ReCAS Resilient Control Architectures and Systems

A N I C I S N E W S L E T T E R

Select Resilience Papers

Resilient Plant Monitoring System: Design, Analysis, and Performance Evaluation
www.inl.gov/icis/resilientplant

Anomaly Detection for Resilient Control Systems Using Fuzzy-Neural Data Fusion Engine
www.inl.gov/icis/anomalydetection

Deception Used for Cyber Defense of Control Systems
www.inl.gov/icis/deception

Human Factors and Data Fusion as Part of Control Systems Resilience
www.inl.gov/icis/humanfactors

Autonomic Intelligent Cyber Sensor to Support Industrial Control Network Awareness
www.inl.gov/icis/cybersensor

Smart Grid Data Integrity Attacks
www.inl.gov/icis/smartgrid

Notional Examples and Benchmark Aspects of a Resilient Control System
www.inl.gov/icis/notionalexamples

Instrumentation Control & Intelligent Systems

Idaho National Laboratory

Resilience Week 2013

During August, a symposium on resilient systems was held in San Francisco. The symposium was sponsored by Idaho National Laboratory (INL) and University of California-Berkeley along with other partners with academic, industry, and professional organizations. Resilience Week is dedicated to promising research in resilient systems that will protect cyber-physical infrastructure from unexpected and malicious threats – securing our way of life. There were approximately 150 attendees, which included numerous representatives from other DOE national laboratories, DoD, NSA and corporations such as Chevron and United Airlines. Resilience Week includes four co-located symposia involving cybersecurity, control, cognitive, and communication systems. INL's foresight has positioned the lab at the forefront of the thought leadership in a resilience strategy in the wake of increasing concern regarding the effects on our infrastructure from natural and malicious attacks. Dr. Tom Langstaff, a representative of NSA and one of the cybersecurity keynote speakers said of the event, "Congratulations on a well-run and very insightful conference. I do feel this was well worth my time and am very glad I was able to be there with you." Plenary keynote speakers included Dr. Dane Egli, national security senior advisor at Johns Hopkins University, Declan Ganley, CEO of Rivada Networks, and Dr. Norman Whitaker, deputy director of the Information Innovation Office at DARPA. Each of the four resilience-focused symposia (control, cyber, communication, cognitive) had semi-plenary keynote speakers focusing on those specific disciplines. Presentations provided by the keynote speakers can be found on the Resilience Week website. Next year's event will be held in Denver, Colo. Aug. 19-21.

Dr. Dane Egli

Resilient Control Systems Metrics Basis

Establishing a metric that can capture the resilience attributes can be complex, at least if considered based upon differences between the interactions or interdependencies. Evaluating the control, cyber and cognitive dynamics, especially if considered from a disciplinary standpoint, leads to measures that have already been established. However, if the metric were instead based upon a normalizing attribute, such as performance characteristics that can be impacted by degradation, an alternative is suggested. Specifically, applications of base metrics to resilience aspects are as follows:

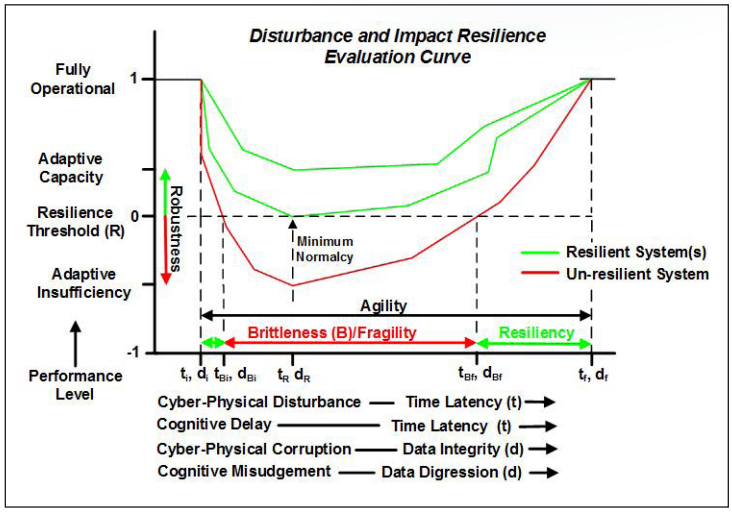

Figure 1. Resilience Performance Basis

Physical Dynamics:
- Time Latency Affecting Stability
- Data Integrity Affecting Stability

