ISRCS 2008

I3P

Zach Tudor
SRI International

September 9-10, 2008
Idaho Falls, Idaho

Survivability and Recovery of Process Control Systems

Zach Tudor, SRI International
Team: MITRE, PNNL, SNL, SRI, UIUC, UTulsa, USMA

1st International Symposium on Resilient Control Systems
September 2008

This material is based upon work supported by the U.S. Dept. 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.

The I3P is managed by Dartmouth College

What Is The I3P?
The Institute for Information Infrastructure Protection

- A national consortium of 27 leading universities, national laboratories and non-profit institutions dedicated to strengthening the cyber infrastructure of the United States
- Managed by Dartmouth College with oversight from DHS
- Established in 2001 to identify and address critical research problems facing our nation's information infrastructure

The Institute for Information Infrastructure Protection

A consortium of leading universities, national laboratories and non-profit institutions dedicated to strengthening the cyber infrastructure of the United States

The I3P

- Helps secure critical infrastructures by identifying vulnerabilities and devising technical solutions
- Conducts cutting-edge research in cyber security
- Partners with industry to meet real-world needs
- Brings multi-disciplinary focus to broad-ranging issues
- Hosts regular workshops to engage and educate stakeholders

27 Member Consortium

* Academic members – 19
* National Laboratories – 5
* Non-Profit Organizations - 3

Research

Process Control Systems

Business Rationale

Digital Identity

Insider Threat

This is I3P's 2nd Program on PCS Security

ISRCS 2008

Team Roles and Responsibilities

ISRCS 2008

Mgmt | **Technical R&D** | **Outreach**

Lead Project

- Regular T-cons
- Quarterly Meetings
- Annual Workshops

Technical R&D

- Application Survivability
- ID Critical Components
- Single Platform Survivability
- Policy-based Evaluation and Enforcement
- Situational Awareness of MODBUS Systems
- Survivability and Recovery

Outreach

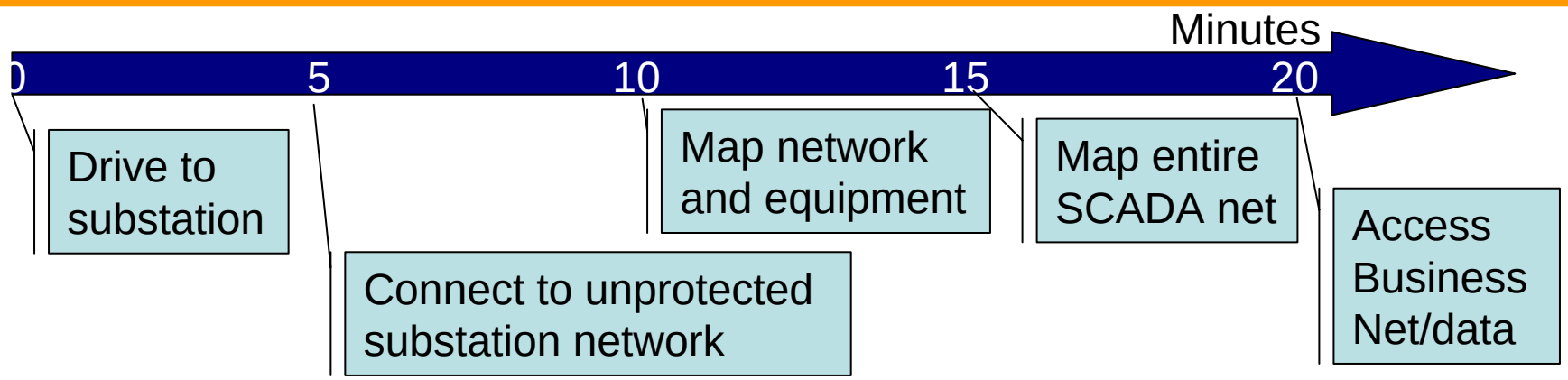
Engage Industry

Engage Academia

- Technology Transfer to Industry
- PCSF-Related Workshops and Tools

- Periodic Publications
- Conference Papers
- Gap Report to DHS

How Vulnerable Are We?



- Early penetration tests succeeded easily: In 2002 Rainbow Mykotronx assessed a southwestern utility serving 4,000,000 customers
- Today: Best practices are being established
  - Commercial tools available (firewalls, etc.)
  - Company networks better protected
- But research and development tasks remain
  - Defense in depth needed, but hard to do right (business, technical)
  - PCS-specific protocols and services not yet protected
- The Threat Grows: Hackers and others have noticed weaknesses

* "SCADA vs. the hackers, Can freebie software and a can of Pringles bring down the U.S. power grid?," Alan S. Brown, Mechanical Engineering, http://www.memagazine.org/backissues/membersonly/dec02/features/scadavs/scadavs.html

A Growing Concern

ISRCS 2008

Gov't

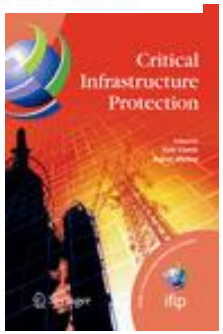
- DHS, DOE and the I3P have established a program in securing PCNs
  - National SCADA testbed (NSTB)
  - Process Control Systems Forum
  - Operator cyber security training underway

Industry

- Associations expanding security to include cyber security
  - American Petroleum Institute/NPRA
  - SANS Process Control and SCADA Summit
  - S4: SCADA Security Scientific Symposium
  - I3P Workshop on PCS Security

Academia

- Programs, conferences exploring new security ideas
  - UC San Diego Control Systems Security Curriculum
  - IFIP Conference on Critical Infrastructure Protection



Government, Industry and Academia are moving to address the issue.

