# Live Wire
## Resilient Control & Instrumentation Systems

THE ANNUAL RECIS NEWSLETTER



### Contacts

Craig Rieger - Lead
208-526-4136
craig.rieger@inl.gov

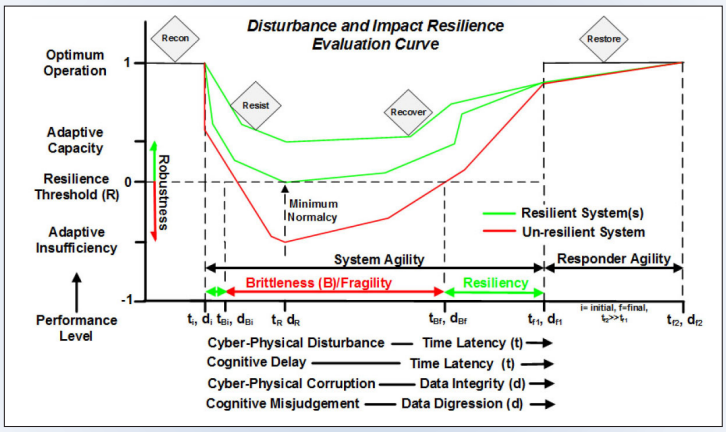
Jodi Grgich - Editor
208-526-9439
jodi.grgich@inl.gov

recis.inl.gov

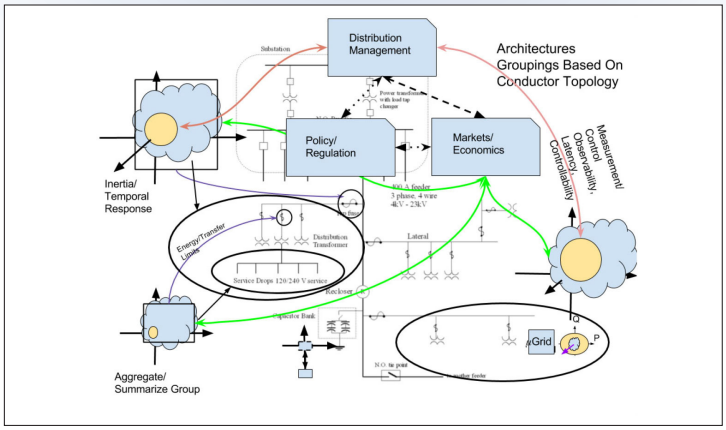

# Resilient Metrics for Control Theory for Electricity Distribution

***By Tim McJunkin***

To understand whether system resilience is improved, one must have the means to measure the resilience. Metrics of resilience relate to the time frame from the initiation of a disturbance. Time frames include short-term resistance to the disturbance, followed by a period of recovery, and finally a restoration time frame. The analysis of the system to prepare for disturbance and understand the expected outcomes, given the magnitude and duration of the event, happens before the event takes place. An electricity distribution system's adaptive capacity for resistance resides in inertia, strength and availability of the upstream wires connecting to a segment of the distribution network. The fast-acting assets in the distribution, such as energy storage and distributed static compensators, provide the recovery response adaptive capacity. The assets must recharge in order for the restoration of the system to be fully optimized. As an example, the HVAC system of a building has some flexibility in its energy usage in adjusting thermostat settings. However, the building will eventually need to enter a recovery phase to bring the building back to a normal set point before it can be asked to provide more support to the electric grid. Specific measurements related to real and reactive power, rolled up through a time-dependent manifold of adaptive capacity, are under development as INL's contribution to the Control Theory Grid Modernization Laboratory Consortium Project.




