www.thei3p.org

Institute for Information Infrastructure Protection

I3P Research on Process Control System Security

Ron Trellue
trellue@swcp.com

I3P PCS Security Research Team

This work was supported under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College.

What Is The I3P?

The Institute for Information Infrastructure Protection

- Funded by U.S. Congress, managed by Dartmouth College with oversight from U.S. Department of Homeland Security
- Established in 2001 to identify and address critical research problems facing the U.S. information infrastructure
- Consortium of 29 universities, non-profit research institutions, and federal labs
- Coordinates a national cyber security R&D program and helps build bridges between academia, industry and government

I3P Accomplishments

"2003 Cyber Security Research and Development Agenda" - Identified eight cyber security research gaps.

Research Projects – Supports high-impact R&D in the areas of economics and process control systems security. The projects are customer focused and have technology transfer explicitly incorporated.

Fellowship Program – Advances the I3P research agenda and build a cadre of investigators focused on critical research challenges.

The I3P Knowledge Base – Promotes awareness and information sharing.

I3P Publications – Bulletins, papers and technical reports provide research results and analysis.

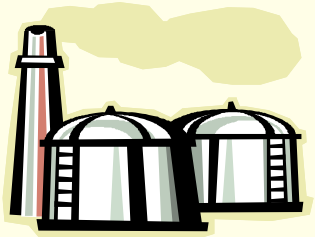
The I3P Team Approach to the PCS Project Proposal

- Assemble a research team of nationally recognized experts in cyber security and Process Control System (PCS) security
- Build on the strengths of the team to address six specific PCS security problems
- Focus on the **oil and gas sector** by partnering with industry – primarily the refinery and pipeline segments
- Develop tools and technology that can enhance the security of PCS
- Communicate and demonstrate results of the research
- Influence owner/operators/vendors and policy decision makers to increase PCS security robustness

Institute for Information Infrastructure Protection
www.thei3p.org

The I3P R&D Initiative to Advance Security of Control Systems

Oil and Gas Industry at Risk



Requirements and Information

System configurations
Operational uses
Business constraints

Engagement through workshops, demonstrations, site visits

Knowledge and Technology Transfer

Vulnerability awareness
Assessment methodologies
Security metrics
Mitigation strategies
Security technologies

2-yr, $8.5 Million I3P Research Project

Team 1	Team 2	Team 3	Team 4	Team 5	Team 6
Risk Characterization *SNL*	**Interdependencies** *UVa*	**Metrics** *PNNL*	**Security Tools** *MIT/LL*	**Information Sharing** *MITRE*	**Tech Transfer** *SRI*

Project Team Members

- Sandia National Laboratories (SNL)
- Pacific Northwest National Laboratory (PNNL)
- MIT/Lincoln Laboratory
- SRI
- MITRE
- Institute for Information Infrastructure Protection (I3P)
- University of Tulsa
- University of Virginia
- University of Illinois Urbana/Champaign (UIUC)
- New York University
- Dartmouth College

Obstacles to overcome in building an effective team

- The 11 institutions had never/rarely worked together before
- Team consisted of over 50 researchers
- Team members varied from grad students, senior academic researchers, to experienced engineers
- The institutions are spread across the country geographically
- Team members even though experts in cyber security had varying levels of experience in process control systems
- Team members had different visions of success

Lessons Learned

- The number of institutions was too large when the team members were not yet familiar with each others expertise
- We divided the effort into six teams. It was very important to select team leaders used to working across institution boundaries
- We started the project with a 2-day tutorial on PCS security to give the team a chance to learn about PCS security and each other
- We meet face-to-face quarterly using Net Meeting for those who cannot attend

  (this has been very successful)

Lessons Learned

- We have frequent teleconferences led by the team leaders (1 or 2 a month)
- We have leadership teleconferences with the project leaders and team leaders
- We defined project goals and metrics for success as well as having defined milestones to meet
- It took a year and a half to move from individual efforts to a more coordinated team effort (unfortunately, we only have 2 years)
- Even though we tried, we should have formed an industry advisory board early on to help us better understand the stakeholders environment

Why is this Project Important?

