Process Control Systems Industry Conference

Survivability and Recovery of Process Control Systems

Project Leader: Robert Cunningham, MIT Lincoln Laboratory
Presented by Ulf Lindqvist, SRI International
Process Control Systems Industry Conference, August 28, 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.

Copyright © 2008 by the Trustees of Dartmouth College. The I3P Logo is a trademark of Dartmouth College.
All information contained in this document may not be reproduced without permission by the I3P.

I3P
Institute for Information Infrastructure Protection

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

What does the I3P do?

- **Helps secure critical infrastructures by identifying vulnerabilities and devising technical solutions**
- **Conducts cutting-edge research in cyber security**
- **Current research programs:**
  - Business Rationale for Cyber Security
  - Safeguarding Digital Identity
  - Human Behavior, Insider Threat and Awareness
  - Security Incentives through Risk Pricing
  - **Survivability and Recovery of Process Control Systems**
- **Partners with industry to meet real-world needs**
- **Brings multi-disciplinary focus to broad-ranging issues**
- **Hosts regular workshops to engage and educate stakeholders**

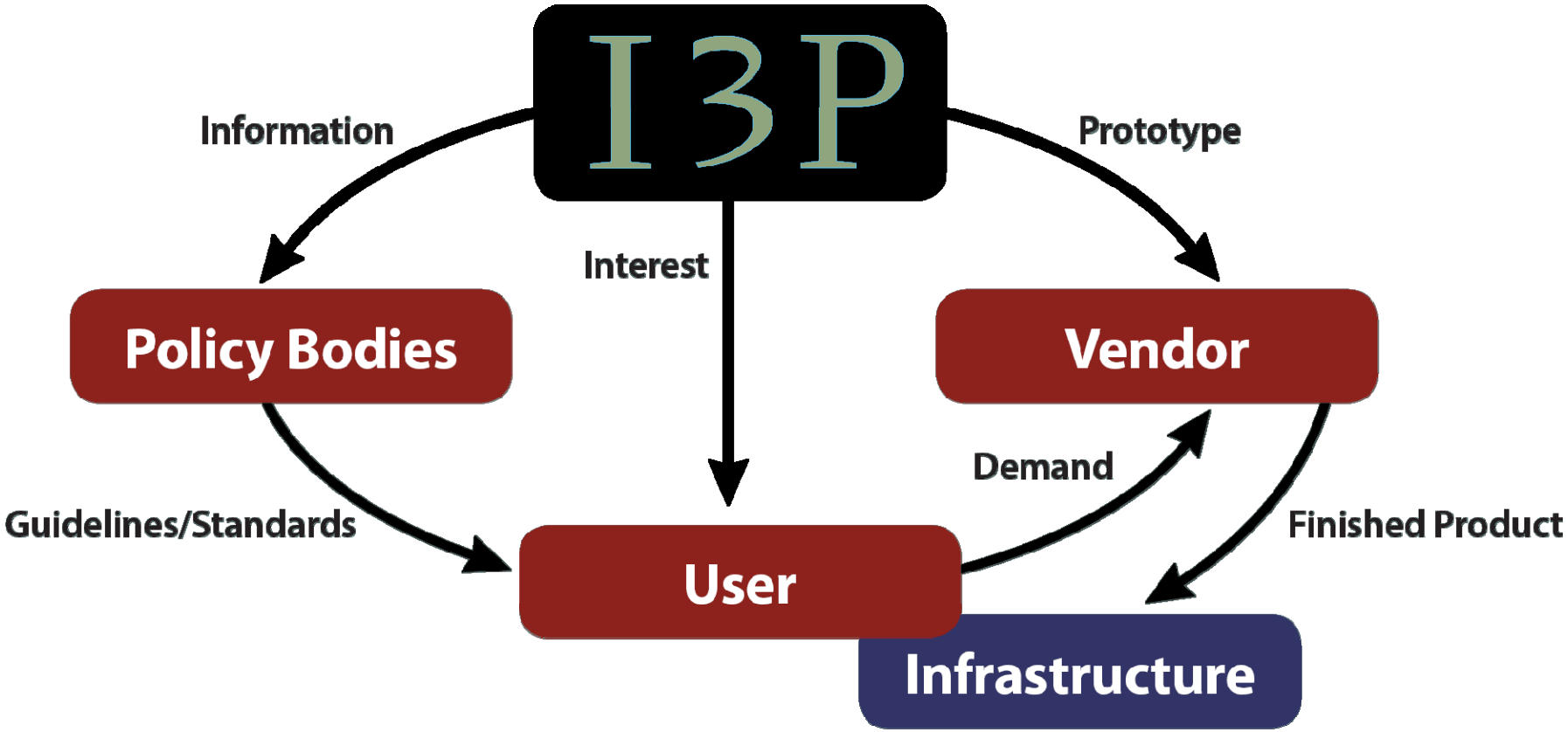
This is I3P's 2nd Program on PCS Security