***Disturbance and Impact Resilience Evaluation curve related the time periods of adaptive capacity utilization.***




***Distribution networks are grouped into economic units that are called upon by market forces or other control mechanisms to stabilize the entire system at the distribution management purview.***

Resilient Control & Instrumentation Systems

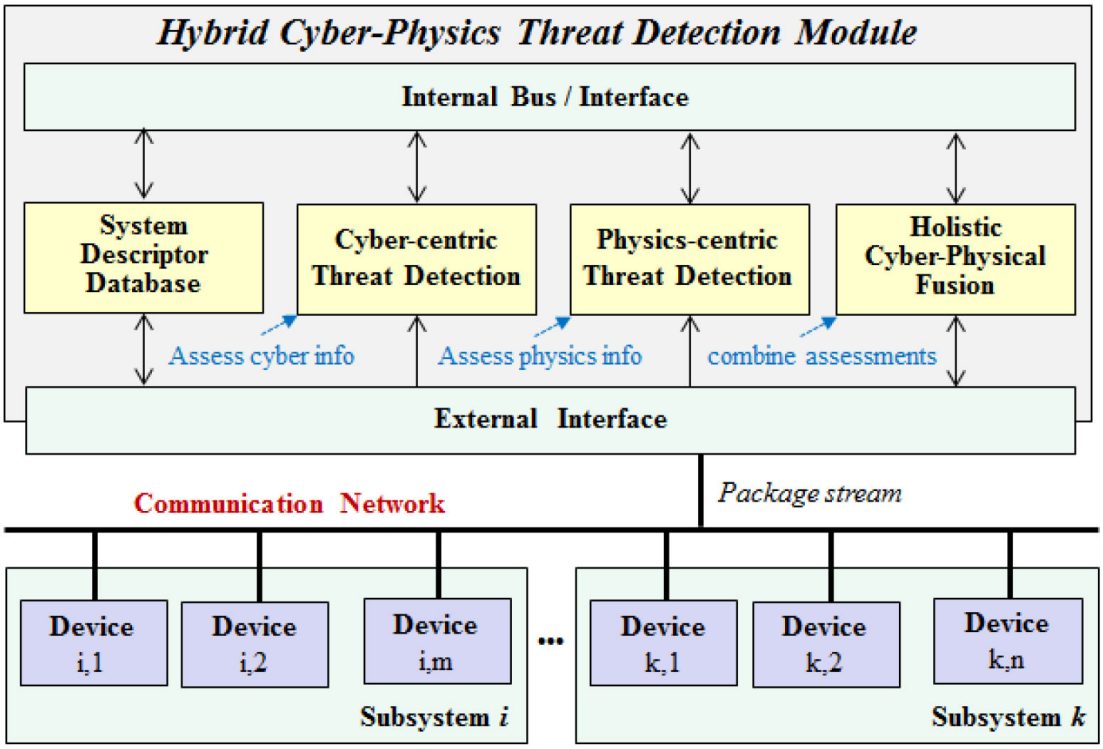
Idaho National Laboratory

## Select Peer-Reviewed Publications

C. Rieger, "Notional Examples and Benchmark Aspects of a Resilient Control System," 3rd International Symposium on Resilient Control Systems, August 2010.

A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart Grid Data Integrity Attacks," IEEE Transactions on Smart Grid, vol.4, no.3, pp.1244-1253, September 2013.

T. Vollmer,M. Manic, "Cyber-Physical System Security With Deceptive Virtual Hosts for Industrial Control Net¬works," IEEE Transactions on Industrial Informatics, vol. 10, no. 2, May 2014.




***Threat detection and diagnosis is accomplished by holistically integrating observations and assessments based on collected cyber and physics behaviors and understanding.***

