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

Using Infrared Thermal Camera Sensor to Recognize Cyber Attacks Externally

By Michael McCarty

The Cyber Partnership for the Advancement of Resilient Control (CyberPARC), an ongoing collaboration with PNNL and SNL, is answering three questions:

1. Can cyber attacks be detected using a thermal camera and other external indicators?
2. Can the alerts be processed in time to prevent the attack?
3. Can analytics and machine learning take advantage of the data and build a model that provides insight into the process that exceeds that which is possible given simplistic threshold alarms?

To detect attacks, cyber sensors frequently tap into the data stream. This presents several difficulties because the sensor's controls and alarms become part of the data stream and the sensor becomes part of the attack surface. Research is being done to find ways to detect cyber attacks using side channel methods, including the use of thermal, electromagnetic, motion and other environmental sensors. These methods of detection open the door to detect things which otherwise would not be detectable, and with their side nature they are on a different plane than the attack so they are out of the attack surface's scope.

During the research it was found that DOS attacks are indeed detectable within a matter of seconds using a thermal camera. During a DOS attack, certain chips on the PLC networking card showed jumps of .5 degrees F, whereas while not under attack the temperature remained very steady. A notable fact to point out was that only one chip on the entire network card, which contains several dozen chips, responded thermally to an attack.

More subtle attacks that inject small payloads into the PLC process cannot be detected by this method. Given that the data is collected at a rate of 10hz, it is impossible to detect a few instructions that are out of place on a Multi MHz processor. Attacks such as a packet of death may be detectable after the fact but not left of boom.

The scale of the response is a determining factor in deciding if the sensor's response is in time to be of benefit. On a small scale of one PLC, the sensor may not be fast enough to respond to an attack. At an entire network scale, once the sensor has found that a single PLC was attacked it can alert the network as a whole to prevent the attack spreading and thus protect at the network scale.

Testing is still being done to see if analytics and machine learning can provide better response time and insight into the status of the PLC.

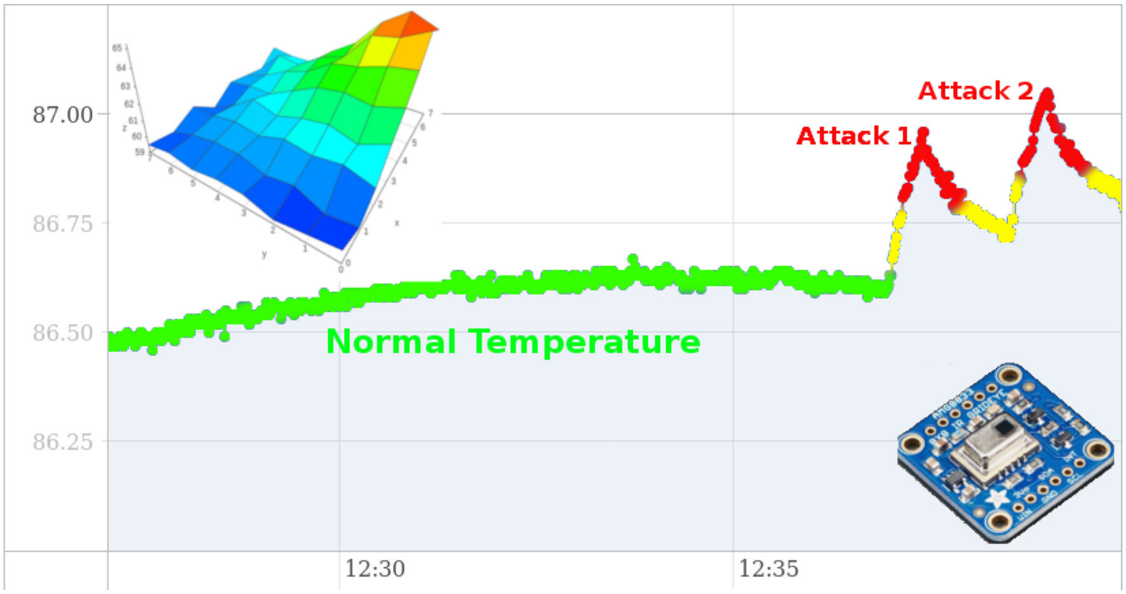


FIGURE 1. This graph shows the clear spike in temperature when a common PLC is under a DOS attack. (top left) 3d temperature graph of 8x8 array produced by inexpensive thermal camera (bottom right)