I3P Institute for Information Infrastructure Protection

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 <u>make a difference</u> only if they are applied by operators of critical infrastructure**
- **To be considered for deployment, solutions must match the <u>needs and requirements</u> of infrastructure operators and make a compelling <u>business case</u>**
- **Tech transfer activities need to be <u>coordinated</u> 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

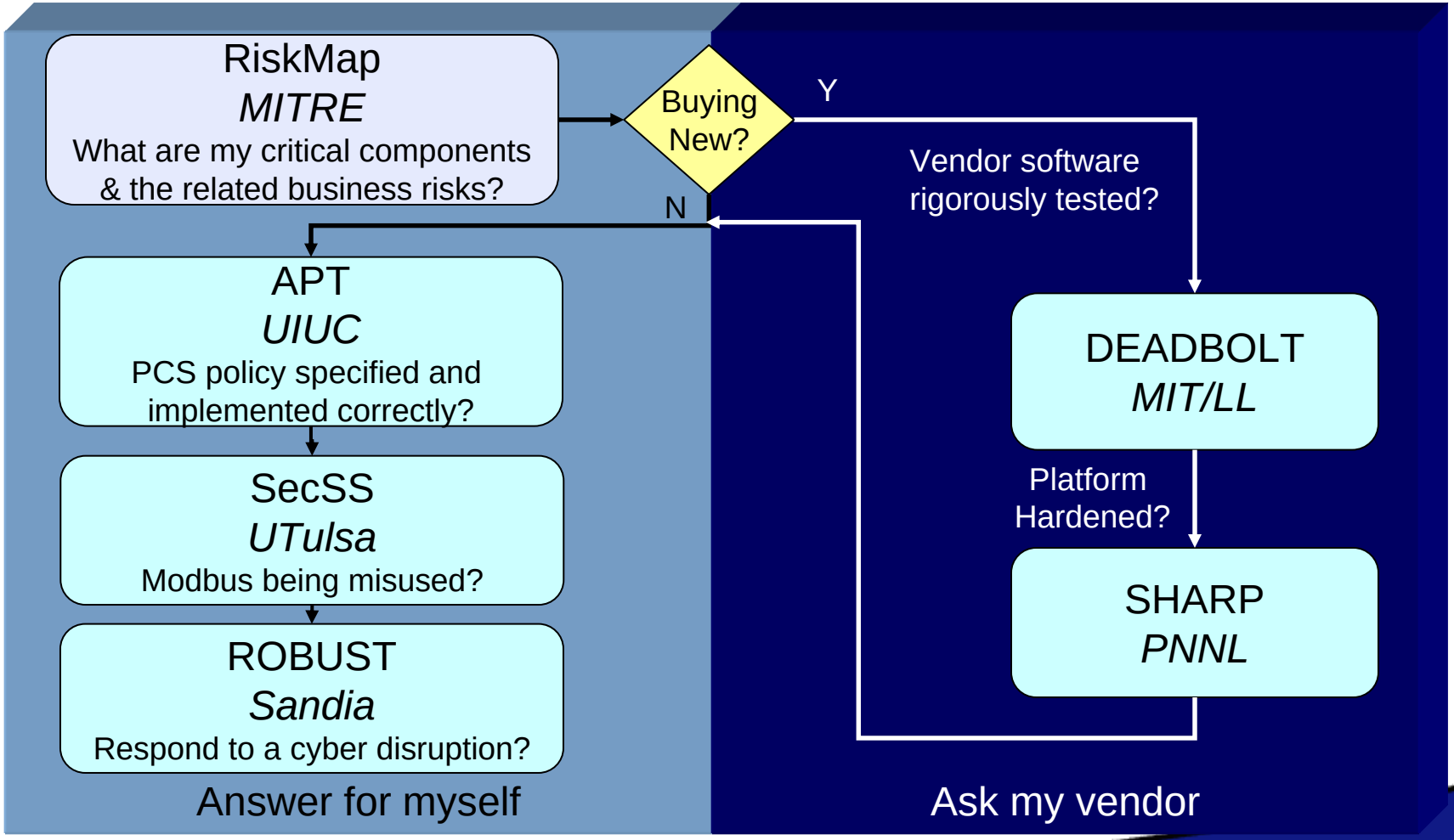
