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

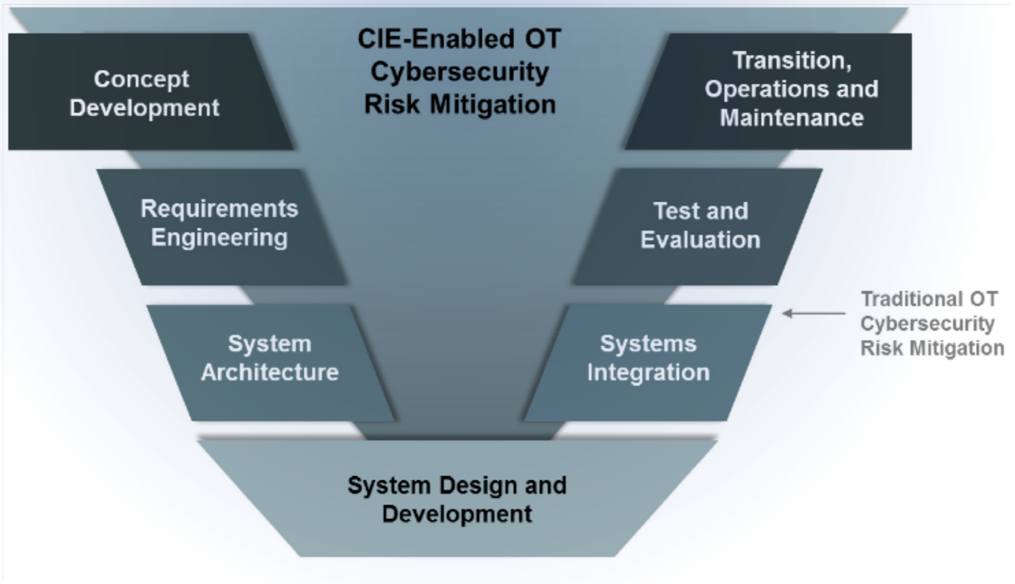
Cyber Informed Engineering

By Virginia L. Wright

Cyberrisk is an emerging factor to be considered in engineering design and risk analysis of operational technology systems. Traditional engineering analysis considers risk applied to functionality, safety and security of operations; however, cyberrisk is typically considered outside of and often after the primary engineering design process. Cyber informed engineering (CIE) is a body of knowledge to characterize and mitigate risks presented by the introduction of digital technology in this formerly analog environment. CIE is focused on the application of traditional engineering techniques informed by an awareness of cyber-security threat and mitigation methods. Managers and engineers can employ this methodology to mitigate cyber-security risk in engineering projects throughout the design and installation life cycle.

CIE identifies 11 key framework elements through which cyber and engineering professionals can engage to identify key cyberrisks early in the design lifecycle:

- Consequence/Impact Analysis - identifying and mitigating potential impact to key process functions
- Systems Architecture – Ensuring information can only flow through the system in desired ways
- Engineered Controls – Engineering decisions to design potential vulnerabilities out of the system
- Design Simplification – Reducing the complexity of the design to the minimum necessary for critical functions
- Resilience Planning – Ensuring that a system can continue operations even when compromised
- Engineering Information Control – Protecting engineering design and operational information from unauthorized access
- Procurement and Contracting – Ensuring that security requirements are understood by vendors, integrators, and third-party contractors
- Interdependencies -- Mitigating cyber risks introduced interdependencies and interconnections with others systems
- Cybersecurity Culture – Institutionalizing cyber-secure practices throughout an organization and its vendors
- Digital Asset Inventory -- Maintaining a complete and accurate inventory of all hardware and software used for engineering functions
- Active Process Defense – Employing dynamic strategies and technical competencies to deter and remove an attacker


CIE-Enabled OT Cybersecurity Risk Mitigation
Concept Development
Transition, Operations and Maintenance
Requirements Engineering
Test and Evaluation
System Architecture
Systems Integration
Traditional OT Cybersecurity Risk Mitigation
System Design and Development

Resilient Control & Instrumentation Systems

INL 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.