Common Strategies To Secure PCS*

ISRCS 2008

*Derived from NERC, *Critical Infrastructure Protection Cyber Security Standards*, CIP-001-1 to CIP-009-1, http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection, 2006.

1. Identify critical infrastructure components
2. Develop a cyber security policy
3. Control access
   - Physical access control (locks, fences, “six wall” defenses)
   - Cyber access control (authenticate users, limit connections, reduce vulnerabilities)
4. Monitor access and use
   - Record physical and electronic access and use
   - Continuously analyze configurations
5. Plan to respond and recover
   - Backup plans and verification
   - Roles and responsibilities in an emergency
6. Train personnel to understand responsibilities and plans

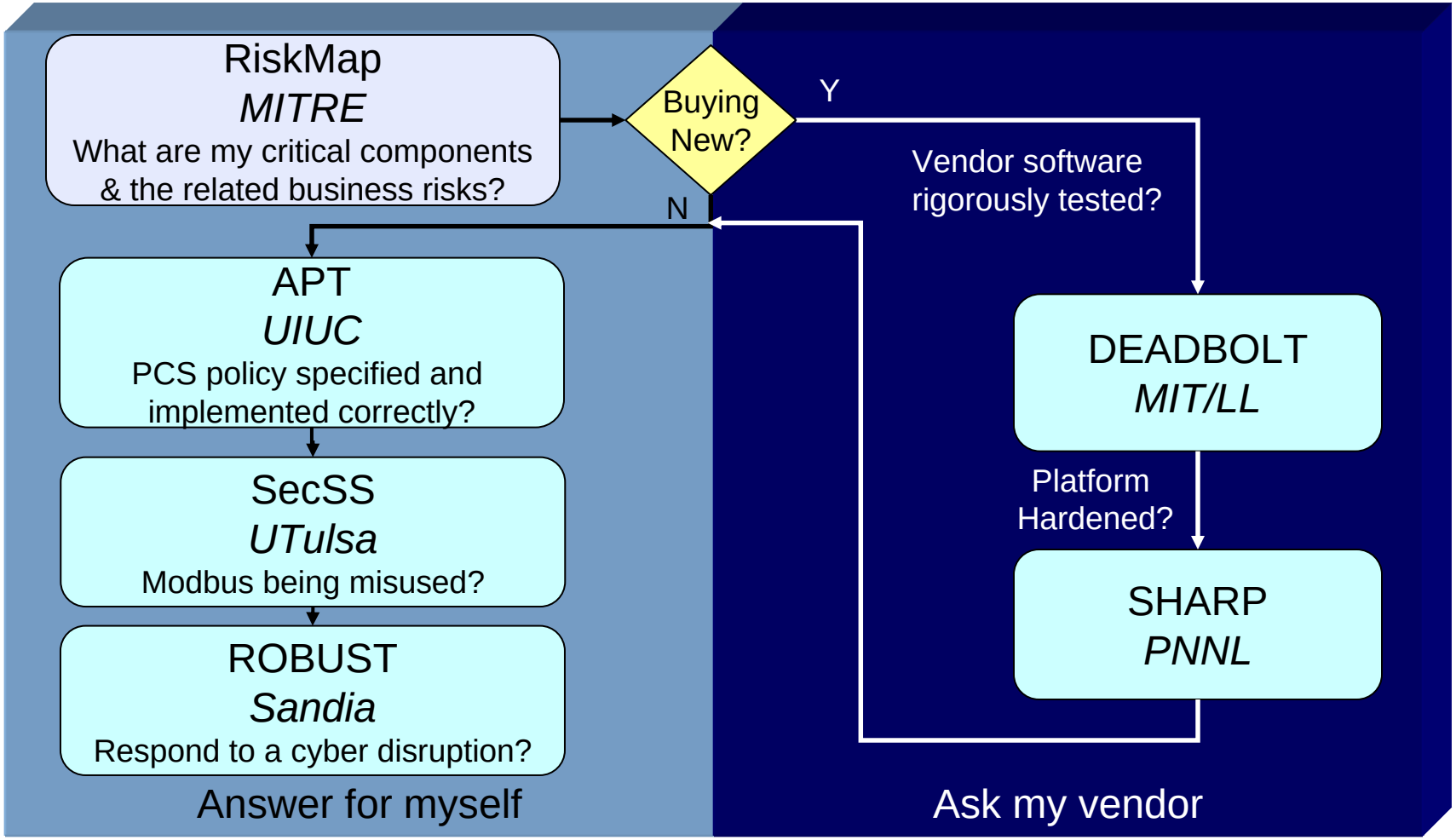
Approaches are understood but tricky to implement–
Refined processes and tools are needed.