Cyber Dynamics:
- Time Latency
- Data Integrity and Availability

Cognitive Dynamics:
- Time Latency in Response
- Data Digression from Desired Response

Such performance characteristics exist with both time and data integrity. Time, both in terms of delay of mission and communications latency, and data, in terms of corruption or modification, are normalizing factors. In general, the idea

Continued next page

Academic & Industrial Leadership

Resilience Week

Resilient Control Systems University Challenge

Technical Committee on Resilience and Security for Industrial Applications (ReSia)

IEEE Transactions on Cybernetics—Special Issue: Resilience Control Architectures and Systems

Continued from previous page

is to base the metric on "what is expected" and not necessarily the actual initiator to the degradation. Considering time as a metrics basis, resilient and un-resilient systems can be observed in Figure 1.

Dependent upon the abscissa metrics chosen, Figure 1 reflects a generalization of the resiliency of a system. Several common terms are represented on this graphic, including robustness, agility, adaptive capacity, adaptive insufficiency, resiliency and brittleness.

Agility: The derivative of the disturbance curve. This average defines the ability of the system to resist degradation on the downward slope, but also to recover on the upward. Primarily considered a time based term that indicates impact to mission.

Adaptive Capacity: The ability of the system to adapt or transform from impact and maintain minimum normalcy. Considered a value between 0 and 1, where 1 is fully operational and 0 is the resilience threshold.

Adaptive Insufficiency: The inability of the system to adapt or transform from impact, indicating an unacceptable performance loss due to the disturbance. Considered a value between 0 and -1, where 0 is the resilience threshold and -1 is total loss of operation.

Brittleness: The area under the disturbance curve as intersected by the resilience threshold. This indicates the impact from the loss of operational normalcy.

Resiliency: The converse of brittleness, which for a resilience system is "zero" loss of minimum normalcy.

Robustness: A positive or negative number associated with the area between the disturbance curve and the resilience threshold, indicating either the capacity or insufficiency, respectively.

On the abscissa of Figure 1, it can be recognized that cyber and cognitive influences can affect both the data and the time, which underscores the relative importance of recognizing these forms of degradation in resilient control designs. For cybersecurity, a single cyberattack can degrade a control system in multiple ways. Additionally, control impacts can be characterized as indicated. While these terms are fundamental and seem of little value for those correlating impact in terms like cost, the development of use cases provide a means by which this relevance can be codified. For example, given the impact to system dynamics or data, the performance of the control loop can be directly ascertained and show approach to instability and operational impact.

The Human Systems Simulation Laboratory is being used to design additional functionality that enhances operator control and awareness.

DOE Unveils New Human Systems Simulation Laboratory at INL

The U.S. Department of Energy's Light Water Reactor Sustainability program has developed a control room simulator in support of control room modernization at nuclear power plants in the U.S. This simulator is part of the Human Systems Simulation Laboratory (HSSL) at Idaho National Laboratory. The simulator is fully reconfigurable, meaning it supports multiple plant models, including those developed by different simulator vendors. The simulator is full-scale, using glasstop touch-sensitive panels to digitally display the analog control boards found in existing plants. The present installation features 45 displays across 15 glasstop panels that are linked together, uniquely achieving a complete control room representation and making this is the largest single installation of glasstop panels in the world. The simulator is also full-scope, meaning it uses the same thermal-hydraulic and physically simulated plant models used by training simulators found at operating nuclear power plants. Unlike in-the-plant training simulators, deployment on glasstop panels allows a high degree of customization of the panels, allowing the simulator to be used for research on design issues of new digital control systems for control room modernization. Control room modernization goes beyond like-for-like replacement of analog instrumentation with digital control systems. The simulator is being used to design additional functionality that enhances operator control and awareness.

Contacts

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

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

www.inl.gov/icis

Multicriteria-based Staging of Optimal PMU Placement for Cyber Resilience

Phasor Measurement Units (PMUs) have recently become one of the major enablers of Wide Area Monitoring, Protection, And Control (WAMPAC) for future power systems. WAMPAC technology enhances stability, reliability and security of power production, transmission and distribution systems and is considered as one of the fundamental components of the smart grid concept.