# Resilient Methods for the Detection and Diagnostics of Cyber-Physical Attacks

***By Humberto Garcia***

Critical infrastructure, like the power grid, transportations systems and others, provide important services to modern societies. Infrastructures typically include both cyber and physical components and use industrial control systems (ICS) to manage their processes through the use of monitoring sensors, controllable actuators, and control platforms. Failure of these ICS can lead to catastrophic impacts to property, public health and safety, and the environment. ICS have been proven to be susceptible to cyber and physical attacks, with numerous reported events demonstrating their vulnerability to intrusion and interference. In order to defend against threats, ICS are typically equipped with diverse cybersecurity elements including threat intrusion detection systems (IDS). These IDS typically monitor network traffic, implementing mechanisms to regulate and assure authentication, access control and message integrity. IDS emphasize the collection of cyber-related attributes, ICS rarely incorporate security rules to evaluate whether the data or commands exchanged violate physics-based semantics, or exploit the compatibility of the measurements and control commands with the underlying physical processes. Consequently, cybersecurity measures based on cyber-centric information and rules are largely ineffective against evolving attack vectors such as advanced persistent threats. A holistic approach is necessary to protect CPS where cyber-centric mechanisms are complemented with physics-centric methods. In support of the Threat Detection Grid Modernization Laboratory Consortium Project, hybrid technologies are under development for hardware-in-the-loop demonstration at INL. This program extracts information from network package streams and analyze them with both cyber- and physics-based methods for the detection and diagnosis of threats to CPS environment to provide resilient cyber-physical security.

## Select Peer-Reviewed Publications

W. Lin; K. Villez; H. Garcia, "Experimental Validation of a Resilient Monitoring and Control System," Journal of Process Control, vol. 24, no. 5, pp. 621–639, May 2014.

D. Vollmer, M. Manic, "Autonomic Intel-ligent Cyber Sensor to Support Industrial Control Network Awareness," IEEE Trans-actions on Industrial Informatics, Vol. 10, No. 2, May 2014.

C. Rieger, "Resilient Control Systems Practical Metrics Basis for Defining Mission Impact," Resilience Week, August 2014.

# Cyber Anomaly Detection

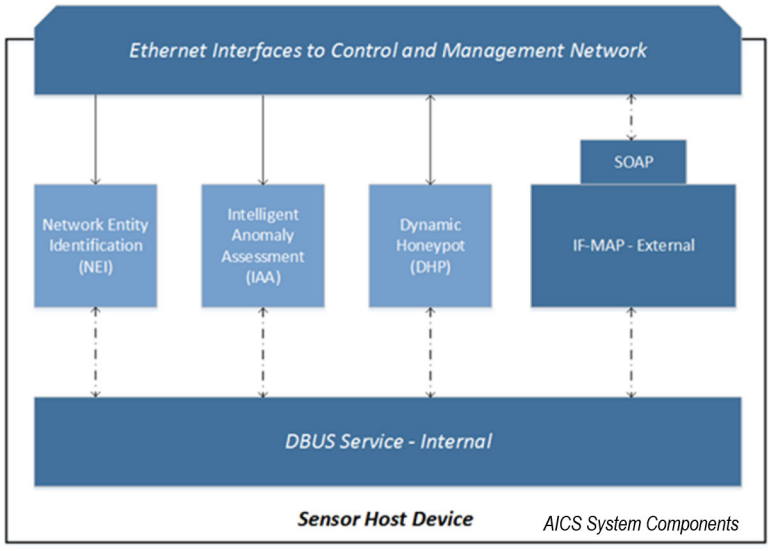
***By Tim Klett***

The detection of intrusion and attacks on computer networks is a vital aspect of sound cybersecurity practices. This identification of anomalous behavior cannot be limited to traditional intrusion detection techniques that rely on signature-based profiles of pre-defined models, as attacks that do not rely on known vectors will go undetected. Adaptive models for anomaly detection fill that gap by learning a model of what the normal behavior of a system is, and flag any activity that AICS System Components deviates from that norm as

potentially malicious. One such adaptive model that employs machine learning techniques to model network behavior, and identifies anomalous activity is the Autonomic Intelligent Cyber Sensor (AICS). AICS was developed at Idaho National Laboratory (INL), and is focused on providing a real-time cyber sensor for the industrial control system (ICS) networks that are at the heart of many critical infrastructure operations.