Resilient Control & Instrumentation Systems

INL Idaho National Laboratory

Energy I-Corps Experience for high temperature tolerant electrical insulation

By Bjorn Vaagensmith and Brad Whipple

Existing Transformer oil impregnated paper insulation is vulnerable to decomposition due to elevated temperatures as low as 90 °C experienced during the launch of an electromagnetic pulse (EMP) attack or a naturally occurring geomagnetic disturbance (GMD). Team Glass paper sought to solve this problem by creating a high temperature tolerate (up to 450 °C) electrical insulation that could better protect transformers from failure after a GMD or EMP event. The team was accepted into the Energy I-corps program to perform an industrial outreach to gauge industrial interest on the technology. The Energy I-corps program proved to be an invaluable experience that teaches researchers how to approach the industrial sector learn about the commercial eco-system and receive valuable feedback on the technology developed within the national laboratories.

Since GMD events are rare and likely not a major concern to commercial entities, team glass paper refocused their value proposition to using the new insulation for make smaller transformers that would operate at higher temperatures. This value proposition, in large, was not well received due to many reasons: other transformer components could not withstand sustained temperatures above 220 °C (and would need to be redesigned), regulations preventing operators from running transformers hotter, and personal safety concerns for working near the transformer. Glass paper's technology gained the most interest from utilities in large cities, where real-estate is expensive and electrical demand is growing, as well as mobile transformer manufactures; however running the transformers hotter was still a safety concern. New features, such as crimping the paper, were found to be very important add-ons to the development of glass paper for transformer applications. The interviews conducted provided solid insight into what niche applications and features would be most interesting or important to customers. The experience is defiantly something all researchers could benefit from. The feedback from customer exploration will help shape how glass paper is developed in the following years and how the value proposition is reshaped.

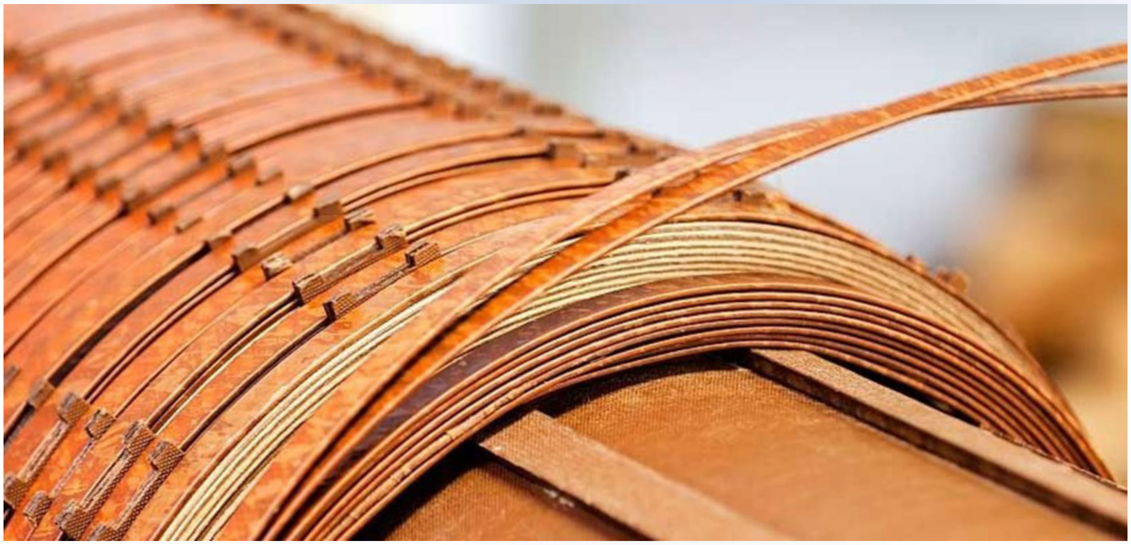


Figure 1. Insulation wrapped conductor being wound onto a transformer core.

