Live Wire

Resilient Control & Instrumentation Systems

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 Control & Instrumentation Systems

iNL Idaho National Laboratory

Resilience in Renewable Energy Integration

By Jake Gentle, Katya LeBlanc and Tim McJunkin

Connecting social science and STEM to advanced technologies hasn't always been easy, but resilient controls embody various multidisciplinary efforts to bridge the gap. An increased push has been made to gain the acceptance of stakeholders for the incorporation of data enabled by a new advanced technology at the lab. INL researchers have developed a method called Dynamic Line Ratings (DLR), which incorporates real-time weather data with computational fluid dynamics to produce an economically viable estimation of the limiting thermal line ratings on individual spans of transmission lines. The DOE Energy Efficiency and Renewable Energy Wind and Water Technology Program Office (WWTPO) supports the optimal integration of wind energy using existing transmission assets.

DLR joins the plethora of new information feeds into the control centers of electric utilities in current smart grid sensor networks. To obtain stakeholder acceptance and ultimately operator utilization, the information must reach confidence thresholds in fidelity of applied algorithms, security of data communications and the effective integration into operating control center displays. The INL weather-based method establishes the first leg through the use of IEEE accepted standards and on-site validation of wind predictive models. These pilot studies were supported by transmission asset owners, Idaho Power Company and AltaLink, LLC, in Alberta, Canada. Second, in partnership with the stakeholders, baseline security support encouraging integrity of the data communication must be created. This baseline may potentially be used as grounds for future research and standards development. Understanding the path of the data to the SCADA systems and data centers is an important aspect of

critical infrastructure data communication support tools. The third and final critical leg is currently supported through the inclusion of human factors into the DOE WWTPO project on dynamic line rating. This research collaboration will provide the science needed to support the effective use of current and future 'smart' critical infrastructure. It will also provide the solid footing needed to make the decisions that will optimize limited resources without putting capital intensive assets in peril of outages or damage. Due diligence to these three supporting legs provides resilience to the technology platform.

Weather station configured on an electric utility transmission line structure.

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.
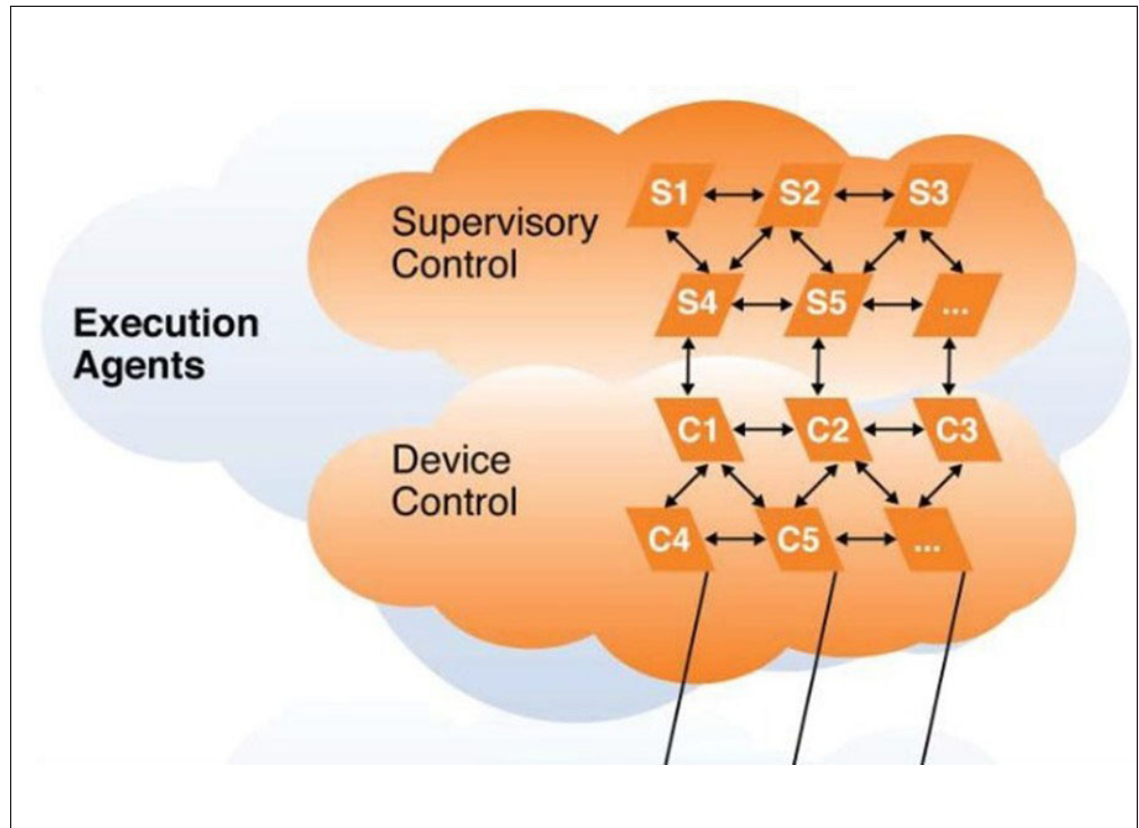
Increasing Critical Infrastructure Resilience through Architecting the Complexity