Wireless Valve Position Indication Sensor System: Enabling Digital Manual Valve Position Verification

By Vivek Agarwal, John Buttles, and Ahmad Al Rashdan

Most operating nuclear power plants (NPPs) in the United States have received approval to extend their operating licenses to sixty years. The nuclear industry is now preparing to extend operating licenses to eighty years. While NPPs are preparing for extensions (sixty years and beyond), the nuclear industry is facing a unique economic sustainability challenge in the current energy market. This is partly due to the present nuclear work practice's dependence on a high number of skilled laborers, which results in high operation and maintenance (O&M) costs. The O&M costs account for approximately 66 percent of the total operating cost. To address these concerns and abide by the Nuclear Energy Institute's "Delivering the Nuclear Promise" initiative, the U.S. utilities are actively embracing digitalization of their work practice to lower the O&M costs by increasing productivity and efficiency while maintaining a safe and reliable operation.

One of the work practices that is performed by labor in an NPP on a regular basis is manual concurrent or independent verification on manual valve position. At present, it requires two and sometimes three persons to operate and verify manual valve position. There are about 150 to 200 manual valves of different types per reactor plant distributed across the plant site. Manual position verification of manual valves in an NPP adds to the O&M costs, possibility of human error, risk of exposing labor to industrial and radiation hazards, inaccurate assessment of valve health and redundant periodic calibration of valves.

To address these above-mentioned concerns, Idaho National Laboratory (INL) researchers have developed a wireless valve position indication (VPI) sensor system (as shown in Figure 1) that can be retrofitted on three main manual valve types (extendible to other manual valve types) to replace manual valve position verification with digital verification and enable online monitoring of manual valves. The technology has achieved Technology Readiness Level 6 and has been demonstrated at Idaho State University's Energy Systems Technology and Education Center experimental flow-loop (Figure 2).

Some of the major advantages of INL's wireless VPI sensor system (in current state) over competing digital technologies include:

- Easy to install EMI/RFI certified prototype on all manual valve types without any valve body modification thereby no recertification is required
- Provide continuous VPI while commercial technologies provide binary or piecewise linear position
- Support Wi-Fi and IEEE 802.15.4 wireless networks
- Provide time stamp on valve movement and sends alarm if incorrect valve movement is detected.

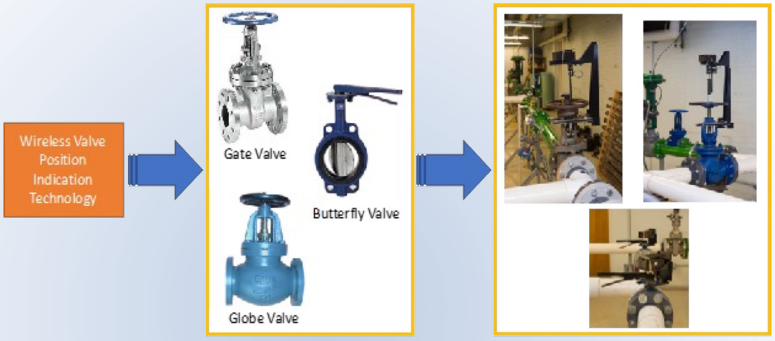


Figure 1. Wireless VPI sensor technology for manual valve types.

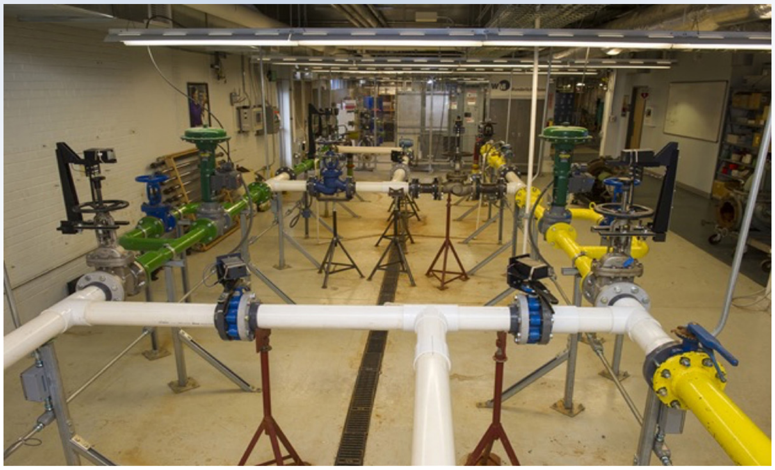


Figure 2: Wireless VPI sensor technology installed at ISU's ESTEC experimental flow-loop.