AICS employs three major analysis components, plus standards-based communication channels to monitor and protect ICS networks: Network Identity Identification (NEI): The NEI performs asset discovery by passively monitoring the ICS network traffic. For each host discovered on the network, the NEI catalogs its IP and MAC addresses, and attempts to identify its operating system. The NEI continually updates this network model to reflect the present composition of hosts on the network, thereby providing network state awareness.

- Dynamic Honeypot (DHP): The DHP utilizes the NEI's constantly evolving network model to automatically configure and deploy deceptive virtual network hosts, otherwise known as honeypots, which imitate the real hosts on the network. These honeypots serve to draw the focus of malicious intent, and thereby provide a decoy attack surface that is easily monitored for anomalous activity.
- Intelligent Anomaly Assessment (IAA): The IAA selectively monitors a prescribed list of host network traffic for anomalous activity, while adjusting its own sensitivity based on observed global network trends. Statistical features are extracted from the traffic of each network host into feature vectors. A fuzzy logic- based anomaly detection algorithm is then used to compute an anomaly score for each vector that ex-presses the belief that the current window of packets contains anomalies. The anomaly score is compared against the dynamic sensitivity threshold to determine whether to raise an alert.
- Communications: AICS captures control traffic by listening on the ICS network switch's SPAN ports. Network host and alert information is delivered externally over the open-standard IF-MAP protocol and syslog. IF-MAP anomaly alerts are raised through a publish/subscribe style messaging system, enabling network stakeholders to selectively receive only those types of alerts which interest them. The AICS communications approach supports flexible deployment options, including the ability to deploy multiple sensors with potentially overlapping host monitoring duties.