By Craig Rieger

When considering the ever increasing complexity of our critical infrastructure and underlying control system architectures, a concern of resilience researchers is how to "restructure" this complexity in order to prevent threats that can lead to cascading failures. These threats can occur in various ways, including: malicious attacks from within or outside of the system, as well as unintended errors. While these diverse attack sources require different approaches, a decomposition principle is already implied by the evolution of current control system designs.

In a control system, a collection elements combine to optimally stabilize the entity. This can be seen from looking at chemical process plants, where a collection of separate unit operations make up an integral plant. The unit operation, in this case, defines an area of local optimization. Within the operation, many physical variables may exist. In a plant made up of many unit operations, the process of determining the optimally stabilizable entities normally results in a minimization of the interactions between individual operations. That is, normally only a few physical variables will make up the interactions between unit operations. For example, the flow between unit operations must remain within a specified range, as the downstream operation is designed to be stabilized for operation within that range.

When examining a less complex approach for subdividing infrastructure to increase resilience, researchers have looked into utilizing various forms of micro or macro grids to subdivide the power grid. Within these subdivided areas, power stability is maintained against threats or the ability to regulate the effects of destabilizing forces such as intermittent generation. Through minimization of cyber, control, power and other dependencies and interdependencies, local regions maintain their own stability and prevent cascading affects. Where interdependencies and dependencies remain, polymorphic isolation techniques can be concentrated to counter propagation of threats. The result is a foundation or building block for greater efficiencies, where wide area supervisory strategies can be built without engendering complex failures.

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, "Autonomous 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.

Dynamically Predicting Operator Errors: Coupling a Simulation of Operator Performance to Thermo-Hydraulics Models

By Ron Boring and Diego Mandelli

Human reliability analysis (HRA) has historically focused on modeling human performance within a focused range of normal and abnormal operations at nuclear power plants. The limitations of conventional HRA approaches become apparent when there are scenarios that change dramatically over the evolution of the event or when human actions are not well scripted, such as during rare severe accidents. As researchers at Idaho National Laboratory (INL) de-velop advanced modeling codes to ac-count for plant behaviors, much of what occurs at the plant is ultimately shaped by the humans that control the plant. Advances in modeling plant dynamics are incomplete without a parallel ability to model human operations.

INL researchers recently developed the computation-based HRA frame-work called the Human Unimodel for Nuclear Technology to Enhance Reli-ability (HUNTER). A unimodel—the U in HUNTER—is a simplified cognitive model. Thus, HUNTER represents a simplified cognitive model or a collection of simplified cognitive models to support dynamic risk analysis. HUNTER is a hybrid approach built on past work from cognitive psychology, human perfor-mance modeling, and HRA. Using these research fields as background, HUNT-ER functions as a simplified model of human cognition—a virtual operator—that, when combined with a computation engine such as a thermo-hydraulics based nuclear power plant simulation model, can produce outputs such as the human error probability, task duration, or even operator decision making.

