



Institute for
Information
Infrastructure
Protection

www.thei3p.org/

PROCESS CONTROL SYSTEMS SECURITY RESEARCH PROJECT

Developing Security Solutions for the Oil and Gas Sector

PROJECT OVERVIEW

The Process Control Systems Security Research Project is supported by the Institute for Information Infrastructure Protection (I3P). The project is focusing cyber security related research at some of the country's top institutions on improving the robustness of the information infrastructure in the oil and gas sector. Eleven institutions from across the country have joined forces to develop new solutions and demonstrate their effectiveness to the oil and gas sector owners, operators, and vendors.

PROJECT GOALS

The team is working to deliver prototype tools and increase knowledge to accomplish the following goals:

1. Increase the awareness of Process Control System (PCS) security risks
2. Develop programs to educate students and stakeholders on PCS security
3. Recommend mitigation strategies for operators and policy makers
4. Develop and prototype technology and tools for PCS security
5. Advance basic research in inherently secure PCS
6. Gain national recognition for the I3P as a leading center of research, knowledge, and expertise in PCS security



PROJECT SUCCESS

The success of the project will be measured by improved robustness in the oil and gas infrastructure through the adoption of research findings and technology.

The project will contribute to significantly increased awareness of security challenges and solutions for the oil and gas sector that can be applied in other infrastructure sectors as well.

Since many of the project team members are located at major universities, the project will also contribute to the education of new cyber security graduates who will become knowledgeable in securing process control systems.

TEAM MEMBERS

The research team is composed of researchers and engineers from the following I3P member Institutions:

- Center for Information Security—University of Tulsa
- Dartmouth College
- I3P Administrative Office
- Information Trust Institute—University of Illinois Urbana-Champaign
- MIT/Lincoln Laboratories
- MITRE Corporation
- Institute for Civil Infrastructure Systems—New York University
- Pacific Northwest National Laboratory
- Sandia National Laboratories
- SRI International
- University of Virginia



Institute for
Information
Infrastructure
Protection

www.thei3p.org/

PROCESS CONTROL SYSTEMS SECURITY RESEARCH PROJECT

Developing Security Solutions for the Oil and Gas Sector

RESEARCH APPROACH

1. Understand the vulnerabilities, characterize the risk, and analyze the consequences of disruption
2. Understand and develop metrics that can be used to measure improvement
3. Research technical solutions
4. Work with the stakeholders in industry, government, and the research community to transfer the knowledge gained and technology developed

Tools currently under development and evaluation include:

DEADBOLT — source code checking tool

SHARP — Security-Hardened Attach Resistant Platform (formerly called the “HSMTU”)

SecSS — Security Services Suite

RiskMap — tool for building a business case for investing in security

APT — Access Policy Tool

EMERALD — intrusion detection and event correlation for PCS

CDIS — prototype for demonstrating secure information sharing

WORKING WITH INDUSTRY

The research team is working with industry to understand their security needs and to develop appropriate scenarios for testing and evaluating the results of the project. Industry participates in project reviews and the team uses the feedback to update their work direction. The team has hosted three workshops with industry: June 2005, November 2005, and June 2006 to present and discuss the work with the key stakeholders.

ACCOMPLISHMENTS TO DATE

Prototype tools are being demonstrated in a “typical” oil and gas architecture test bed, at conferences, and at stakeholder sites.

Partnerships with PCS vendors are underway to forge paths for technology transfer. Publications, technical reports, and presentations are available on the following topics: risk characterization, interdependences, metrics, tools, and secure information sharing. Classes in PCS security are being introduced by a number of the member institutions and these seminars are being made available to industry.

Information about the project may be found at www.thei3p.org/research/scada/index.html

I3P Publications may be found at www.thei3p.org/about/publications.html

Points of Contact:

Project Director: John Cummings, jccummi@sandia.gov (505) 845-9937

Project Leader: Ben Cook, bkcook@sandia.gov (505) 844-3795

I3P Assistant Director for Research & Analysis : Eric Goetz, egoetz@thei3p.org (603) 646-0692