

Evidence suggests that process control systems—the computer networks that drive such critical operations as the refining and flow of petroleum and natural gas products—are increasingly vulnerable to cyber attack. Aware of this trend, Dartmouth’s Institute for Information Infrastructure Protection (I3P), a key player in the field of cyber security research and development, will host a workshop on April 28 in Houston to address critical security issues facing the energy sector.

Intended for representatives from oil, gas and electric companies, the I3P event will highlight vulnerabilities that could compromise a control center overseeing such operations as drilling and pipeline flow, among others; the workshop will also introduce new tools and approaches to increase control system security.

Featuring the work of eight I3P member institutions, the workshop will attract a broad audience of engineers, security officers, system operators and software vendors from the energy sector. Participants will not only hear about best practices in process control system security but will learn about specific tools the I3P and its consortium members are researching, designing and commercializing.

In addition, the workshop will address the following topics:

- National R&D priorities related to critical infrastructure protection
- The future of PCS security: how can security best meet the needs of individual companies?

David Batz of Alliant Energy will deliver the keynote address, “The Wrath of Mother Nature: Implications for Cyber Security,” describing how catastrophic flooding in 2008 disrupted operations at a major utility and how the lessons learned might help a control system operator respond to a cyber attack.

This year’s workshop, the I3P’s fifth in the area of process control security, meets a clearly identified need. “Process control systems, which typically rely on a dispersed network of sensors and other smart devices to drive industrial processes, are vulnerable to sabotage on myriad fronts,” says project leader Robert K. Cunningham of MIT Lincoln Laboratory. “The I3P brings a holistic perspective to the security of these systems that is greatly valued by industry.”

“Moreover,” adds Charles C. Palmer, director for research at the I3P, “in an applied research program such the one presented at this workshop, close collaboration between researchers and industry is not just ‘nice to have’ but in fact is a requirement for success.”

The workshop also serves as the kickoff event to the 81<sup>st</sup> annual ENTELEC conference. Greg Vaughn, president of ENTELEC will deliver a speech that emphasizes the importance of research and development in a talk titled “Today’s Technology Launching Tomorrow’s Solutions.” [Insert quote from Vaughn]

The I3P is a national consortium of leading universities, national laboratories and non-profit institutions dedicated to strengthening the cyber infrastructure of the United States.

Founded in 2002, with funding from the Department of Homeland Security and the National Institute of Standards, the I3P is managed by Dartmouth College.

and include lectures, discussions and demonstrations. Feature talks by experts from eight I3P member institutions as well as demonstrations and discussions of will introduce a suite of tools and lead discussion sessions on new approaches to process control system security.

takes its educational role seriously and has presented tools and other technological breakthroughs for improving the security of the computer networks that run oil refineries, gas pipelines and drilling operations.

project leader Robert K. Cunningham of MIT Lincoln Laboratory.

Houston one day prior to the 81<sup>st</sup> annual ENTELEC conference, which draws a large crowd of oil, gas and electric sector energy and telecommunications specialists.

Recognizing the value of reaching a broad community of engineers, operators, the I3P is timing its workshop to be the kickoff event to the 81<sup>st</sup> annual Entelec conference. Entelec, an association of...will \_\_\_-on April – to – in Houston.

Specifically, the workshop will

In a world awash in cyber threats, protecting critical infrastructures, such as oil refineries, gas pipelines and other energy facilities against digital sabotage has become a critical security issue.

These computerized systems however are vulnerable to a broad array of cyber threats.

---

eed resilience must harden their defenses against cyber attack and devise strategies to ensure their rapid recovery and restoration in the event of an attack.

In a world ever more vulnerable to cyber disruption, critical infrastructures, including oil and gas facilities, are increasingly at risk of attack. To address security issues related to process control system security...

---

At the end of April, Dartmouth's Institute for Information Infrastructure Protection (I3P), will host a workshop to address computer vulnerabilities in the oil and gas sector. The event—to be held in Houston on April 2—will showcase new tools and technologies for process control system security.

A team of experts from eight I3P member institutions will present tools and other technological prospects for improving the computerized control systems that run oil refineries, gas pipelines and drilling operations.

According to Robert K. Cunningham, leader of the I3P control system project,

Specifically, the workshop will address the following:

Oil refineries, gas pipelines and electric generating plants—among other industrial processes—depend heavily on computerized control systems.

Intended for \_\_\_\_\_, the workshop will bring together security experts  
to explore recent technological breakthroughs in this area.

leath consequences for the oil and gas sector that could range from a refinery shutdown to an environmental disaster.

introduce a suite of tools the I3P and its consortium members are developing and

on the latest tools and security strategies highlighting vulnerabilities in the oil and gas sector and presenting strategies for closing them.

A team of experts from eight I3P member institutions will highlight vulnerabilities as well as introduce new tools and approaches to control-room security.