PCS Program Objectives

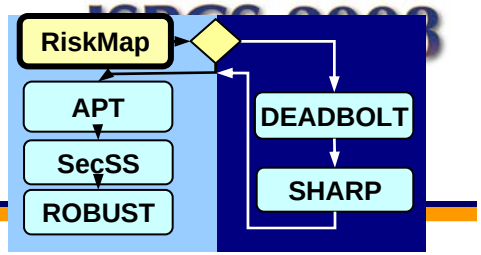
ISRCS 2008

- Identify critical infrastructure components
- Reduce the opportunity for an attack
  - Limit network and host access: Specify, implement and enforce policy that results in survivable operations
  - Ensure survivability of legacy and future platforms and applications
- Increase the likelihood of detection if such an attack is made
  - Establish situational awareness of MODBUS networks
- Ensure that operators can effectively respond and recover
- Ensure relevance
  - Limit duplication of effort
  - Work for tech transfer of best systems

I3P Tools Answer Difficult Operator Security Questions Simply

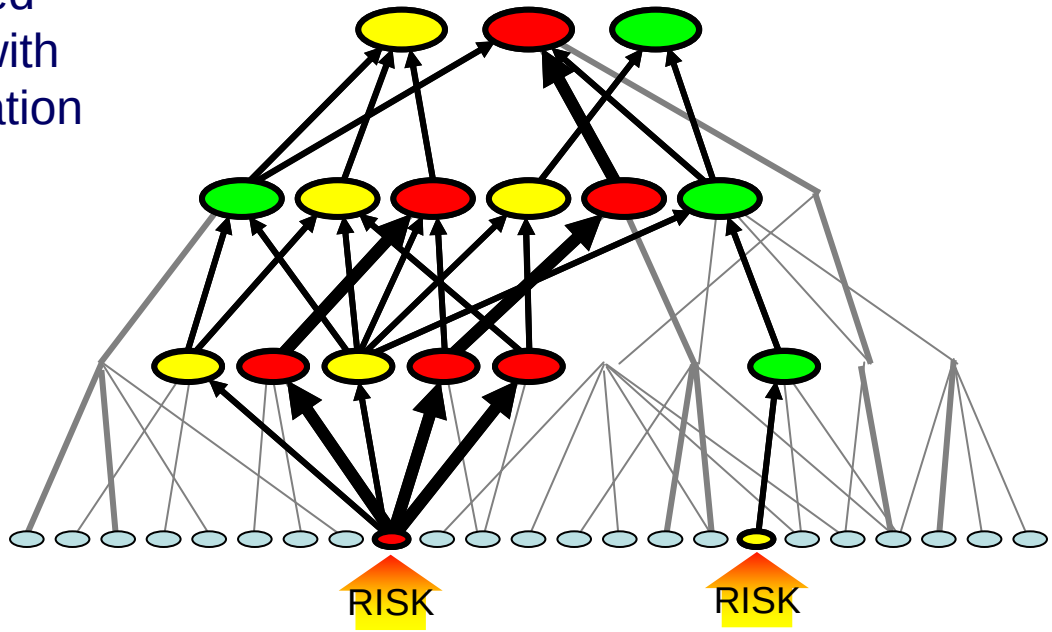


RiskMAP



- A process for assessing PCS network risk <u>and translating the results</u> into terms meaningful to corporate-level managers

- RISKMAP provides a structured way to link mission objective with operational tasks, with information assets, with network nodes.



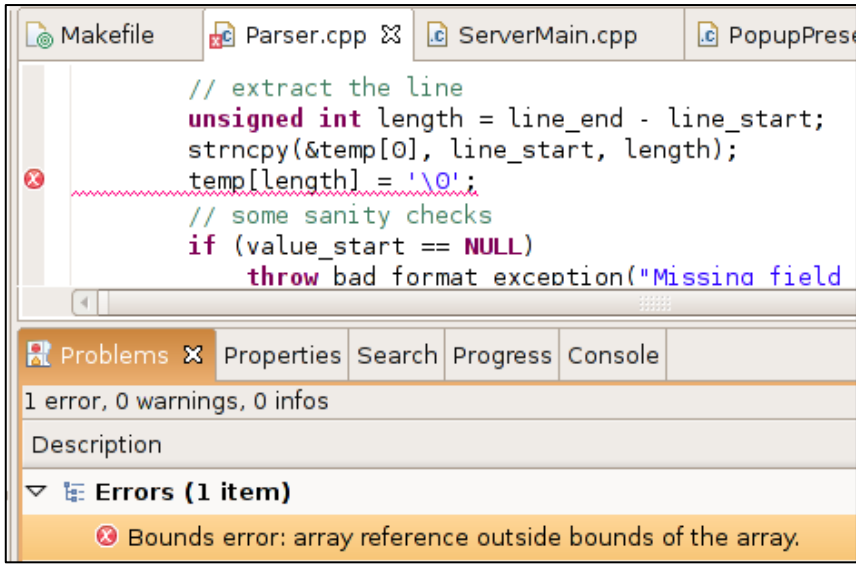
Risk Follows Dependency Paths

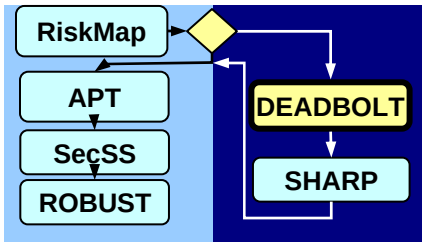
DEADBOLT

ISRCS 2008

Adaptive Testing Tool Suite

- Analyzes and tests C and C++ software
- Automatically creates failure-inducing test cases
- Determines exact problem location
- Leverages existing tools and environment familiar to developers
- Detects memory corruption
  - Buffer overflows
  - Double-free errors
  - NULL-pointer dereferences
- Detects resource exhaustion
  - Memory leaks (current research)
  - Mismanagement of files, sockets, locks, etc (future work)
- More Information
  - Michael Zhivich mzhivich@ll.mit.edu at MIT Lincoln Laboratory