Common Strategies To Secure PCS*

*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.

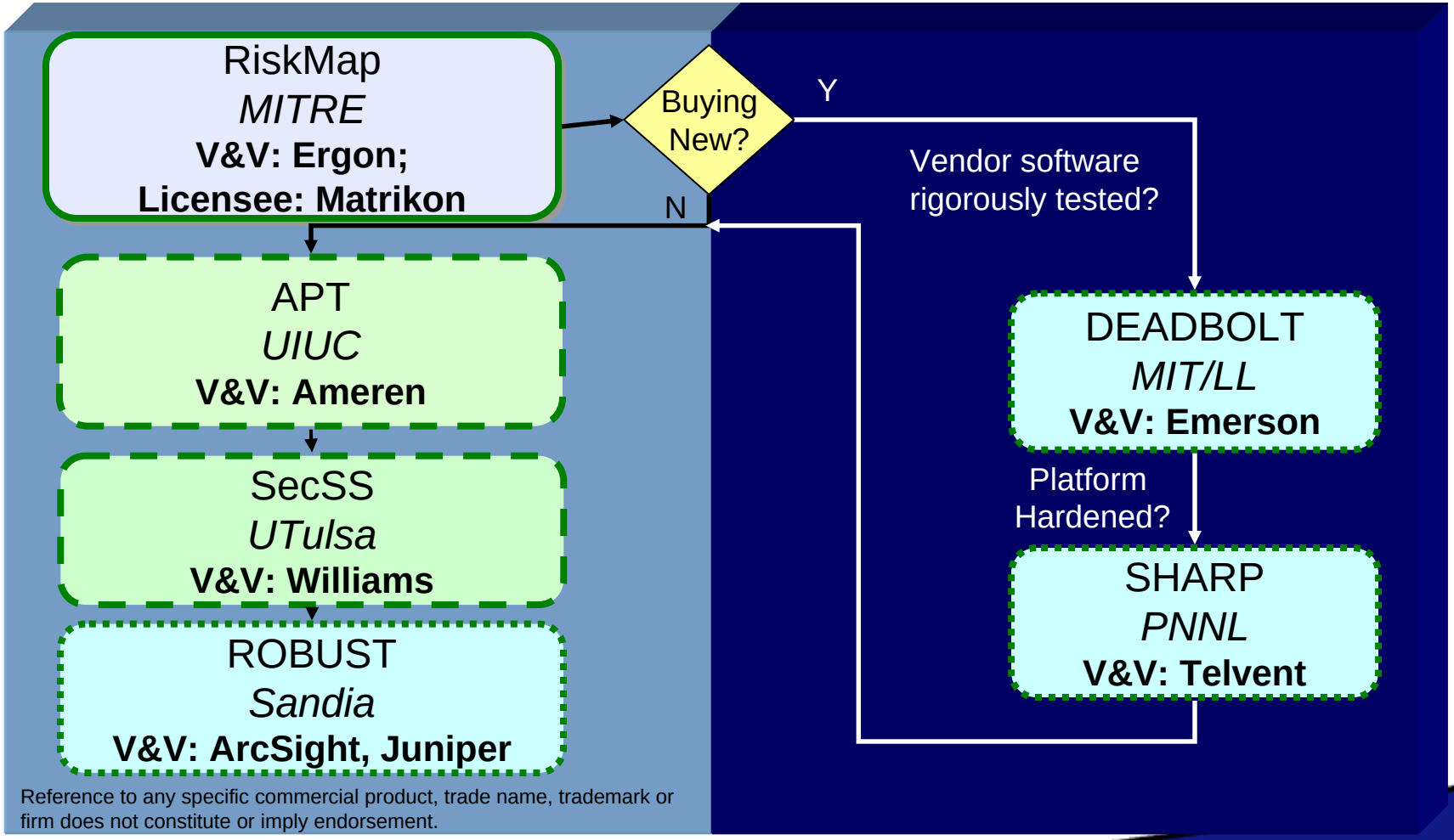
1. **Identify critical infrastructure components**
2. **Develop a cyber security policy**
3. **Control access**
   - Physical access control (locks, fences, "six wall" defenses)
   - Cyber access control (authenticate users, limit connections, reduce vulnerabilities)
4. **Monitor access and use**
   - 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.