Some of the major advantages of PMUs when compared to traditional power measurements techniques can be summarized as follows:

1. Location-independent-measurement synchronization using Global Positioning System (GPS)
2. Direct measurements of voltage and current phase angles
3. Increased accuracy, frequency, reliability, and security of state measurements

The placement of PMUs into the power grid is a major contribution to overall resiliency of this critical infrastructure. The problem of Optimal Placement of PMUs (OPP) entails finding a minimal set of PMUs that must be installed in order to provide full system observability.

Because of the large number of PMUs required and their cost, it is important to partition the installation of PMUs into several stages. The prioritization of PMU placement is a function of various criteria, each with different importance (weight). Criteria values and their importance are difficult to be described using discrete numerical values.

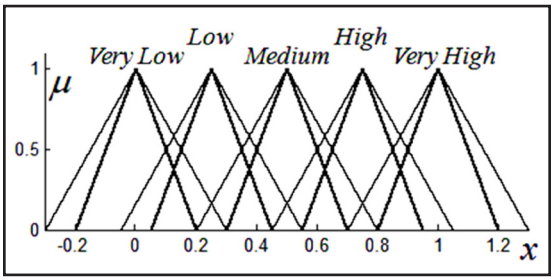

Figure 1. Fuzzy membership of the importance criteria

To address these needs, a multicriteria-based two-step method for optimal PMU placement was developed that uses Memetic Algorithms (MAs) and Linguistic Weighted Average (LWA). In the first step, MA is used to compute the OPP solution based on the requirement of full system observability and maximum measurement redundancy. In the second step, PMU installation criteria are modeled as Interval Type-2 Fuzzy Sets (See Figure 1) and LWA is applied to rank PMU installation sites. The criteria of observability, cost, importance, and security were used for the multi-criteria decision-making.

A user-friendly, interactive Graphical User Interface (See Figure 2) was implemented that enables the visualization of various scenarios and metrics related to the OPP problem.

The developed method was applied to benchmark IEEE 14, 30, 57 and 118 bus data sets. Figure 3 shows two scenarios where importance is changed from observability to security.

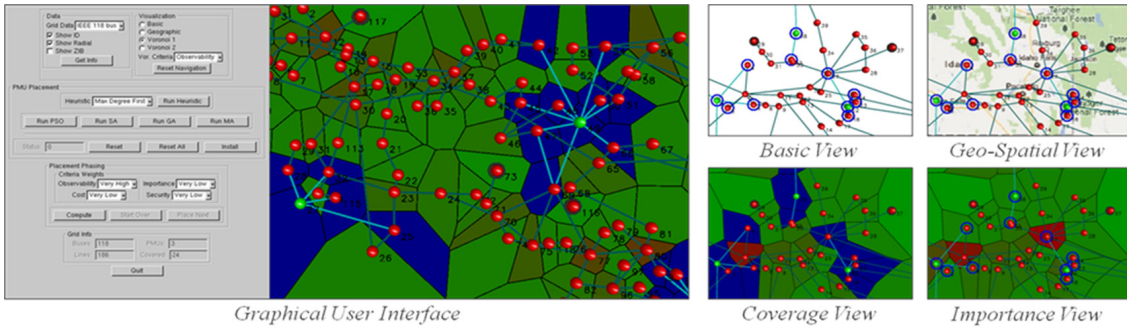

Figure 2. Implemented Graphical User Interface (GUI) with multiple visualization modes

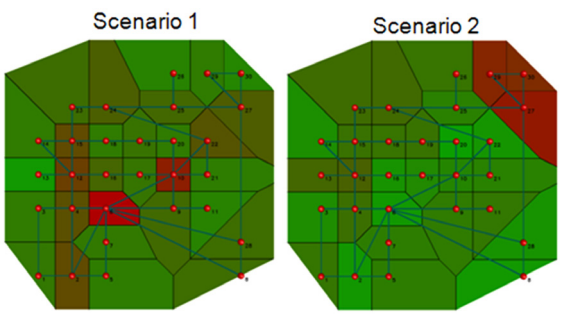

Figure 3. Visualization of observability (Scenario 1) vs. Security (Scenario 2) as the most important criterion. Red represents the most important PMUs while green represents the least important.