Bellingham, WA – June 10, 1999

Control systems are critically important to the safe and efficient operation of infrastructure systems but are vulnerable to cyber attacks:

- Control systems security problems and remediation approaches are different from enterprise information technology systems (IT)
- Effects of cyber attacks on operations and interdependent infrastructures not well understood

Six hard problems being addressed

Team 1. What is the risk to infrastructure caused by potential vulnerabilities of their process control systems?

Team 2. What consequences could vulnerabilities in process control systems cause to the interdependencies between infrastructures?

Team 3. How can metrics be defined that express the costs, benefits, and impacts of security controls within the specific operational context?

Six hard problems being addressed

Team 4. Vendors & operators need to develop, distribute, configure, and quantify the benefit of secure systems

Team 5. Lack of secure information sharing methods within the Gas & Oil sector leaves the sector and consumers at risk

Team 6. How do we share these research results and products with our industry and government customers?

Research Approach

- Understand vulnerabilities, characterize the risk, analyze the consequences of disruption (Teams 1 and 2)
- Understand and develop metrics that can be used to measure improvement (Team 3)
- Research technical solutions (Teams 4 and 5)
- Work with customers to transfer the knowledge gained and technology developed (Team 6 with the support of the other 5 teams)

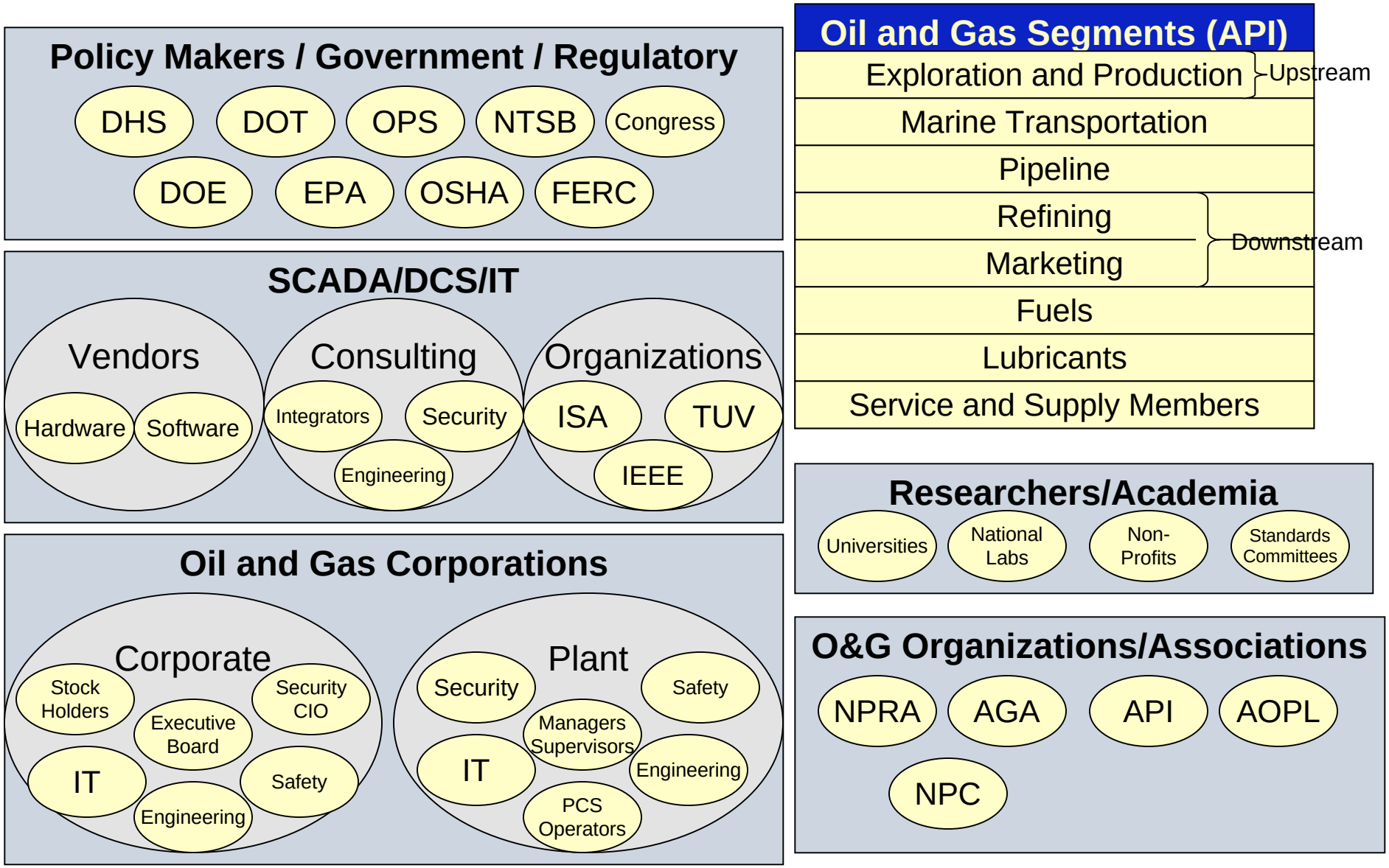
Project Goals –

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

Results and Outreach

- **Three workshops** hosted by the I3P have engaged gas and oil infrastructure owners, operators, vendors, and the research team – next workshop is Feb 2007
- The team has presented the project results at over **twenty** process control systems related conferences
- Researchers have participated in **site visits** for in depth industry interaction
- The team has **published** a substantial number of journal articles, technical reports, and conference papers
- PCS security **classes** have been developed and are being taught at several of the participating universities

Potential target audiences with concerns for security of PCS systems in the Oil and Gas industry



Why Is There A Problem?

Control system side

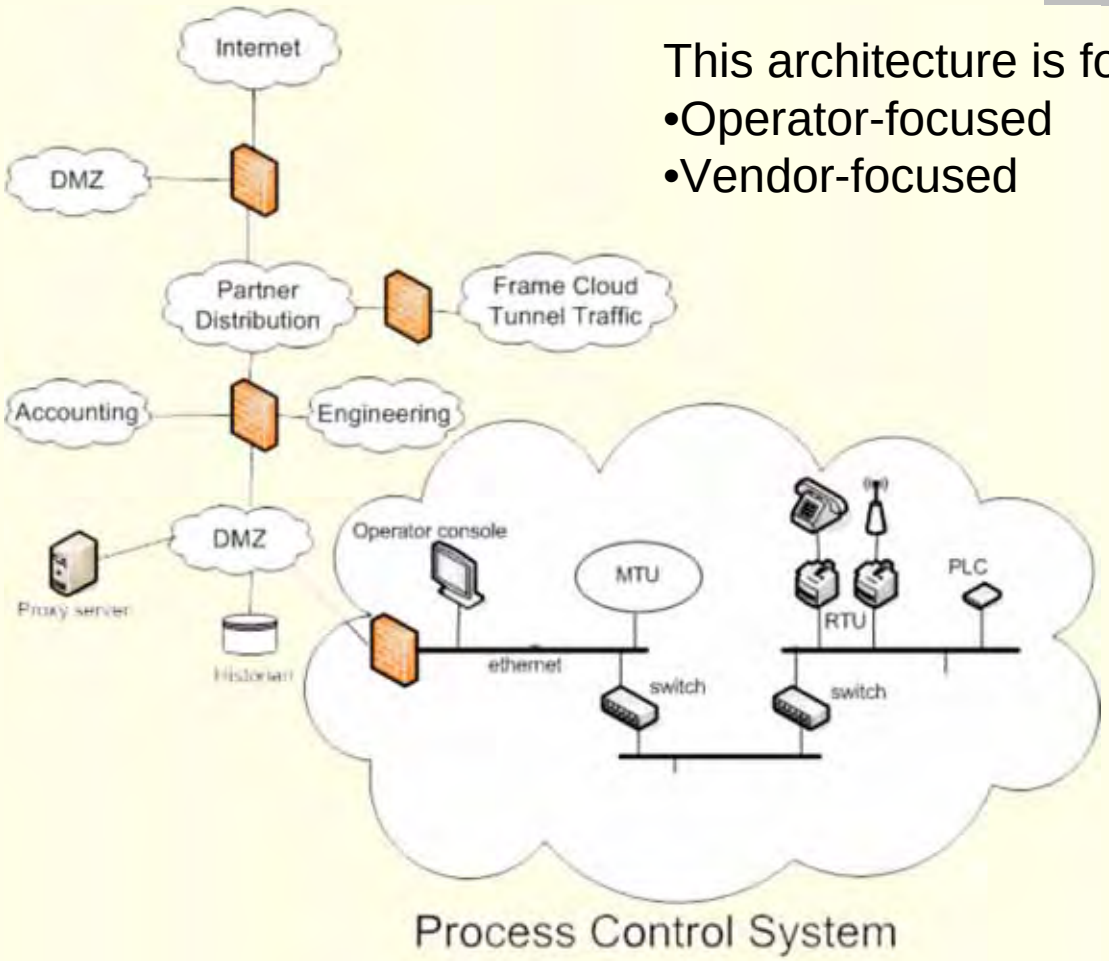
- Top priority is reliability and availability, not security
- Traditionally relied on obscurity and isolation
- Trend: using general hardware and OS
- Owner/operator companies are in the hands of vendors
- Vendors often have backdoor modem lines
- Default passwords