I3P Tools Answer Difficult Operator Security Questions Simply



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.

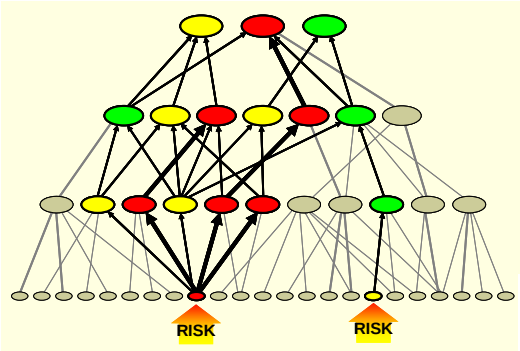
Commercial Version

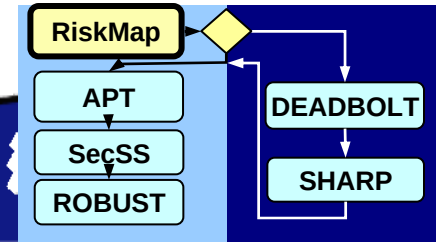
Vendor V&V Support

Operator V&V Support

RiskMAP

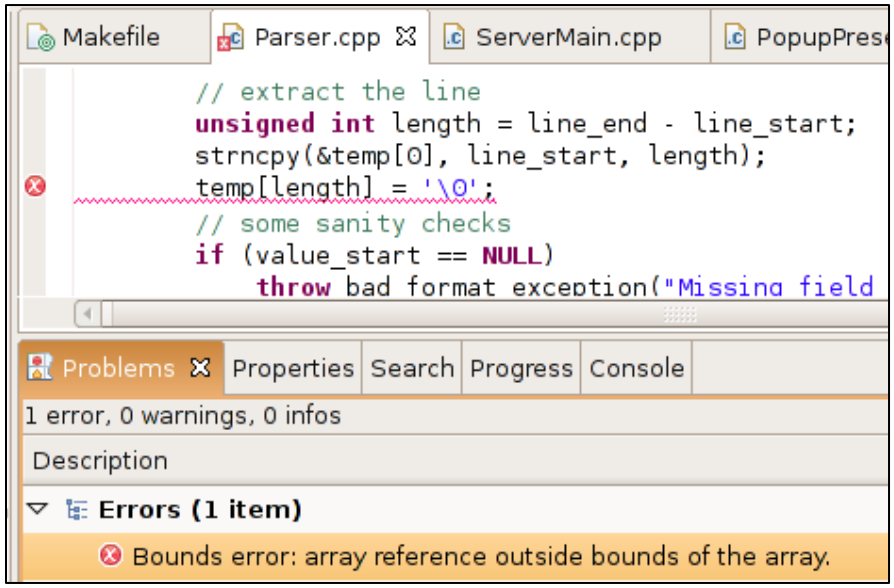
- A process for assessing PCS network risk <u>and translating the results</u> into terms meaningful to corporate-level managers
- See the next presentation by Jim Watters