Select Peer-Reviewed Publications

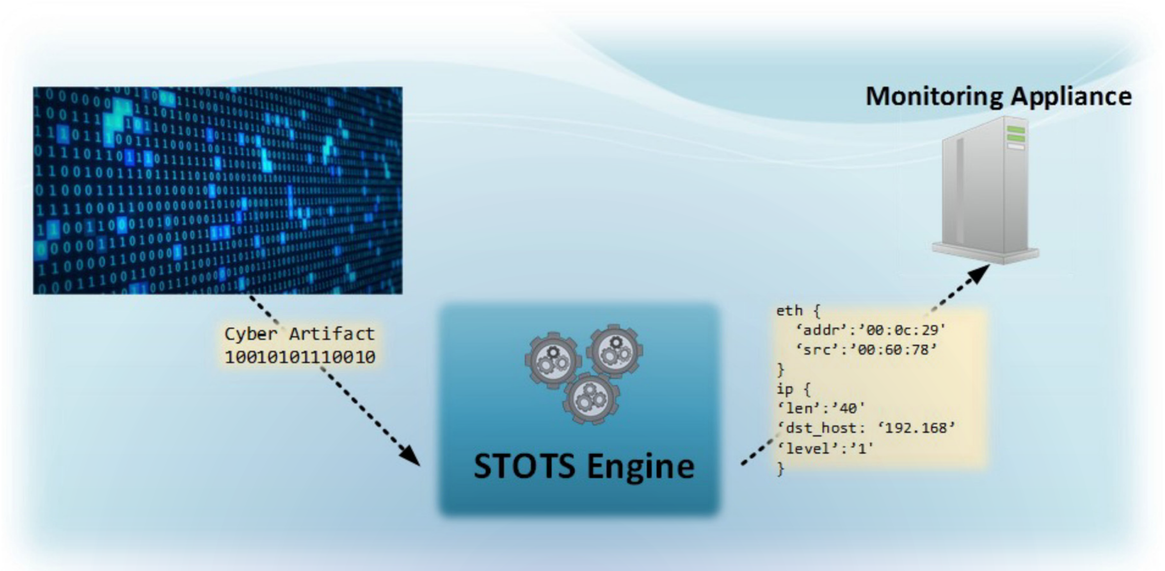
T. Vollmer, M. Manic, "Cyber-Physical System Security With Deceptive Virtual Hosts for Industrial Control Networks," IEEE Transactions on Industrial Informatics, vol. 10, no. 2, May 2014.

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 Intelligent Cyber Sensor to Support Industrial Control Network Awareness," IEEE Transactions 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.

D. Wijayasekara, O. Linda, M. Manic, C. Rieger, "FN-DFE: Fuzzy-Neural Data Fusion 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.



```
eth {
  'addr':'00:0c:29'
  'src':'00:60:78'
}
ip {
'len':'40'
'dst_host: '192.168'
'level':'1'
}
```

Creative Destruction and Agnostic Detection using a Structured Threat Observable Tool Set

By Bryce McClurg

An agnostic tool set, non-intrusive to operational environments, and applicable to automated response can be tailored to a wide variety of substation automation and energy management system technologies. Current methods for finding indicators of compromise (IOC) in Industrial Control Systems (ICS) rely on pre-existing sensors, firewalls, or intrusion detection systems (IDS). Every sensor added increases the cost of maintenance and complexity of reviewing logs. Cyber defenders are searching for creative, stealthy adversaries who don't want to be found. In essence, they are finding the proverbial "needle in the haystack".

