ReCAS Resilient Control Architectures and Systems

Volume 1, Number 1 AN ICIS NEWSLETTER July 2010

Resilience Papers

Resilient Control Systems: Next Generation Design Research
http://www.inl.gov/icis/nextgendesign

Deception used for Cyber Defense of Control Systems
http://www.inl.gov/icis/cscyberdefense

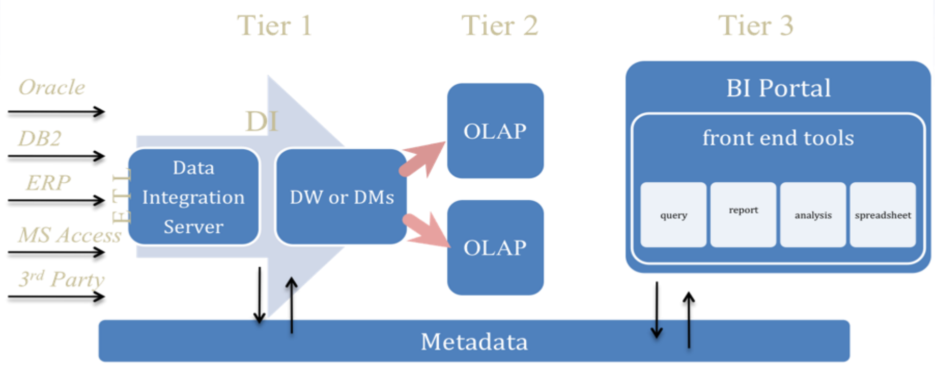
Human Factors and Data Fusion as Part of Control Systems Resilience
http://www.inl.gov/icis/csrhumanfactors

Critical Infrastructure Modeling: An Approach to Characterizing Interdependencies of Complex Networks & Control Systems
http://www.inl.gov/icis/criticalmodeling

Instrumentation Control & Intelligent Systems

Second International Symposium on Resilient Control Systems

The symposium was sponsored by the INL, ISU, and the U of I. Technical co-sponsorship was also received from the IEEE Industrial Electronics Society (IES). This second symposium was organized to communicate, discuss, and further develop high level visions and ideas for resilient control systems via community participation and to vet, modify, extend, and endorse particular concepts that will lead to a specification of research needs. Desired products of the symposium were the generation of summary presentations and paper proceedings for those identified concepts that will set the stage for task group execution, and the identification of future research strategies and products. The symposium evolved this year and included an open registration and call for papers. Focused panel discussions were also included instead of breakouts. Over fifty people representing government, academia, and industry attended the symposium, including roughly 12% international participation and the remaining from the United States. Keynotes were provided in both of the track areas. Professor Ross Anderson from the University of Cambridge provided a perspective in the cyber awareness area with his presentation titled, “Security Economics and Critical National Infrastructure.” Professor David Woods from Ohio State University gave an overview of the resilience engineering research field of human systems with his presentation, “Fundamentals to Engineer Resilient Systems: How Adaptive Systems Fail and the Quest for Polycentric Control Architectures.” An academic and practical view of complex networks also came in keynotes from Professor John Doyle of the California Institute of Technology (Caltech) and Mr. Michael Assante of the North American Electric Reliability Corporation in their presentations titled, “The Architecture of Robust, Evolvable Networks” and “North American Bulk Power System: Need for Resilient and Secure Designs,” respectively.



Integrated Control System Data Fusion

Modern critical infrastructure control and security systems have the capability to provide facility managers, operators and security personnel with an abundance of monitoring data. This data comes from multiple sources, including process and control status as well as network and physical security information, that are deployed at different levels within the system to provide both situational awareness and defense in depth. However, due to the complexity and amount of the data, it is challenging for operators to quickly analyze situations and respond appropriately. This increasing volume of situational data and the time-critical nature of related decisions makes data fusion a critical technology for transforming large amounts of information into timely, actionable intelligence. This second year ICIS research effort hypothesizes that a holistic assessment and prioritization of control system and security information will provide a basis for fusing data from various sources and in a specific manner so as to draw the relationships among them. The envisioned data fusion system can be illustrated by the following 3-tier architecture shown in the figure above.

The main tiers of this system would execute: ETL (Extraction, Transformation, and Loading) of disparate data sources along with creation of Data Warehouses (and Data Marts), followed by OLAP (On-Line Analytical Processing) tier, and resulting in front end suite of tools for query, analysis, and reporting. The results of this effort are expected to provide a capability that will aid in enhancing manager/operator response and increase overall facility stability and efficiency.