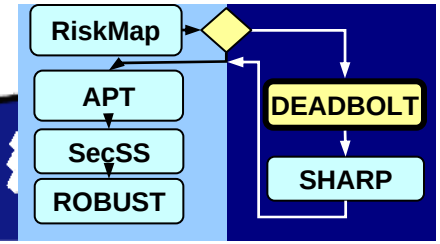




Adaptive Testing Tool Suite

- **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

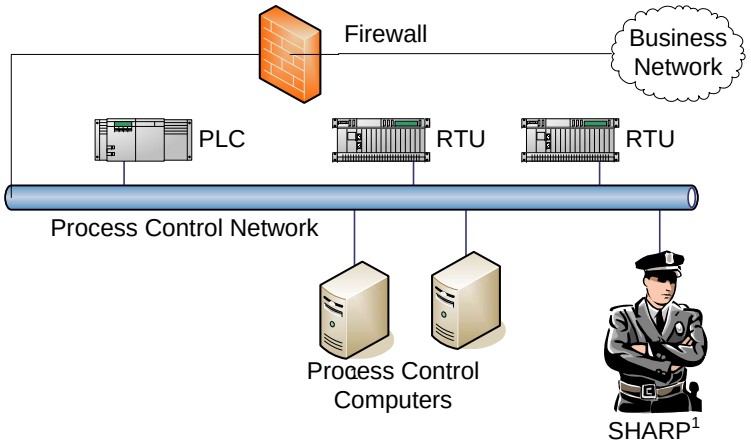


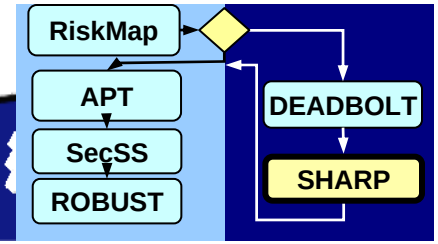


SHARP

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**

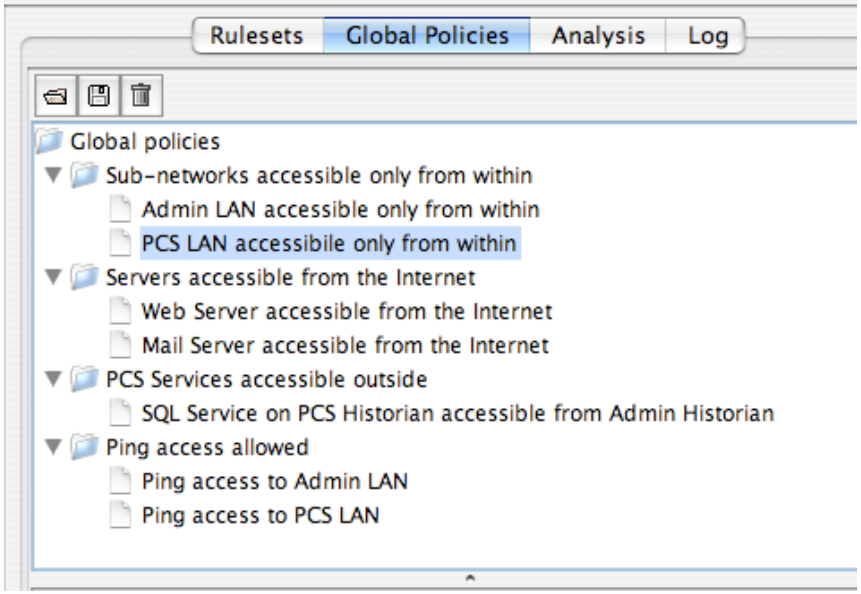


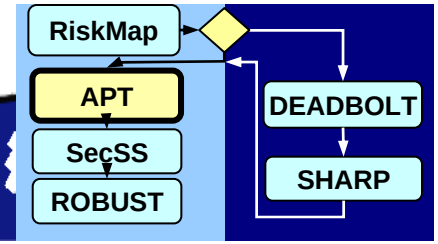


The Access Policy Tool (APT)