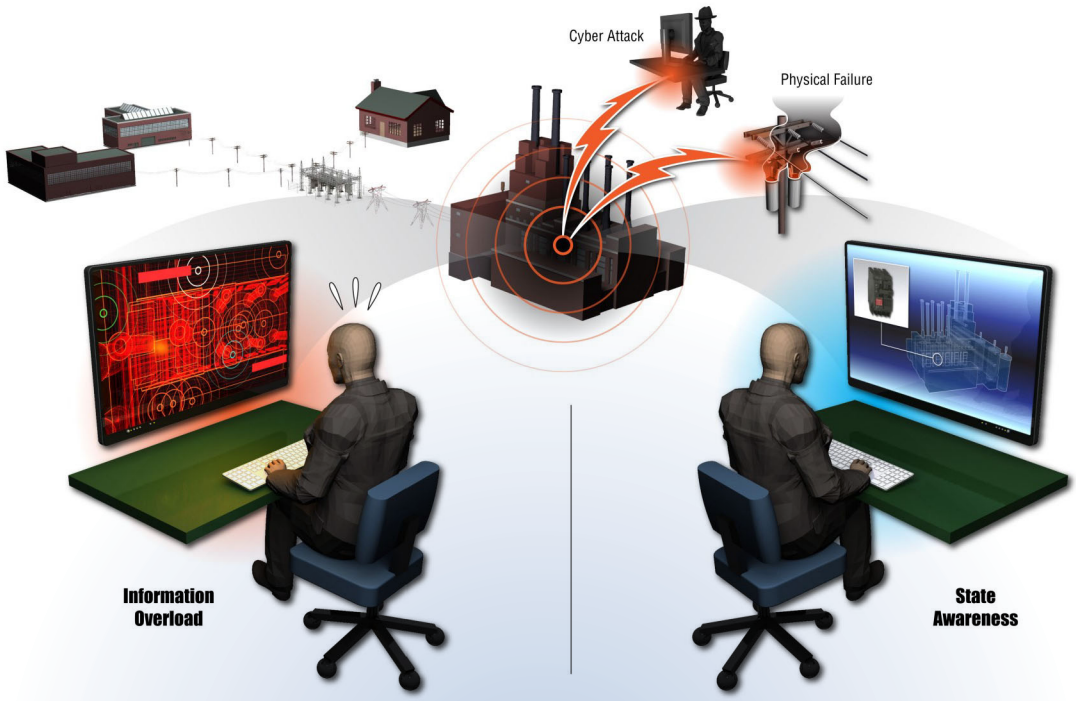

***Sensor Host Device – AICS System Components***

## Select Peer-Reviewed Publications

D. Wijayasekara, O. Linda, M. Manic, C. Rieger, "FN-DFE: Fuzzy-Neural Data Fu¬sion Engine for Enhanced Resilient State-Awareness of Hybrid Energy Systems," Special Issue on Resilient Architectures and Systems, IEEE Transactions on Cybernetics, vol.44, no.11, pp.2065-2075, November 2014.

H. E. Garcia, W.-C. Lin, S. M. Meerkov, and M. T. Ravichandran, "Resilient Monitoring Systems: Architecture, Design, and Application to Boiler/Turbine Plant," IEEE Transactions on Cybernetics, Vol. 44, No. 11, November 2014.

K. Eshghi, B. Johnson, C. Rieger, "Power System Protection and Resilient Metrics," Resilience Week, August 2015.




# Humans are still essential for ensuring cybersecurity in critical infrastructure

***By Katya Le Blanc***

Cybersecurity is emerging as one of the great challenges in ensuring the reliability of critical infrastructure. Data breeches and compromises have affected everything, from the financial industry to the electric grid. To date, the majority of research and development to ensure protection of cyber assets in critical infrastructure have focused on automated technological tools, such as intrusion detection systems, anomaly detection systems and intrusion prevention systems. These tools, while necessary, are not currently sufficient to meet the ever-changing landscape of cyber threats. Even with recent advances in artificial intelligence and machine learning techniques, humans are still the most capable of adapting to the dynamic threat that a cyber adversary poses. One persistent challenge is ensuring that the appropriate information related to cybersecurity be presented to the right human at the right time, and in a way that that human can understand to make timely and effective decisions. Idaho National Laboratory (INL), in partnership with several organizations, is investigating how to facilitate human decision making in the face of cyber threats. These projects are focusing on assessing existing risk analysis techniques for their applicability to cyber security in commercial nuclear power plants and how to present cyber security information to electric grid operators.

## Select Peer-Reviewed Publications

T. McJunkin, C. Rieger, A. Rege, S. Biswas, M. Haney, M. Santora, B. Johnson, R. Boring, S. Naidu, J. Gardner, "Multidisciplinary Game Based Approach for Generating Student Enthusiasm in Addressing Critical Infrastructure Challenges," ASEE's 123rd Annual Conference & Exposition, June 26-29, 2016.

P. Penkey, M. Alla, B. Johnson, and T. McJunkin, "Improving transmission system resilience using an automation controller and Distributed Resources," in 2016 Resilience Week (RWS), Aug. 2016, pp. 89–94.

M. Manic, K. Amarasinghe, J. Rodriguez-Andina, C. Rieger, "Intelligent Buildings of the Future: Cyberaware, Deep Learning Powered, and Human Interacting," IEEE Industrial Electronics Magazine Vol. 10(4):32-49, December 2016.

# Real-time Resilience Framework and Quantification

***By Manish Mohanpurkar, Sayonsom Chanda, Rob Hovsapian; Edited by Craig Rieger***

For a modern society, the reliability of the power grid has become a dependency and an expectation for our way of life. Electric grids have gone through a multi-dimensional transformation over the last few decades including deregulation and high levels of digitization. Electric grids are currently subjected to extreme stress and black-outs, with concerns for cyber and physical attacks also growing, lending to concerns from utilities to maintain reliable supply. With growing use of digital controls and communication networks that help manage the grid, utilities are interested in understanding the threat landscape and potential impacts on grids. Ultimately, grid resilience to these threats is a new research paradigm that must be considered.

Device and system failures in any intercon-nected system such as the power grid may be attributed to either unintentional causes or malicious attacks. Unintentional causes which include improper operating conditions, extreme weather events, inaccurate commands, etc., may lead to the failure of devices and systems and leading to a power outage. Malicious causes such as cyber-physical attacks are intended to disable ser-vices and interrupt the supply of electricity.