Consequence-driven Cyber-informed Engineering: Evolving Cybersecurity

By Sarah Freeman and Curtis St Michel

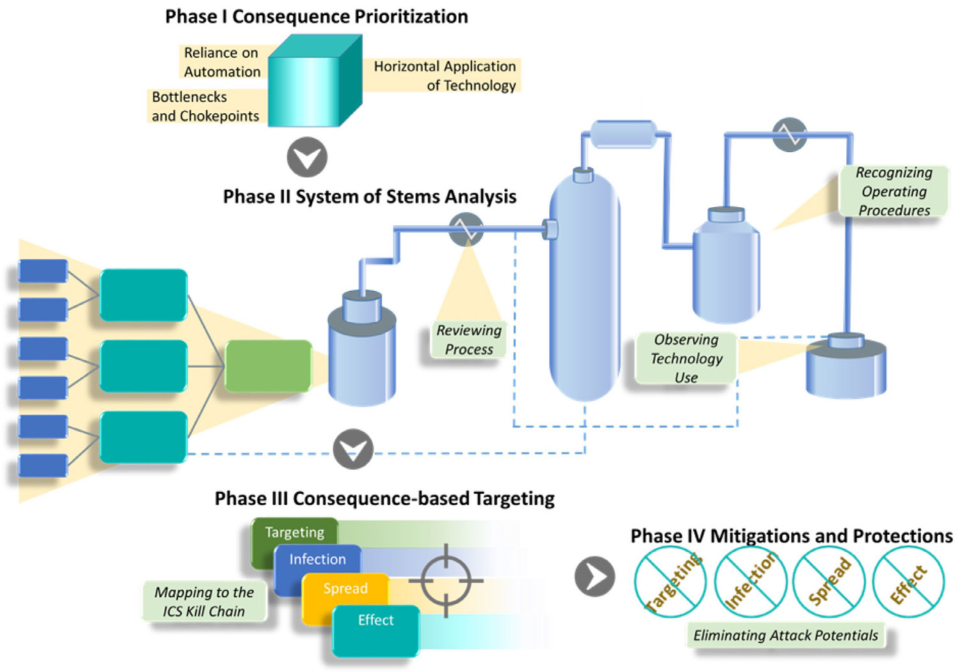
In late March and early April 2018, four U.S. pipeline companies experienced disruptions to their electronic communications systems that supported customer interaction. Three of the companies experienced an outage due to an assessed cyberattack against the third party provider of the system, with the fourth voluntarily disabling their system as a precaution. These events highlight how a shifting landscape of technology adoption and the abstraction of "core" functions to third parties has shifted the attack surface of organizations.

Within this changing landscape, organizations can overlook risk areas when employing traditional cybersecurity approaches. In this case, for example, the targeted system lay outside these organizations' information and operational technology boundaries, and outside of their cyber-focused security efforts, processes, and procedures. Convergence of technology has provided new opportunities for the cyber adversary.

In this reality, Consequence-driven Cyber-informed Engineering (CCE) represents a shift in focus for traditional cybersecurity approaches. Rather than deploy limited resources to address the latest vulnerability or threat actor activity alerts, CCE refocuses these efforts based on the potential impact or consequence of a cyber event. For the most serious outcomes, CCE identifies methods to re-engineer systems, processes, and procedures so that wherever possible, potential cyberattack chains are broken, limiting or eliminating the potential for a devastating cyberattack.