- **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/

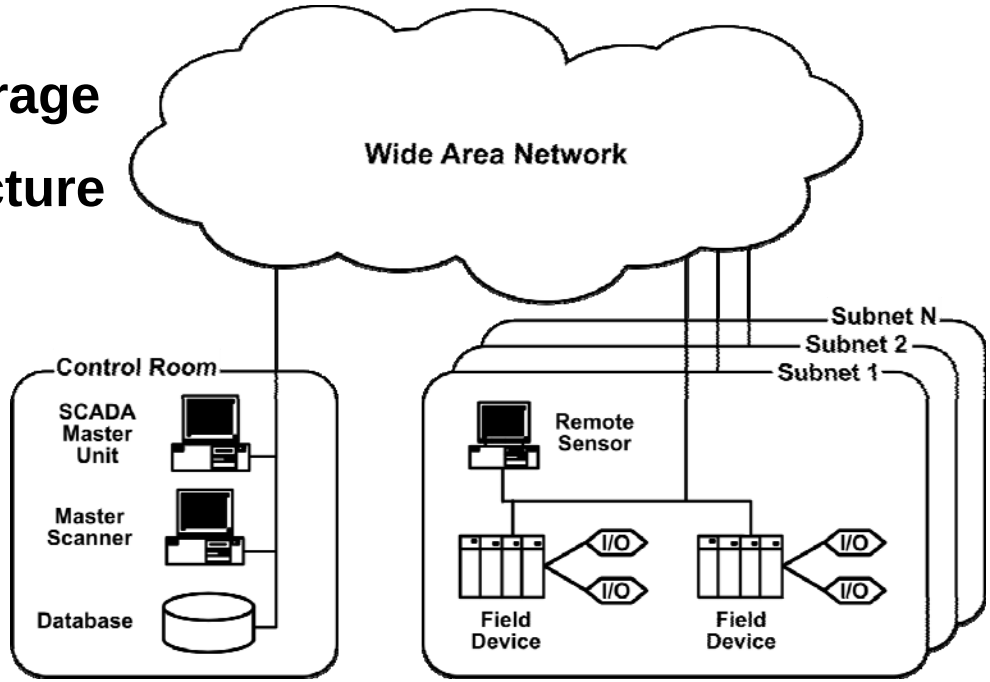


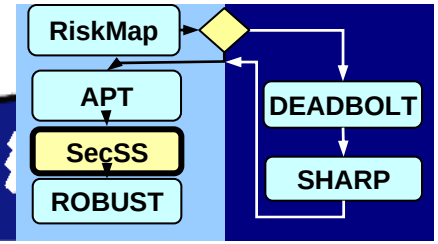


SecSS: Monitoring Tools for Process Control Networks

- **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



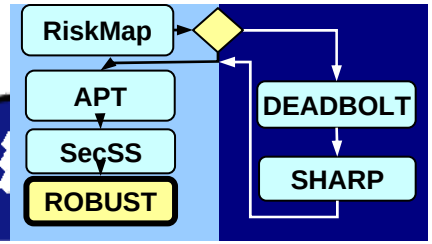


ROBUST: A Concept of Operations to Ensure System-Level Survivability and Recovery

- **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)**

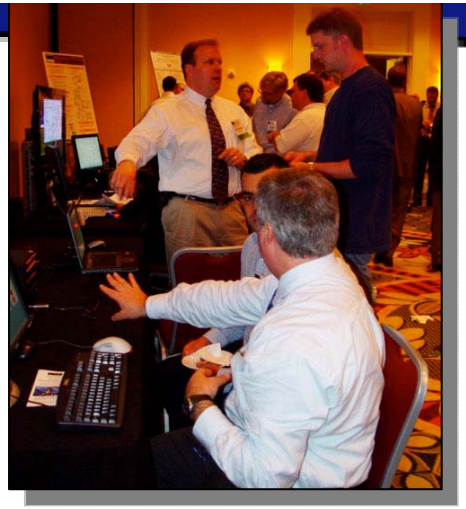
More Information

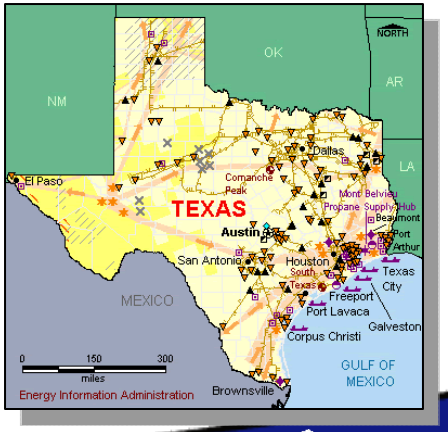
– Bryan Richardson
btricha@sandia.gov
at Sandia National Laboratories



Workshops

- **Briefings of the latest research results**
- **Hands-on technology demonstrations in a science fair setting**
- **Opportunities to interact with the I3P researchers**
- **1-day workshop held on March 6, 2008**
  - In conjunction with NPRA 2008 Security Conference
  - Very well received by attendees





5th Annual Workshop on April 28, 2009 in Texas