As part of the California Energy Systems for the 21st Century (CES-21) project, Idaho National Laboratory has developed a Structured Threat Observable Tool Set (STOTS), using Structured Threat Information Expression (STIX), as a method for detection and monitoring that can be used by the most advanced and the most basic cyber personnel to find IOCs for configuration specific systems. The tools developed in STOTS focus on surgical detection and response for a specific threat, enabling cyber defenders to be more agile in defense against cyber adversaries. This provides an agnostic tool set which enables detection in the absence of, or in coordination with commercial-off-the-shelf (COTS) products. Refocusing STOTS to large data analytics provides the "needle in the haystack".

Select Peer-Reviewed Publications

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.

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, Aug. 2016, pp. 89–94.

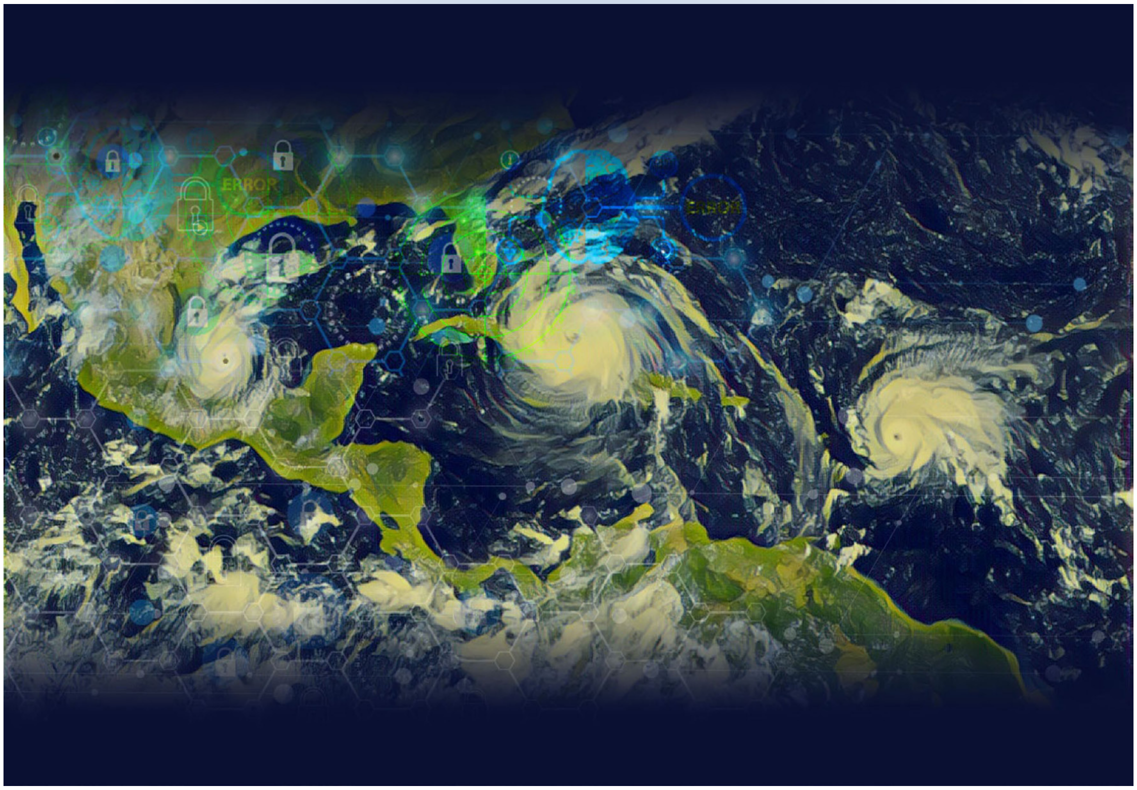
M. Manic, K. Amarasinghe, J. Rodriguez-Andina, C. Rieger, "Intelligent Buildings of the Future: Cyberaware, Deep Learning Powered, and Human Interacting," IEEE Industrial Electronics Magazine Vol. 10(4):32-49, December 2016.

