or two levels of SCADA network data, such as transport or content levels, and continuously generate a large number of alerts without further analyzing them for causal reasoning.In this talk, we present an anomaly detection system, called EDMOND, and a causal reasoning framework for attacks on Smart Grid SCADA networks, called CAPTAR. EDMOND is an edge-based anomaly detector, which analyzes SCADA network anomalies at all three levels of network traffic data (transport, protocol, content levels), aggregates alerts to decrease the volume of alerts, and sends aggregated alerts to control center for causal analysis. CAPTAR is a cloud-based causal reasoning framework which correlates and matches aggregated alerts to causal polytrees. Bayesian inference is performed on the causal polytrees to produce a high-level view of the security state of the protected SCADA network. We will discuss the anomaly detection and causal reasoning analyses on attack examples, and show experimentally that, using MODBUS and DNP3 network traffic, we can doanomaly detection and attack reasoning in real-time. |
| **Michael Keane, Electrical Engineer, Federal Energy Regulatory Commission (FERC)****TBD** |
| **CREC IAB Meeting****CREDC IAB Meeting- PRIVATE- Only open to essential CREDC staff, CREDC IAB members, and DOE/ DHS** |