CCE structures analysis around four core areas or phases: 1) Consequence Prioritization, 2) System of Systems Analysis, 3) Consequence-based Targeting, and 4) Mitigations and Protection. Collectively, these phases are designed to teach the controls systems engineer (the local expert on their system), how an adversary will attack. The first phase centers on identifying the most significant functions, services and the critical operations for an organization. The second phase systematically dissects the technology, components, and devices in use, as well as relevant operations, processes, and procedures. In the third phase, comprehensive attack scenarios are described, built on concepts of access, information, and ICS payload requirements. This exercise illuminates specific adversary actions that must be performed in order to achieve success, with complimentary disruptive recommendations designed in the last phase.

CCE is currently conducting a second pilot study to improve the process and training materials, and validate the effectiveness of this industry agnostic approach.


Phase I Consequence Prioritization
Reliance on Automation
Horizontal Application of Technology
Bottlenecks and Chokepoints
Phase II System of Stems Analysis
Recognizing Operating Procedures
Reviewing Process
Observing Technology Use
Phase III Consequence-based Targeting
Targeting
Infection
Spread
Effect
Mapping to the ICS Kill Chain
Phase IV Mitigations and Protections
Targeting
Infection
Spread
Effect
Eliminating Attack Potentials

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.

Evaluations of BR2 Silicon Carbide Temperature Monitors

By K.L Davis, B.J. Heidrich, T.C. Unruh, P. Calderoni, S.V. Dycka, A. Goussarova. I. Uytdenhouwen, K.M. Verner, A. Al. Rashdan, A.A. Lambson

Since the early 1960s, SiC has been used as a post-irradiation temperature monitor. Several researchers have observed that neutron irradiation induced lattice expansion of SiC annealed out when the post-irradiation annealing temperature exceeds the peak irradiation temperature.

Twelve silicon carbide (SiC) temperature monitors were irradiated in the Belgain Reactor 2 (BR2) as part of a Nuclear Science User Facilities (NSUF) Project and were delivered to the High Temperature Test Lab (HTTL) for evaluation to determine their peak temperature achieved during irradiation. The reactor exposure was performed using the Basket for Material Irradiation (BAMI) rig of the BR2, Mol, using standard non-instrumented capsules.

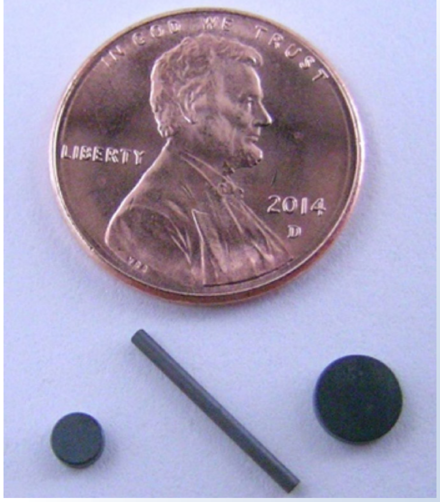


Figure 1. SiC temperature monitors available for use in irradiation testing include small rods and disks.

Temperature monitors were fabricated from material meeting the Rohm Haas specification SC003. This material was produced via chemical vapor deposition (CVD) process with a high purity (99.9995%) and a density close the maxim theoretical. Using this characteristic, the SiC monitors were manufactured to exceed a resistivity > 1000 ohm/m. SiC monitors used in the experiment were manufactured as cylinders with a 1 mm diameter and a 12.5 mm (±5 μm) length (reference Figure 1).

The SiC monitors are evaluated by heating in the annealing furnace using isochronal temperature steps. After each isochronal annealing, the specimens are placed in a resistivity measurement fixture located in the constant temperature chamber (maintained at 40°C) for a minimum of 30 minutes. After the 30 minute wait time, each specimen's resistance is measured.

Table 1 shows the results for the evaluation. The calculated verses measured peak irradiation temperatures had good agreement comparable to published data.