Live Wire Resilient Control & Instrumentation Systems

Systems Resilience and Risk Framework: Components, Systems, and Embedded Intelligence

By Gavin Hawkley

Complex adaptive systems (CASs) comprise complex systems such as infrastructure that can be evaluated as combinations of interacting components with the ability to adapt to variables as a result of learning processes. Many components are capable of learning from stressors and past experiences, and adapting to future expectations, such as systems that adjust electric generation outputs to meet varying power loads (IEEE 2001). Complex systems are characterized by having a large number of dimensions, feedback loops, unknown or inherently random parameters, emergent behavior and lagging dynamics, etc. On the contrary, complicated systems are not easy to understand, but they are oftentimes knowable. They are highly integrated systems with low dynamics, and their decomposition for analytical goals is reasonable and known. A central question is whether the established methods of risk and reliability assessment developed for complicated systems can also be applied to complex systems. The likelihood of emergent phenomena and hidden failures in large-scale systems increases as the number of components increases, and with increased interdependencies with other systems. The importance of dynamics across connected systems has been evidenced by large scale blackouts in the electric power grid, showing a high degree of coupling between the network and control systems. Failure of these complex systems is often the result of relatively slow initial degradation escalating into cascading component failures. This provides opportunity for a platform that couples an analytical framework of models with experimental test loops, to validate data and capture the interaction of complex adaptive systems, such as the electric power grid and automation systems.



Select Peer-Reviewed Publications

T. McJunkin, and C. Rieger, “Electricity Distribution System Resilient Control Metrics,” in 2017 Resilience Week, 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.

C. Rieger, I. Ray, Q. Zhu, M. Haney, “Industrial Control Systems Security and Resiliency,” Springer International Publishing, Volume Series 75, Copyright 2019.

R. Boring, T. Ulrich, H. Medema, R. Lew, “Operator Resilience to Cyber Interdictions in Nuclear Power Plants,” Resilience Week, November 2019.

Resilience Week 2019

By Craig Rieger

The 12th Resilience Week was successfully completed in San Antonio, and saw a 40%+ increase in participation. Industry, DOE-OE and DOE-EERE sessions were included at the event this year and included several industry associations (EEI, AGA, UTC) and members (Southern Company, PJM, etc.) discussing near and long term resilience challenges. Cross-DOE EERE sessions were held, including both WETO and SETO, and will continue as part of accepted panel and ongoing program sessions to discuss hybrid application of renewables and future programs. A highly successful exhibitor session included two dozen cyber, power, lab and industry associations, providing a recovery mechanism for the event, which includes three receptions, long breaks, and numerous networking opportunities. The event was opened by the Dean of Engineering at UTSA, followed by Congressman Joaquin Castro. Jonathon Moken, Senior Director PJM and Anne Bomar, Senior Vice President, Dominion provided plenaries on the second day. UTSA, the co-sponsor, had opportunity to discuss their National Security Collaboration Center and CyManII proposal to the DOE-EERE/AMO cyber manufacturing call, which included multiple labs and industry. The final panel, discussing the Grid of the Future, included Rita Baranwal, Assistant Security, DOE-NE; Jonathon Monken, Senior Director, PJM Interconnection; Kimberly Denbow, Managing Director, AGA; and Pat Hoffman, Principal Assistant Secretary, DOE-OE. It is worth noting that the diversity represented on this panel was typical of other plenaries, keynotes and panels throughout the symposium.

Select Peer-Reviewed Publications

M. Soltani, W. Fatnassi, A. Bhuyan, Z. Rezki, P. Titus, “Physical Layer Security Analysis in The Priority-Based 5G Spectrum Sharing Systems,” Resilience Week, November 2019.

J. Ulrich, B. Vaagensmith, C. Rieger, J. Welch, “Software Defined Cyber-Physical Testbed for Analysis of Automated Cyber Responses for Power System Security,” Resilience Week, November 2019.

C. Becker, K. Derr, S. Ramirez, A. Baset, “Plug and Play Flexible Signal Classification and Processing System,” Resilience Week, November 2019.

T. Ulrich, R. Boring, R. Lew, “On the Use of Microworlds for an Error Seeding Method to Support Human Error Analysis,” Resilience Week, November 2019.

IEEE
Resilience and Security for Industrial Applications (ReSia)

Save the Date!

Resilience Week 2020
October 19-22, 2020