HUNTER has been developed under the U.S. DOE's Light Water Reactor Sustainability Program as a framework to model dynamic risk of human activities in complex systems. HUNTER is the HRA counterpart to the Risk Analysis and Virtual control ENvironment (RAVEN) framework for hardware failure modeling, as depicted in Figure 1. HUNTER was created with the goal of including HRA in areas where it has not been represented and to reduce modeling uncertainty by accounting for human performance more accu-rately than current HRA approaches. Figure 2 depicts
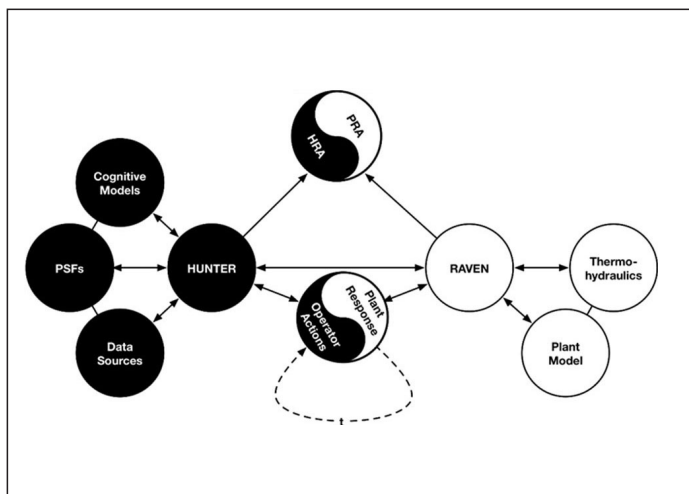

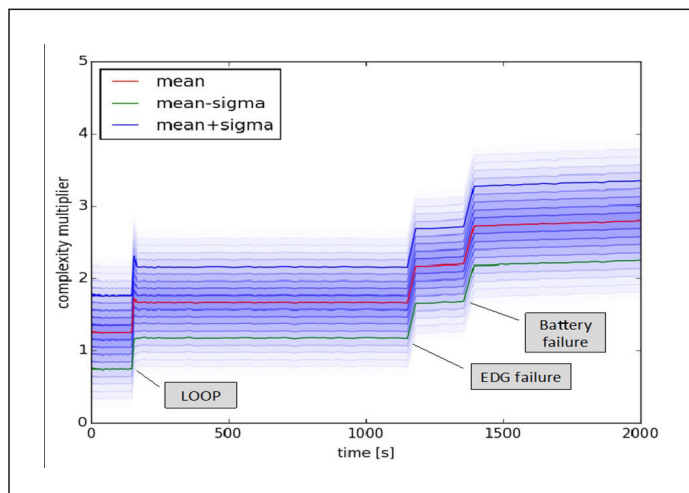*Figure 1. Framework for computation-based HRA.*

Figure 2. Example of HUNTER modeling an operator complexity coefficient for loss of offsite power (LOOP), emergency diesel generator (EDG) failure, and battery failure

example output in modeling the task complexity coefficient in response to changing plant conditions. The task complexity coefficient is, in turn, used as one basis for quantifying human error and determining task duration.

The HUNTER project is part of the Risk Informed Safety Margin Characterization (RISMC) research pathway within the U.S. Department of Energy's Light Water Reactor Sustainability (LWRS) program that aims to extend the life of the currently operating fleet of U.S. commercial nuclear power plants.

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.

INL Sponsors Resilience Week 2016

By Craig Rieger

Resilience Week 2016 was held in Chicago in August at the Lisle Hilton with two hundred ten people in attendance. Resilience Week included 5 multidisciplinary symposia on Resilient Control, Cyber, Cognitive and Communications systems in addition to a more government-industry focused Resilient Critical Infrastructure Symposium. Institute of Electrical and Electronics Engineers (IEEE) Industrial Electronics Society (IES) was the technical co-sponsor. Organizing support came from several organizations, including universities such as Johns Hopkins Applied Physics Laboratory and the University of Illinois, Urbana-Champaign, and government agencies such as Naval Surface Warfare Center and Argonne National Laboratory.