	Dose	Temperature [°C]		%
ID	[dpa]	Calc.	Meas.	Dev
M1-Low-A	0.5	255	240	-6%
M2-Low-A	0.2	255	Indet.	n/a
M1-High-A	0.5	310	320	3%
M2-High-A	0.2	310	330	6%
M1-Med-A	0.5	410	390	-5%
M2-Med-A	0.2	410	380	-8%

Table 1 - Evaluation results for the BR2 monitors.

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.

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.

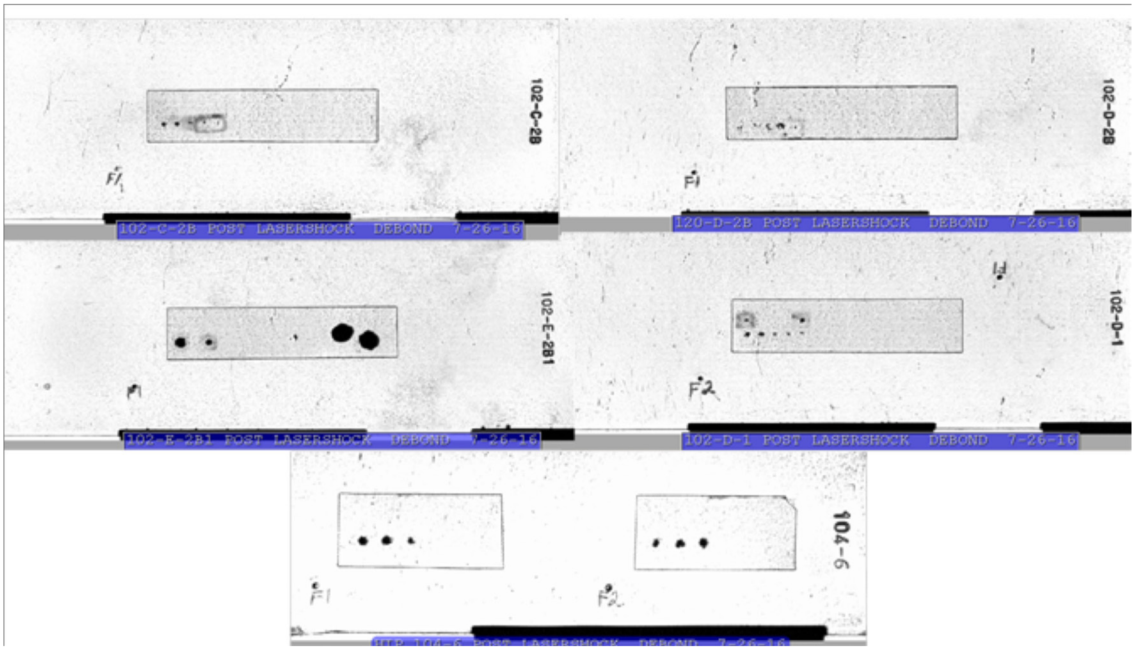

102-C-2B
F1
102-C-2B POST LASERSHOCK DEBOND 7-26-16
102-D-2B
F1
120-D-2B POST LASERSHOCK DEBOND 7-26-16
102-E-2B1
F1
102-E-2B1 POST LASERSHOCK DEBOND 7-26-16
102-D-1
F1
F2
102-D-1 POST LASERSHOCK DEBOND 7-26-16
104-6
F1
F2
HIP 104-6 POST LASERSHOCK DEBOND 7-26-16

FIGURE 1. Ultrasonic C-scan images of the fabricated fuel plates that have been laser shock tested. The dark regions indicate debonds in interfaces that reflect ultrasound and keeps ultrasound from traveling through the fuel plate to the back side. The size of the debond is a relative indication of the bond strength for the different fabrication processes. The backside surface velocity generated by the shockwave is a quantitative measure of bond strength. While the HIP process appears to have healed the coating blisters on foil 2B1, the bond strength is low and the debond areas are large. Note that the exceptionally large debond areas for foil 2B1 corresponds to the blistered side of the foil.