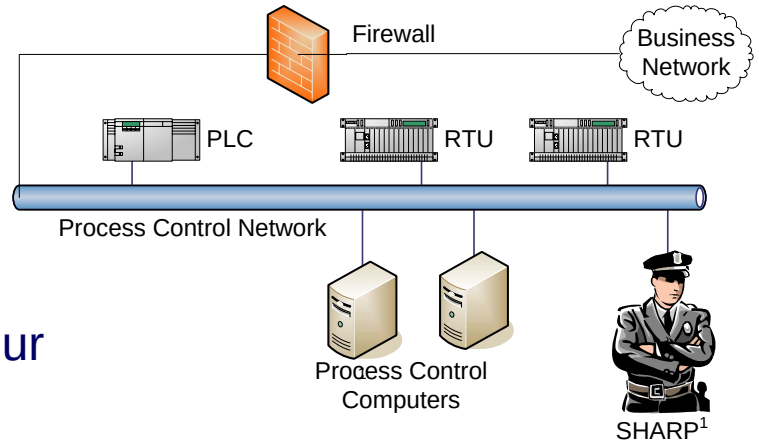


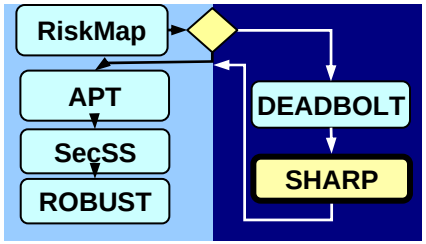


SHARP

The Security-Hardened, Attack Resistant Platform

- SHARP is a hardware appliance that is designed to plug into existing PCS control computers and provide an attack resistant environment
- Protection for a High-Value Asset Computer
- Policy enforcement – Mitigation of Insider attack
  - Two-factor Authentication
  - HMI/MTU hardware I/O routed through SHARP for policy enforcement and then passed via Ethernet
- Active resource modification detection and restoration – Protection against zero-day and day-after attacks
  - File Monitor
  - Process Monitor
- Mitigation of Denial of Service attacks
  - Network Monitor/ Data Flow Throttling
- Talk to PNNL about adapting SHARP to your Process Control Network applications
- Licensing opportunities and collaborations: Ron Pawlowski ron.pawlowski@pnl.gov



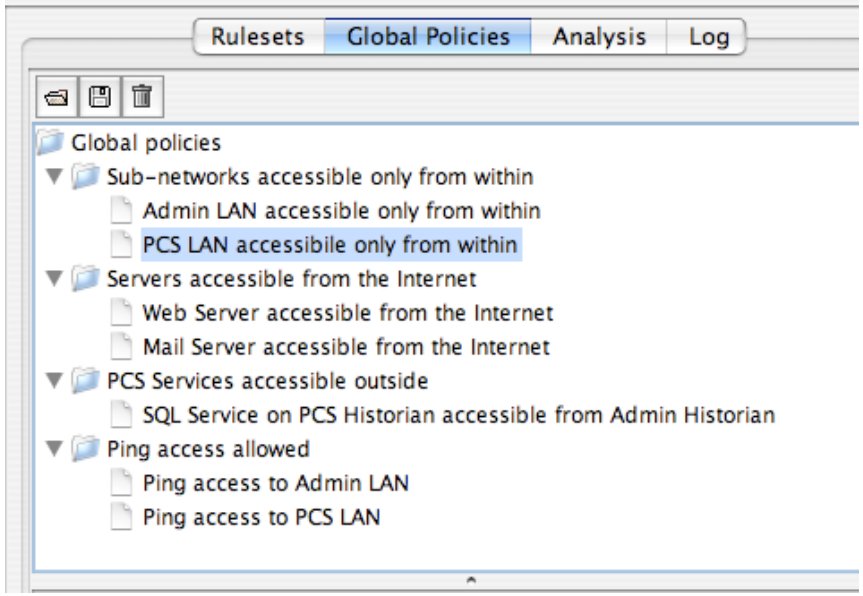


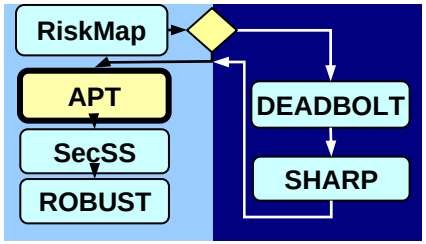
The Access Policy Tool (APT)