Potential impacts (from attack) on power grids with a real-time resilience assessment framework have been assessed. Early identification of threats and attacks enables the proposed monitoring system to implement resilient responses to minimize vulnerabilities.

Using real-time telemetry data gathered, the proposed monitoring system also quantifies resilience of the power system, aids in visualization of system vulnerabilities and suggests actions. Our approach is generic, integrable, and scalable, i.e., it can be used for quantifying resilience of buildings, microgrids, and large power grids.

A formal approach has been developed to evaluate the operational resiliency of power distribution systems (PDS), and quantify the resiliency of a system using a code-based metric as shown in Figure 1. A combination of steady state and dynamic simulation tools is used to determine the resiliency metric. Dynamic simulation tools help with analyzing impact of short-term events, which might affect operational resiliency in long term. The proposed theoretical approach is validated using a simple power distribution system model and simulation results demonstrate the ability to quantify the resiliency using the proposed code-based metric. The time dependent quantification of resiliency has been demonstrated on a system of two connected CERTS microgrids (a widely accepted microgrid configuration) as shown in Figure 2.

The present metrics formulation quantifies the ability of the system to supply critical loads with reduced resources. Though the metrics have been developed for a PDS, the metrics can be generalized. This metrics can be used to quantify the level of resilience with which the consumers are served. Based on resilience values under several operating and planning scenarios, cost-benefit analysis of distribution system investments can be justified. Thus, the developed approach for resilience measurement is quite versatile in providing useful information to manage networks at a higher quality of service.

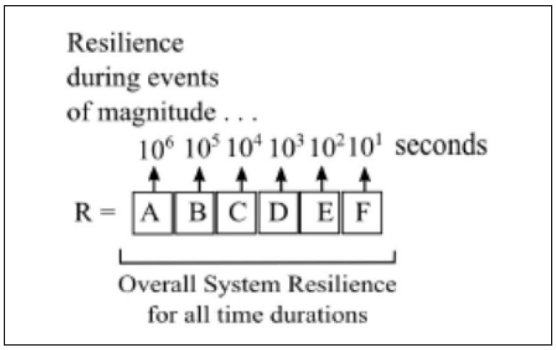



***Figure 1: Resilience Metric Code based on time***

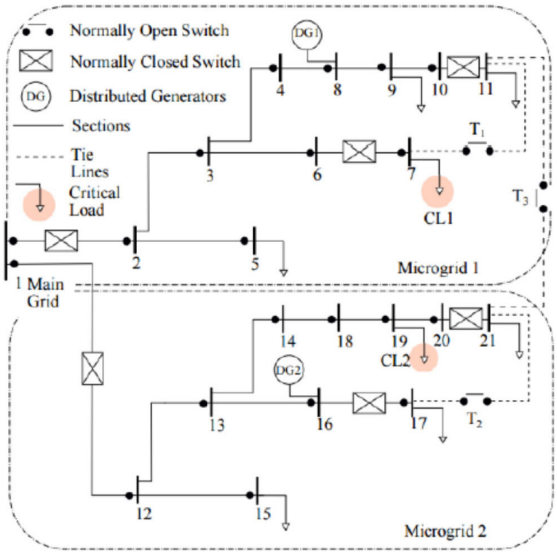



***Figure 2: Resilience assessment of CERTS microgrid as an example***

## Select Peer-Reviewed Publications

T. McJunkin, and C. Rieger, "Electricity Distribution System Resilient Control Metrics," in 2017 Resilience Week (RWS), Sep. 2017, pp. 103-112.