Four well-known plenary speakers presented on cross-disciplinary resilience research in France, defense advanced research, power system resilience, and other resilience topics. The opening welcome was provided by Retired Admiral Bill Leigher, Director of Government Cyber Solutions, Raytheon Company. The other plenary speakers included Dominique Luzeaux, Deputy Director of the Joint Directorate for Networks Infrastructure and Information Systems, France's Ministry of Defense; Massoud Amin, Director of TLI, University of Minnesota and Honorary Chair; and Brian Pierce, Deputy Director DARPA I2O.

With the increased focus on resilience in the United States, federally funded centers have begun to be established. Both the Department of Homeland Security and National Institute of Standards and Technology were represented, with the former's Critical Infrastructure Research Institute (CIRI) led by the University of Illinois Urbana-Champaign had a significant contribution to the symposium. Student competitions were also held to highlight the next generation of resilience researchers. An expansion of the third day of the symposium included a focused track on the human dimension, led by Department of Energy labs.

With the world's dependence on control systems for automating critical infrastructure, the next generation of resilient systems and associated infrastructure will be critical to ensure that these operations perform in a safe and dependable manner. The Resilience Week symposia series provides a cross-disciplinary avenue for interacting with representatives from government, industry and the academic community to shape this vision. Relevance is provided in the application of resilience to real world industry challenges. Attendees see papers in each area of resilience, but more importantly, sessions that combine two or more aspects.

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.

IEEE

Resilience and Security for Industrial Applications (ReSia)

Save the Date!

**Resilience Week 2017
September 18-22, 2017**

The Workforce of the Future:
Complex Problems Require Interdisciplinary Perspectives

By Craig Rieger

Over the years of having advanced my own education and moving from a practitioner to a researcher, I have seen the nuances of opinion on what education should provide to students. That is, what a student should be exposed to before graduation. If you go through an engineering track, you are exposed to curricula that have evolved slowly over recent decades. These curricula include aspects that are unrelated to the discipline, historically integrated to provide a broader "education" as compared to vocational training. In this Renaissance man perspective, in contrast, goes back centuries. While I would like to question why current humanities students aren't required to take a technologies class to broaden their education, I will instead use this same context as segue to future workforce needs.

The Renaissance man perspective suggests a liberal education is beneficial in developing critical thinking beyond a single subject area. Whether this is being achieved in the university environment today is worthy of discussion on its own. I will suggest that to solve the complex problems of today, education that exposes students to the complexity of the issues is critical importance. Issues of cybersecurity, control system autonomy and human interaction with autonomy cross-cut a range of disciplines from the liberal arts, sciences and engineering. Knowing the issues indicates another important perspective, which is establishing the challenges to inspire the next generation to pursue a STEM education.

Some educators and agencies have long recognized the potential value of such education, and yet the nuances involved are dependent on the problem set. From a practitioner standpoint, engineers will often work with technicians, but did their education provide them a perspective on each other's value and contribution to a team? This is unlikely. Yet the dynamic established by multidisciplinary engineering teams could have benefited from the perspective provided ahead of entering the job market. By using a technician to take design input from the engineer and successfully build a bench scale pilot, a positive understanding of a professional dynamic is established. Many of us have worked on projects with different disciplines, but did they effectively communicate? Was there a clear understanding of contributions to recognize equally the importance of each other's contribution….an interdisciplinary team? Establishing this dynamic is even more important with teams that cross not only engineering boundaries, but the boundaries between science and engineering and the underlying disciplines.

Today's highly technological environment has created some natural challenges to the next generation of bright young minds. The desire to advance to a Star Wars or I Robot level of autonomy is upon us, fulfilling an ongoing desire to reduce the cost of production and efficiency. However, the pathway to achieve resilience while developing these systems is ever present. Not only to ensure these new control systems will be threat-resilient (from cyber attack, hurricanes, human error, control system failure, etc), but to achieve resilience within our current complex infrastructures and industry. Resilient solutions are not possessed within any one person or discipline, but in a combination. The effectiveness in providing teams that will successfully address this resilience challenge will also be an educational challenge and a mindset change—for how we educate and how we build teams.