ISRCS 2008

- Access in networked process control systems controlled by configuration of many policies
- Misconfiguration is a major source of security vulnerabilities
- APT analyzes security policy *implementation* for conformance with global security policy *specification*
  - Integrates policy rules (configuration information)
  - Comprehensive offline analysis
  - Dynamic online analysis of incremental configuration
- APT ensures that global access constraints are reflected in the configuration
- More Information
  - Bill Sanders (whs@uiuc.edu) or David Nicol (nicol@crhc.uiuc.edu)

  http://www.perform.csl.uiuc.edu/apt/

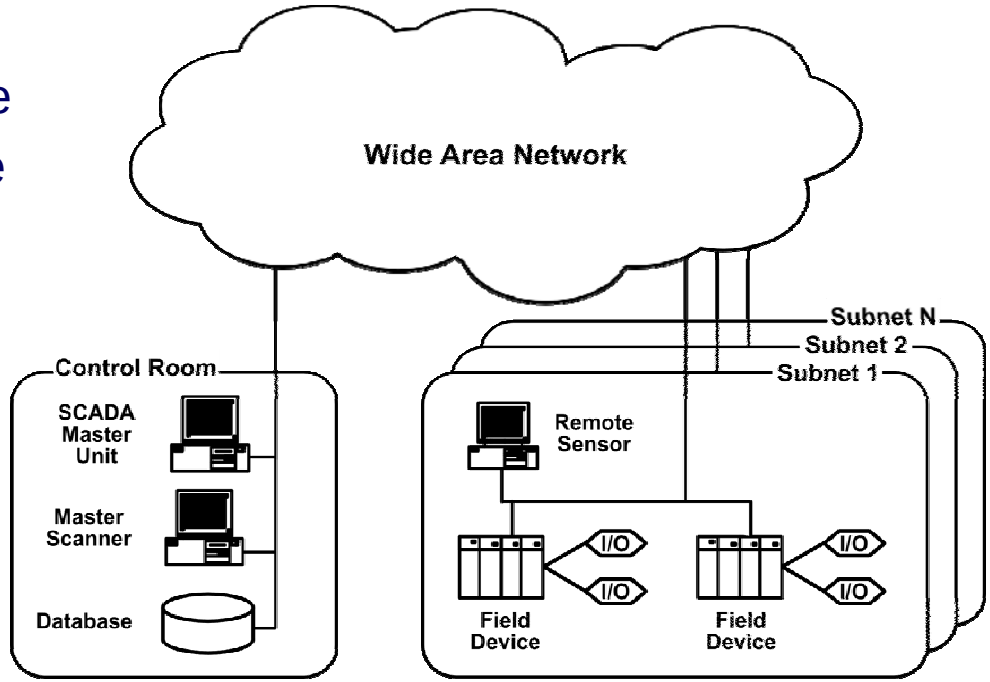


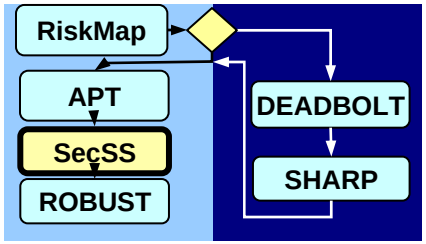


SecSS: Monitoring Tools for Process Control Networks

- LAN/WAN level monitoring for SCADA protocols over TCP (Modbus and DNP3)
- Reduce risk of RTUs that may not respond well to certain TCP/IP messages
- Centralized command and storage
- Scalable/Distributable architecture
- Low impact
  - Sensor operation and communication can be scheduled
  - Sensors only transmit when new data is available
- For more information

  Mauricio Papa
  mauricio-papa@utulsa.edu



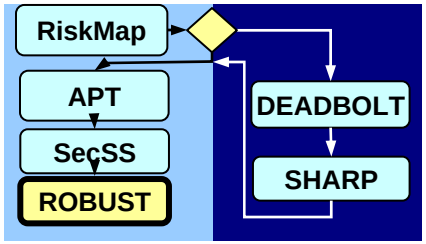


ROBUST: A Concept of Operations to Ensure System-Level Survivability and Recovery

- Developing system survivability methodology and codifying it in a response planning tool called ROBUST
- Implementing ROBUST prototype and validating it with disruption scenarios on Sandia test bed
- Developing knowledge base and hands-on demonstration
- Sandia is building on previous work in LOGIIC, which looked solely at situational awareness (no response component)

