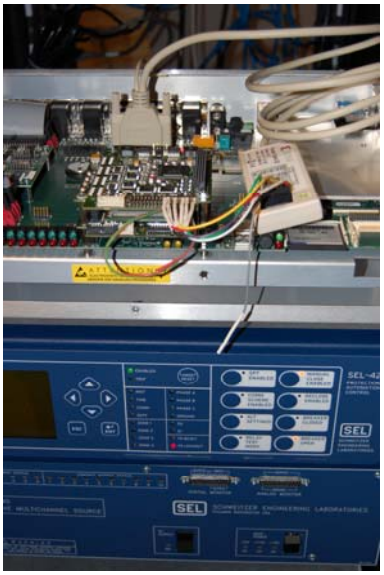
PRESS RELEASE

From the University of Illinois Information Trust Institute

Information Trust INSTITUTE

Major Donations from Industry to the Information Trust Institute's New Power Systems Networking Lab

A group of leading high-tech companies has come together to make a series of major equipment donations that are playing a crucial role in the creation of the new Power Systems Networking Laboratory in the University of Illinois Information Trust Institute (ITI).



Equipment donated to the new Lab includes this data aggregator, distance relay, and test system from Schweitzer.

The Power Systems Networking Laboratory has been established as part of ITI's Trustworthy Cyber Infrastructure for the Power Grid (TCIP) Center, with funding from the U.S. National Science Foundation as well as industry. The newly donated equipment will make it possible for Laboratory researchers to accomplish some of the major goals of the TCIP Center, which is addressing the challenge of how to protect the nation's power grid by significantly improving the way the power grid infrastructure is built, making it more secure, reliable, and safe. TCIP, which involves researchers from Washington State University, Cornell University, and Dartmouth College as well as ITI, is focused on securing the low-level devices, communications, and data systems that monitor and control the power grid, to ensure trustworthy operation during normal conditions, cyber-attacks, or power emergencies.

The purpose of the Power Systems Networking Laboratory is to create a realistic, flexible, configurable, and customizable environment to enable research in trustworthy power system communications and control. The Laboratory will use a mixture of commercial power system equipment and simulation to create a representative control network for the electrical power grid. The network will consist of both the power equipment that monitors and regulates the flow of electricity, and the computer and communications system that records, aggregates, and communicates data about the health of the power grid to human operators. It will be used to experiment with next-generation technologies that span the communications from substation devices to control centers and all the way to regional system operators.

The single largest industry contribution came from Open Systems International (OSI), which is a leading supplier of open automation solutions for real-time management and optimization of complex production, transport, and delivery networks for utilities in the electric, oil and gas, transport, and water industries. OSI's generous donation included equipment and training, including a Monarch Energy Management System (EMS) and four advanced RTUs. OSI's President & CEO, Bahman Hoveida, is enthusiastic about the new Laboratory and his company's role in making it possible. "The U of I is my alma mater, and I am specially pleased that our company has had the opportunity to be involved in the creation of this laboratory," he said. "The cyber security research to secure our nation's power grid is an important issue, and I am confident that the industry can benefit immensely from the fine research to be conducted under this program."

Another major donor is Schweitzer Engineering Laboratories, Inc., which supports the protection, monitoring, control, automation, and metering of electric power systems in over 100 countries. It donated several pieces of equipment, including data aggregators, power system protection relays, and serial line encryption transceivers.

Other significant contributions came from OSIsoft, which donated its PI data historian software and training; InStep Software, LLC, which donated its InStep data historian software and training; GE Multilin, which donated multiple intelligent relays; and Siemens AG, which donated a transmission system protection relay. OSIsoft's PI System is the industry standard in enterprise historians. InStep Software specializes in real-time, fault-tolerant data acquisition, provisioning, and analysis systems. GE Multilin is a leader in protection, control, metering, communications, and automation systems. Siemens is one of the world's largest engineering and electronics companies and addresses a wide range of application areas, including power.

It is anticipated that the new laboratory will be fully furnished and ready for experimentation by the end of October 2007.

About the Information Trust Institute (ITI)

The Information Trust Institute is a multidisciplinary cross-campus research unit housed in the College of Engineering at Illinois. It is an international leader combining research and education with industrial outreach in trustworthy and secure information systems. ITI brings together over 90 faculty, many senior and graduate student researchers, and industry partners to conduct foundational and applied research to enable the creation of critical applications and cyber infrastructures. In doing so, ITI is creating computer systems, software, and networks that society can depend on to be trustworthy, that is, secure, dependable (reliable and available), correct, safe, private, and survivable. Instead of concentrating on narrow and focused technical solutions, ITI aims to create a new paradigm for designing trustworthy systems from the ground up and validating systems that are intended to be trustworthy. www.iti.uiuc.edu

Contact: Molly M. Tracy, Associate Director, Information Trust Institute, 217/333-3437, mollyt@iti.uiuc.edu.

Writer: Jenny Applequist, Information Trust Institute, 217/244-8920, applequi@iti.uiuc.edu.

Released October 11, 2007

University of Illinois at Urbana-Champaign