

# Survivability and Recovery of Process Control Systems



Institute for Information  
Infrastructure Protection

## A Critical Challenge

Process Control Systems (PCS) are crucial to the safe, reliable and efficient operation of critical infrastructures throughout the United States and other parts of the world. These computerized systems, which typically rely on a dispersed network of electronic sensors and other smart devices, drive complex industrial processes (including petrochemical refineries and electric grids) with remarkable reliability and efficiency.

But their reliability comes at a cost: many older PCS function with few, if any, security mechanisms. PCS are thus vulnerable to the numerous cyber threats—both malicious and inadvertent—that afflict our digital world. To complicate matters, PCS increasingly rely on off-the-shelf components and well-known protocols to facilitate communication within their corporate network and also with the Internet. Such systems, while inexpensive and time-tested, are unfortunately familiar—and therefore accessible—to attackers, who can change settings, leading to industrial failure or worse.

Not surprisingly, the survivability and recovery of PCS has emerged as an area of paramount concern to national security. PCS need to be made more secure, equipped with the ability to detect and deflect intruders, and at the same time able to nimbly recover in the event of a system malfunction.

## Project Overview

With support from the Institute for Information Infrastructure Protection (I3P), researchers from eight leading academic institutions, federally-funded labs and non-profit organizations across the U.S. are engaged in an intense effort to increase PCS resiliency and strengthen the nation's critical infrastructures.

*The Survivability and Recovery of Process Control Systems* project represents the first concerted effort to make PCS broadly resistant to cyber disruption. Researchers are developing processes and technologies to harden security and allow PCS to operate despite internal and external attacks and operator error.

Integrated into the industrial life cycle, these tools will not only preserve efficiency but will enable PCS to quickly recover should a disruption occur. In addition, *Survivability and Recovery* researchers are developing a suite of tools and technologies with long-term versatility that can rapidly adapt to a shifting cyber landscape, work with both legacy systems and next-generation PCS, and function within a range of industrial environments.

Moreover, because the project evolved from an earlier I3P initiative on vulnerabilities in control systems security, it benefits from an existing cadre of tools, methodologies, expertise, and relationships. Collectively, the two projects embody a wealth of critical findings relevant to the security and economic well-being of the U.S. "Infrastructure operators, who understand the seriousness of a system malfunction, frequently cite the survivability and recovery of process control systems as an area of paramount concern," says Charles Palmer, Chair and Director of Research at the I3P.

The Institute for Information Infrastructure Protection (I3P) is a national consortium of leading academic institutions, federally-funded laboratories, and non-profit organizations dedicated to strengthening the cyber infrastructure of the United States.



Infrastructure operators, who understand the seriousness of a system malfunction, frequently cite the survivability and recovery of Process Control Systems as an area of paramount concern.

## Team Members

MIT Lincoln Laboratory  
MITRE Corporation  
Pacific Northwest National  
Laboratory  
Sandia National Laboratories  
SRI International  
United States Military Academy  
University of Tulsa  
University of Illinois at  
Urbana-Champaign

## Working with Industry

Researchers are reaching out to industry partners from the planning to the implementation stages to make certain their proposed solutions meet real world security needs. To impart knowledge and facilitate technology transfer, researchers also regularly host workshops and interactive tool demonstrations for stakeholders.

An advisory board of industry experts is working with the team, including:

- Steve Elwart, Director of Systems Engineering, Ergon Refining Inc.
- Eric Cosman, Engineering Solutions Architect, The Dow Chemical Company
- Morgan Henrie, Consultant, Alyeska Pipeline Service Company
- Scott Crane, Manager of IT Compliance at the Williams Companies, Inc.
- Bob Huba, Senior Product Manager, Emerson Process Management
- Perry Pederson, Vice President, Wurldtech Labs

Overall, *Survivability and Recovery* researchers are joining forces with industry partners to devise solutions that meet PCS security needs, work with the industrial life cycle and are functionally attractive to operators of critical infrastructures.

## Making an Impact

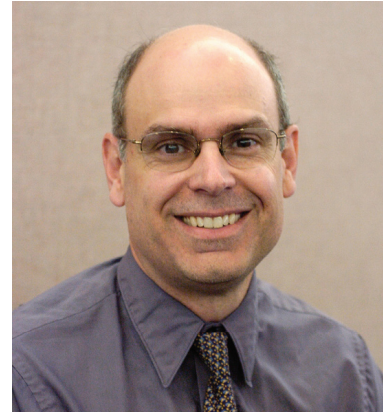
The goals of the *Survivability and Recovery of Process Control Systems* project are to:

- Provide operators with a tool for identifying mission-critical network nodes, enabling them to prioritize their PCS security efforts
- Ensure every significant human-issued control has been unobtrusively authenticated
- Develop tools to track and monitor the activities of MODBUS networks without disrupting normal operations
- Develop software that specifies, implements and enforces policies to keep intruders out
- Develop a simulator to allow operators to safely explore responses to a cyber event
- Partner with industry to ensure stakeholder needs are met and that developed technologies will be readily adopted
- Track other PCS research projects in the U.S. and share the information gathered with government and industry stakeholders

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.



Institute for Information  
Infrastructure Protection



“Automated process control systems represent a nexus between the cyber and physical worlds, controlling and regulating key industrial processes with great efficiency. Unfortunately, the growing inter-connectivity of these systems increases the risk of cyber attack. Devising ways to allow the systems to operate safely and efficiently is a crucial challenge.”

Robert Cunningham  
MIT Lincoln Laboratory  
and Team Leader

Information about the project can be found at:

[www.thei3p.org](http://www.thei3p.org)

or by contacting  
Robert Cunningham,  
Team Leader at  
[rkc@ll.mit.edu](mailto:rkc@ll.mit.edu)  
or  
Charles C. Palmer,  
I3P Director for Research at  
[charles.c.palmer.@dartmouth.edu](mailto:charles.c.palmer.@dartmouth.edu)

The I3P is managed by Dartmouth College