More Information

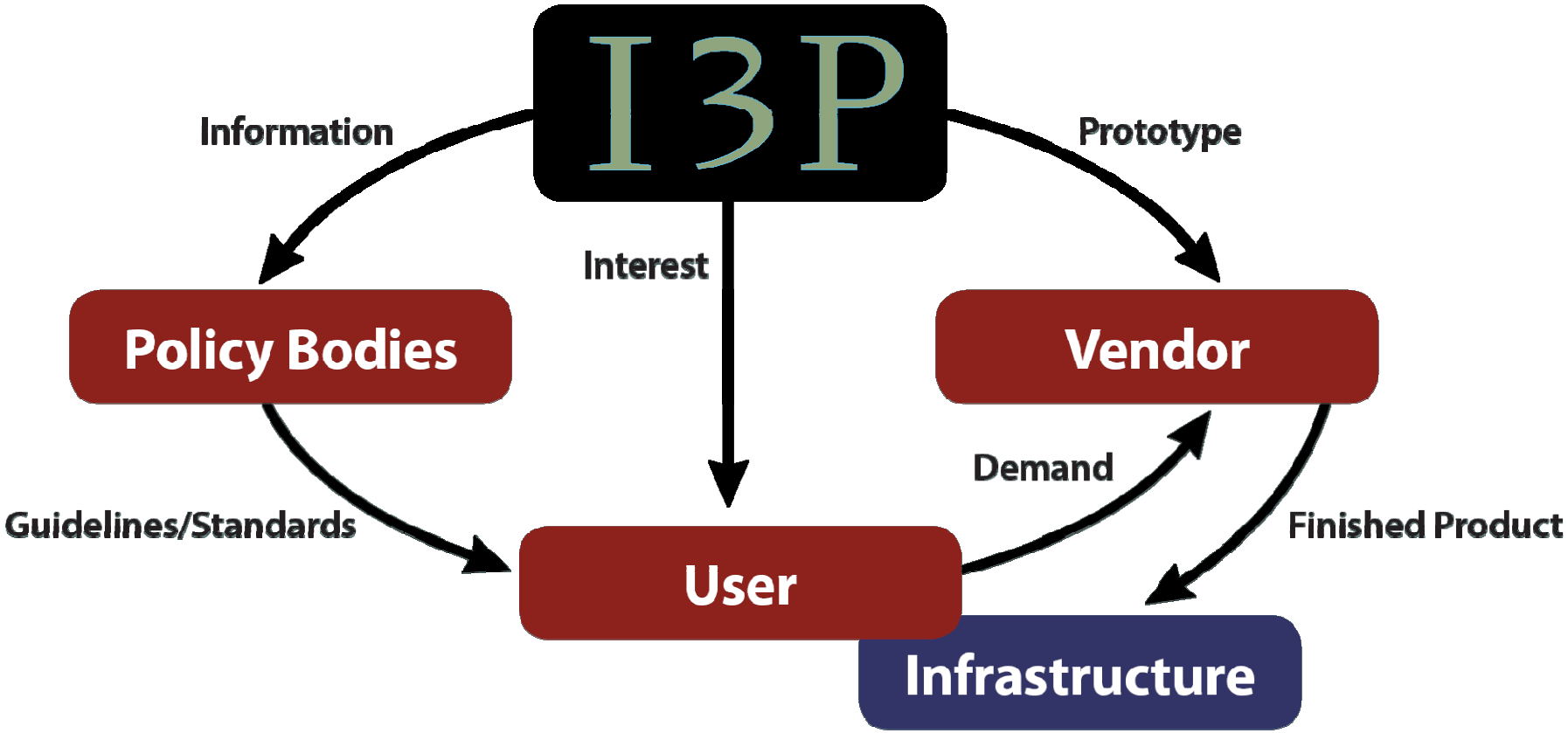
– Bryan Richardson
btricha@sandia.gov
at Sandia National Laboratories



Need for Organized Tech Transfer

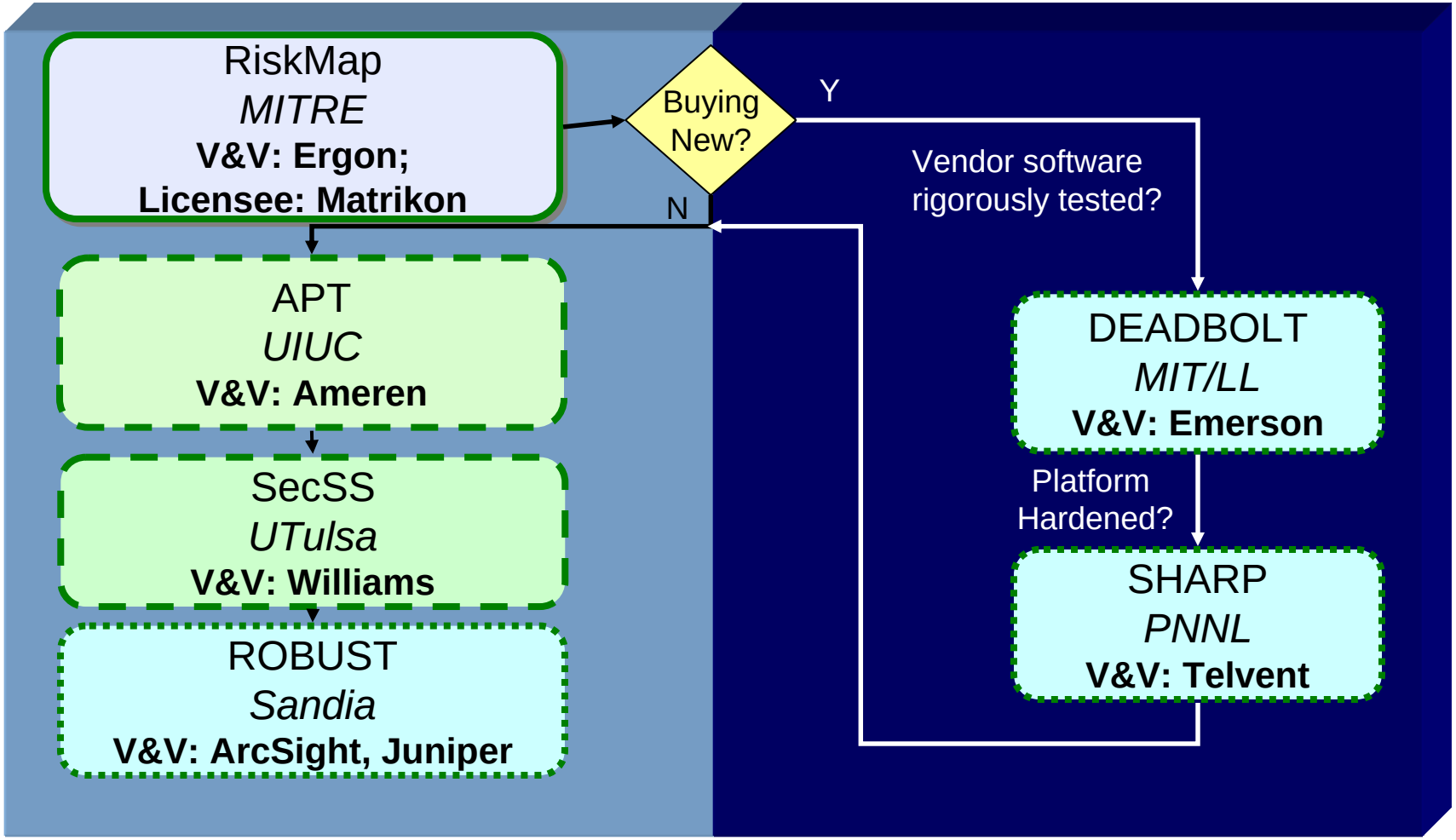
- Transfer of knowledge and technology from academia to industry is often a slow and haphazard process
- Results and tools developed by the I3P team will make a difference only if they are applied by operators of critical infrastructure
- To be considered for deployment, solutions must match the needs and requirements of infrastructure operators and make a compelling business case
- Tech transfer activities need to be coordinated across this multi-institution team, to optimize ROI on:
  - Time contributed by industry partners
  - Federal R&D funding
  - Dedicated efforts by the team members