INL Idaho National Laboratory

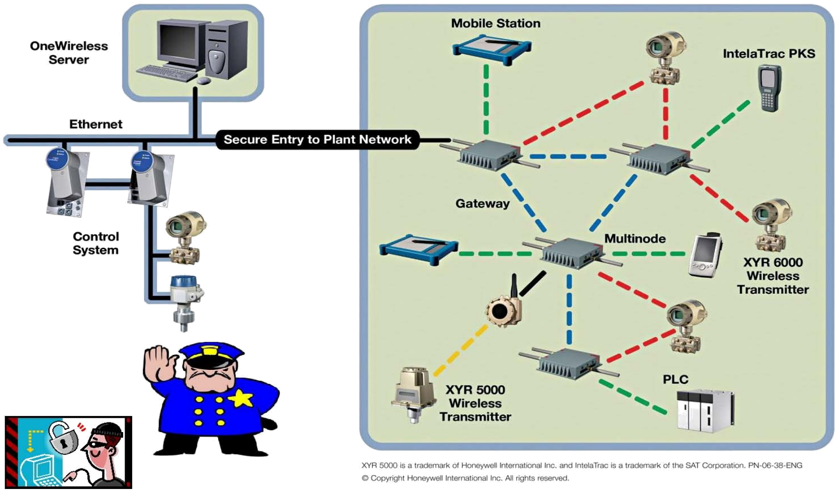
For more information

Technical Contact:

Craig Rieger
(208) 526-4136
Craig.Rieger@inl.gov

www.inl.gov/icis

A U.S. Department of Energy
National Laboratory


OneWireless Server
Ethernet
Secure Entry to Plant Network
Control System
Mobile Station
IntelaTrac PKS
Gateway
Multinode
XYR 6000 Wireless Transmitter
PLC
XYR 5000 Wireless Transmitter

XYR 5000 is a trademark of Honeywell International Inc. and IntelaTrac is a trademark of the SAT Corporation. PN-06-38-ENG
© Copyright Honeywell International Inc. All rights reserved.

Resilient Wireless Sensor Networks

Wireless sensor networks (WSN) are becoming an integral component in modern industry. Their implementation includes factories, electric plants and distribution, municipal water and sewer facilities, natural gas storage, and distribution facilities and even nuclear facilities. These devices aid in measuring and managing the operation of these services and in process control for manufacturing facilities to improve the overall efficiency and safety. As an integral component, they are an important element in designing a resilient control system. Resilient design considers the reliability of WSN in control systems that provide the pathway for both sensory inputs and the active control responses when making decisions and transmitting a control command.

The reliability of these systems depend on understanding the effect of radio frequency (RF) and/or cyber interference to wireless sensors which can lead to a control system failure. John Buttles' LDRD hypothesis suggests that radio frequency (RF) and/or cyber interference to a Wireless Sensor Network (WSN) will lead to destabilization of a control system by introducing latency or modifying data. He will design, build, and analyze several full scale WSN control systems at the CAES facility with tools that enable the application of multiple interference types. The CAES facility was selected due to its combined industrial and office-like environment that best resembles a real world installation. This will provide a comprehensive look at the weaknesses and vulnerabilities within WSN designs and investigate the effects of multiple interference types on WSN.

Currently, the wireless sensor testing capability being developed is built around several vendor and protocol type sensors, WSN transmit and receive test equipment, and RF test equipment to create an industry deployment environment. This environment will have the ability to vary the types and amounts of wireless sensors deployed, operate multiple types of radio systems, and generate other sources of interference.

This research will add to the current resilient design research at INL and will also be used by vendors to improve their next generation designs. The developed approaches and solutions will be used to resolve system degradation and failures resulting in improved reliability of WSN.

Resilience News

- Marketwire, *TELX Plans to Join With Neutral Tandem to Expand New Ethernet Exchange Network Services to 21 Key U.S. Locations*, June 2010.
- Marketwire, *Cisco 'Connected Grid' Solutions Help Bring Intelligence, Resiliency and Security to the Smart Grid*, May 2010.
- Marketwire, *Intercept Chooses 3PAR Utility Storage for High Performance Server and Desktop Virtualization*, May 2010.
- Marketwire, *Cavium Networks Announces the Availability of Its Highly Integrated Single Chip PureVu™ Video Processor Family Enabling Whole-Home Wireless Display Capability*, May 2010.
- Mark Cox, *EMC Announces Virtual Storage Breakthrough with VPLEX Technology*, May 2010.
- Ellen Messmer, *Cyberattacks Seen as Top Threat to Zap U.S. Power Grid*, June 2010.