

NEWS RELEASE

Release Date:
1.22.2007

Contact: Laurie Burnham
(603) 646.0686

PROTECTING CRITICAL PROCESS CONTROL SYSTEMS

Workshop to address urgent security needs facing the oil and gas industry

Somewhere in the world, a cyber terrorist punches keys on a laptop, his attention focused on a pipeline thousands of miles away. Operating via public computer networks, the stealth terrorist successfully hacks into the network of a petroleum transport company, gaining control of a set of flow valves. Hazardous material is released that forces the evacuation of a nearby town and results in an expensive cleanup.

An actual event? Not yet. But hypothetical attacks of this type represent a real and growing threat to the United States, according to the Institute for Information Infrastructure Protection (I3P) a consortium of universities, government labs and research institutions managed by Dartmouth College. With funding from the Department of Homeland Security, this multi-disciplinary research group conducts cutting-edge research in the field of cyber security and is actively developing software tools to safeguard the nation's infrastructure against cyber crime.

To specifically address the urgent need for security technologies in the oil and gas industry, the I3P announced today that it will hold a two-day workshop in Houston, Texas on February 15 and 16, 2007. A multidisciplinary team of experts will present an overview of hypothetical cyber attacks on critical infrastructures and also demonstrate new tools that can prevent, detect and respond to future cyber intrusions.

"Many industrial control systems are vulnerable to hackers, and the consequences of such an attack could be devastating," says Ulf Lindqvist, program director in the Computer Science Laboratory at SRI International, a member of the I3P.

The workshop will showcase the I3P's leadership in tackling critical issues in infrastructure security. According to John Cummings, project director for the I3P control systems research project and senior manager at Sandia National Laboratories, a cyber event leading to the disruption of a control system could have serious safety, environmental and economic impacts. "Not only do control systems play a critical role in the automation of industrial facilities, but they are increasingly connected via business networks to the Internet. Add to the mix the widespread adoption of standard hardware and software systems and no wonder we're seeing a proliferation of security concerns," says Cummings.

Specifically, the I3P workshop will highlight three key areas:

- **Identifying vulnerabilities and assessing the impact of cyber attacks on process control systems**

Participants will learn about the growth in cyber incidents and about major weaknesses in the computer-controlled operations of essential industries.

- **Managing risk while seeking adequate safeguards for critical infrastructures**

Attendees will gain an in-depth understanding of the technical, business, and societal risks posed by cyber attacks and be introduced to ground-breaking risk assessment tools.

- **Adopting effective security tools and technologies**

The audience will participate in demonstrations of integrated security tools that can be used to help design, deploy and maintain secure process control systems.

The workshop is intended for a broad audience of control systems engineers, operators, information and security officers and vendors, as well as security experts from government, industry associations and academia. Participants are expected to walk away with a greater understanding of potential risks to process control systems, system interdependencies, and the tools and technologies for ensuring secure systems.

The I3P Control Systems Research Team includes specialists from Dartmouth, MIT Lincoln Laboratory, the MITRE Corporation, New York University, Pacific Northwest National Laboratory, Sandia National Laboratory, SRI International, the University of Illinois Urbana-Campaign, the University of Tulsa and the University of Virginia.

More information about the workshop can be found at the I3P web site: <http://www.thei3p.org/r/10094>

Members of the media interested in attending the workshop are asked to RSVP to Gail Walker at [gail.walker@dartmouth.edu/](mailto:gail.walker@dartmouth.edu)

The I3P, a consortium of universities, government labs and research institutions, was established in 2001 to address security issues threatening the cyber infrastructure of the United States.