Tech Transfer Strategy



SRI helps the team coordinate outreach to users, vendors, and policy bodies

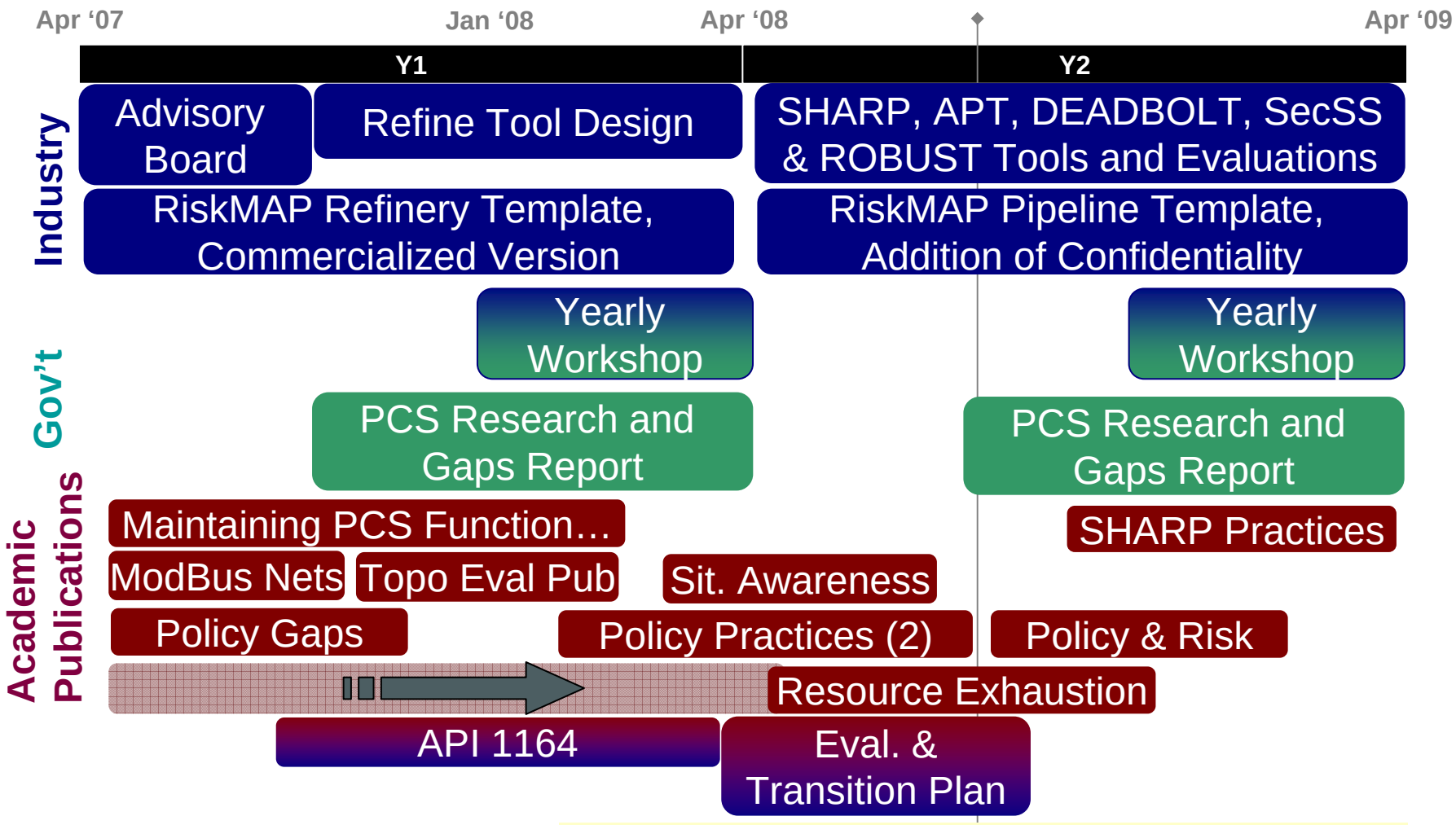
I3P Tools Are Being Commercialized and Verified by Operators and Vendors



Reference to any specific commercial product, trade name, trademark or firm does not constitute or imply endorsement.