# Resilience Week 2017

***By Craig Rieger and Cherrie Black***

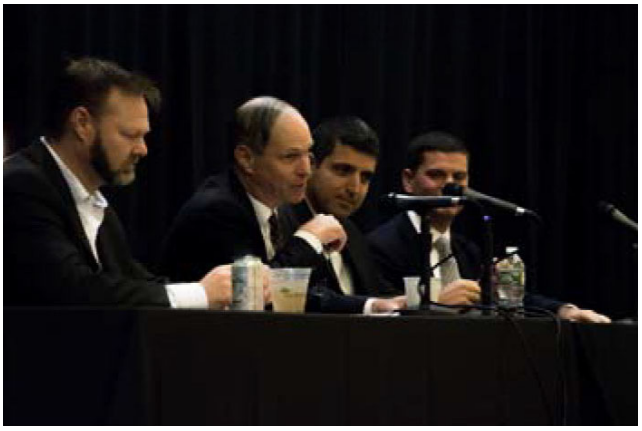
This year marked the 10th anniversary of Resilience Week, which was held in Wilmington, DE, from Sept. 18 - Sept. 22, at the Chase Center on the Riverfront. Since its inception, Resilience Week has grown to include five multidisciplinary symposia on resilient control, cyber, cognitive and communications systems in addition to a more government-industry focused resilient critical infrastructure (RCI) symposium. Peer-reviewed papers were solicited in all symposia areas, including critical infrastructure (CI), with final publication of accepted papers in the Institute of Electrical and Electronics Engineers (IEEE) Xplore. Three well-known plenary speakers and a plenary panel warmed attendees with presentations on state-level energy resilience initiatives, power system resilient design challenges, industry practice and government policy to achieve a more resilient infrastructure.

The exemplary plenary speakers and panel included:

- Richard Mroz, President, NJ Board of Public Utilities and Chair of the Critical Infrastructure Committee for the National Association of Regulatory Utility Commissioners (NARUC)
- John McDonald, Director, Technical Strategy and Policy Development for GE Energy's Digital Energy and Hon-orary Chair
- Patricia Hoffman, Principal Deputy Assistant Secretary, Department of Energy, Office of Electricity Delivery and Energy Reliability (DOE-OE)
- Paul Stockton, Sonecon, Moderator, and Panelists: Jonathon Monken, PJM Interconnection; Mikhail Falkovich, Con Edison; Jamey Sample, Ernst & Young LLP

This year added a special industry-organized session on Monday, which provided a cross-cutting perspective on cyber resilience, including policy, design and future threats. As with last year, the research and development symposia also included two special series of invited paper and keynote speakers, and topically covered resilience models and measures, and mixed human-automation resilience. These two series were started a few years ago to develop greater interdisciplinary interaction, and proved to nicely meet expectations. The former track includes and will maintain collaboration through the Industrial Electronics Society (IES) Resilience and Security for Industrial Applications (ReSia) technical committee in focusing on terminology, metrics and a use case for future events with the intent to develop an eventual IEEE standard. In addition, a social resilience track was added to consider the broader impacts of technology in the realm of community resilience.

The critical infrastructure track opened with a keynote address by Professor Stephen Flynn, who examined five critical resilience barriers and discussed the need to advance CI resilience by leveraging knowledge acquired through disasters. As in past years, the RCI track featured multiple lightning talk sessions and for the second year, a student competition comprising a lightning talk and poster session. Panels focused on: the Regional Resilience Assessment Program, with an introduction by Director Scott Breor; an owner-operator forum on lifeline resilience; and a panel of practitioners with expertise in visualizing data, communicating information, and promoting insight in CI resilience. Finally, the session closed with a keynote from Professor Tom Seager, ASU, on "Resilience Lessons from the Oroville Dam: Dynamic Robustness and Graceful Extensibility."



***From right to left: Jonathon Monken, PJM Interconnection; Mikhail Falkovich, Con Edison; Paul Stockton, Sonecon; Jamey Sample, Ernst & Young LLP***

IEEE Resilience and Security for Industrial Applications (ReSia)

## Save the Date!

***Resilience Week 2018***
***August 20-23, 2018***