Characterization of Irradiated Fuel Plates

By James Smith

The United States High Performance Research Reactor (USHPRR) Fuel Development (FD) pillar is tasked with the development and qualification of a novel high density U–Mo alloy based fuel which will enable USHPRR conversions to LEU. The notable FD undertakings include the demonstration of novel fuel that passes the operational safety, dimensional stability, thermal stability, and other requirements of the applicable regulatory agency. The main FD Project objective is to advance the technical means necessary to replace HEU fuel with LEU fuel in research and test reactors. To predict the performance of nuclear fuels and materials, irradiated fuel plates must be characterized efficiently and accurately in high rad environments. The characterization must take place remotely work in settings largely inhospitable to modern digital instrumentation. Characterization techniques based on non-contacting laser sensing methods enable remote operation in a robust manner within a hot-cell environment. Laser characterization instrumentation offers high spatial resolution and remain effective for scanning large areas. A Laser Shock system is currently being developed as a Post Irradiation Examination (PIE) technique in the Hot Fuel Examination Facility (HFEF) at Idaho National Laboratory. The laser shock technique will characterize material properties and failure loads/mechanisms in various composite components and materials such as plate fuel and next generation fuel forms in high radiation areas. The laser shock-technique induces large amplitude shock waves to mechanically characterize interfaces such as the fuel-clad bond. As part of the laser shock system, a laser-based ultrasonic C-scan system will be used to detect and characterize debonding caused by the application of the laser shock. The laser shock system has been used to characterize the resulting bond strength within plate fuel which have been fabricated using different fabrication processes. The results of this study will be used to select the fuel fabrication process that provides the strongest interface.

Autonomic Intelligent Cyber Sensor (AICS)

R&D100 Award Winner for 2018, commercialized by Trust Automation

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.

B. Vaagensmith, T. McJunkin, K. Vedros, J. Reeves, J. Wayment, L. Boire, C. Rieger, J. Case"An Integrated Approach to Improving Power Grid Reliability: Merging of Probabilistic Risk Assessment with Resilience Metrics," Resilience Week, August 2018.

K. Savchenko, H. Medema, R. Boring, "Trouble in Paradise: Mutual Awareness, Teamwork, and Hawaii False Ballistic Missile Alert," Resilience Week, August 2018.

IEEE

Resilience and Security for Industrial Applications (ReSia)

Save the Date!

Resilience Week 2019
November 4-7, 2019

Resilience Week 2018

By Craig Rieger

Resilience Week returned to Denver this 11th year and had a full slate of tracks from Monday-Thursday, August 20-23 at the downtown Embassy Suites. The very popular student competition and owner/operator panel returned to the infrastructure track, as well as regional, cross-disciplinary panels and talk providing insights on regional and national resilience. The plenary panel for this year focused on infrastructure interde-pendencies and response challenges from one or more attacks on the intertwined communications, gas and power distribution and water networks. John Garstka, Deputy Director, Cyber, Office of the Under Secretary of Defense, Mark Weather-ford, SVP & Chief Cybersecurity Strategist, vArmour, and Vilas Mujumdar, ASCE Board of Direction and Northeastern Global Research Institute rounded out the plenary speakers. Seventeen full papers were accepted, and numerous posters and abstracts were presented at the event, which includes several networking socials and breaks. In addition to the student competition in the infrastructure track, two gaming competitions developed student interest in cyber security and power systems. New cyber security technology developments from the Department of Homeland Security's Transition to Practice (DHS-TTP) program were presented in a track that is lead off by speakers presenting the national security challenges. Tours of the local National Renewable En-ergy Laboratory (NREL) Energy Systems Integration Facility (ESIF) facility, a user fa-cility that hosts number collaborative experiments in renewable energy, was offered to event participants at the conclusion of the week. About 200 participants and attendees attended this year's event.

From left to right: Adrian Chavez, Sandia National Laboratories; Manimaran Govindarasu, Iowa State University; Alison Gotkin, United Technologies Research Center; Kevin Reifsteck, National Security Council; Doug Maughan, Department of Homeland Security