Commercial Version | Vendor V&V Support | Operator V&V Support

Deliverables and Schedule



Mostly on schedule.

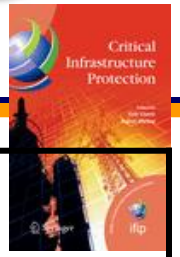
Success Metrics Status (1 of 2)

ISRCS 2008

10 Academic Research Papers (4 in press)

10 Industry Presentations (7 performed)

5 Invited Presentations (8 performed)



Goals:

Aug. Y1	Emerson Global Users Exchange: I3P PCS Booth
Oct. Y1	NPRA Cyber Security Round Table: *Making a Case for Cyber Security in the Company's Budget* ISA: I3P PCS Booth
Nov. Y1	API Training: *The I3P Control Systems Security Awareness and Education Course: Understanding Cyber Risks and Mitigation Strategies* UVA-I3P Workshop on investing in Cyber Security **API IT Security: *US Government Perspective on Process Control/SCADA Systems*** **API IT Security: *Keeping your Enterprise Running: Strategies for Securing Interconnected Critical Infrastructure Networks***
Jan. Y1	***S4: Maintaining PCS Functionality Despite an Active Cyber Exploitation*** ***Northeastern Entretech Forum: Securing Process Control Systems*** ***SANS Process Control & SCADA Security Summit 2008: The Most Valuable Research Projects in SCADA Security***
Feb. Y1	***SANS: A Practical Approach to Cyber Security within Control System Environments***
Mar. Y1	***NPRA: Cyber Security Workshop: Where are We Now?*** ***NPRA: Cyber Security Workshop: Coming to the Table of Cyber Security*** ***ISSA: Control System Security and System Survivability*** ***IFIP: Attack Taxonomies for the Modbus Serial and TCP Protocols*** ***IFIP: Assessing the Integrity of Field Devices in Modbus-Based Pipeline Control Networks*** ***IFIP: Application of Trusted Network Technology to Industrial Control Networks***

Success Metrics Status (2 of 2)

- Tools evaluation plans in development and/or execution
  - Validation: Will the tool meet the need?
  - Verification: Is the tool built as specified?
- Regular Interactions with DHS, industry advisory board (IAB)
  - ✓ DHS: June, Sept., Nov., Dec.
  - ✓ IAB: Sept., Dec.
- Two workshops run
  - ✓ First will be with co-located with NPRA
- Stretch goal: Get tools into the hands of asset owners
- Added: Five separate instances of protected intellectual property

Summary

- Process control systems connect the computer and physical worlds
  - These systems are vulnerable
  - Adversaries have taken note
- Two-track approach is needed now
  - Educate asset owners to secure their process control networks
  - Assist vendors in developing more secure components
- Longer range research is also needed, being pursued
- I3P Consortium members have developed and are commercializing new tools in this space

Thanks for Your Time!!

I3P Institute for Information Infrastructure Protection
www.thei3p.org

Survivability and Recovery of Process Control Systems

THE CHALLENGE

Process control systems (PCSs) are instrumental in the safe, reliable, and efficient operation of critical infrastructures such as gas pipelines and electrical grids. However, most PCSs in use today are connected to the Internet, exposing critical infrastructures to established and emerging cyber threats.

PROJECT OVERVIEW

The I3P brings together leading research and development organizations to make control systems more resilient and to allow for rapid recovery in the case of inadvertent or intentional disruption.

PROJECT GOALS

The I3P will develop and demonstrate procedures and technologies that allow owners and operators to continue providing services in the presence of a cyber-related disruption. Tools developed by the I3P will enable better protection, situational awareness, and rapid recovery of systems during and following cyber-related disruption.

TEAM MEMBERS

SRI International · Illinois · Sandia National Laboratories · Lincoln Laboratory Massachusetts Institute of Technology · MITRE · Pacific Northwest National Laboratory · CIS

RESEARCH OBJECTIVES

1. Track and leverage R&D efforts for government and industry.
2. Identify critical assets to better plan for PCS survivability.
3. Ensure survivability of legacy and future platforms.
4. Specify, implement, and enforce policy that results in survivable operations.
5. Establish situational awareness of MODBUS networks.
6. Ensure system-level survivability and recovery.
7. Work with industry to ensure that research is on the proper path and that technical transition is happening smoothly.

STRATEGY FOR TECHNOLOGY TRANSFER

ABOUT I3P

The Institute for Information Infrastructure Protection (I3P) is a national consortium of leading academic institutions, federally-funded labs, and non-profit organizations dedicated to strengthening the cyber infrastructure of the United States. For more information about this project, contact Robert Cunningham, Project Leader, at rkc@ll.mit.edu.

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. December 2007

ISRCS 2008

I3P

Zach Tudor	**zach.tudor@sri.com**	**(703) 247-8717**