IT side

- Traditional security tools may not work for control systems
- IT people do not know control systems
- Enterprise networks are being connected to control systems
- Control systems are overlooked because they are not managed by IT

Proposed Demonstration Architecture

(Hypothetical Existing System for Oil/Gas Refinery)



This architecture is for two demos:

- Operator-focused
- Vendor-focused

Examples of Differences between Business & Process Control Networks

Aspect	Business Network	PCN
Anti-virus	Widely used, centrally deployed, automated	Often difficult/impossible to deploy, manually updated
Systems Lifecycle	3-5 yrs	5-20 yrs
Outsourcing	Often used	Rarely used
Patching	Frequent	Slow (and normally requires vendor approval)
Change	Frequent, formal, and coordinated	Rare, informal, frequently not coordinated
Time Criticality	Delays OK	Critical (possibly safety dependent)
Availability	Scheduled Outages are OK	Needed 24/ 7/ 365
Security Skills & Awareness	Fairly Good	Often Poor
Automated Tools	Widely used	Limited and need to be used with care
Physical Security	Secured data centers	Often remote and unmanned

Risk Characterization
2005 Workshop Observations

- Operator and vendor panels
- Common concerns surfaced:
  - Wireless connectivity
  - Need for standards, guidelines
  - Interoperability among organization levels
  - Security addressed throughout the life-cycle
  - Legacy system maintenance/upgrade
  - Economic justification

Risk Characterization

Pressures Against Effective PCS Security

- Inertia against recognizing security as critical for automation system development, deployment, and management
- Few if any documented security management policies and procedures for PCS and automation systems
- Wide availability of conventional information technology (IT) hardware and software/operating systems
- Desire for improved operational and process efficiency
- Lack of business case for PCS security investment
  - Little concrete data on automation system attacks
  - Legal precedent not well-established
  - Automation products that have few intrinsic security capabilities
  - No contractual requirements for security
- Security is 5-10 years behind typical IT systems

Risk Characterization
Vulnerability Analysis

- Industry concerns include:
  - Wireless security
  - Intrusion detection
  - Security implementation
  - Legacy systems
  - Standards
  - Training and awareness
  - Design
  - Network structure
  - Policies and plans
  - Incident handling

Risk Characterization
Characterized Vulnerabilities

Vulnerability Category	Description and Examples
System Data	• Lack of understanding of what data is considered sensitive, how it should be separated and protected.
Security Administration	• Lacking policies, standard procedures, training, and corporate/industry security plans. • Formal configuration management needed for upgrades, legacy plans, and patching.
Architecture and Design	• No integrated security in PCS designs. Security must be an add-on. • Centralized storage or control mechanisms are single points of failure.
Platforms	• Patching, backups, passwords, OS security, application security, and security policies for access control and file sharing are needed. • Physical access control is lacking.
Networks and Communications	• Wireless security, monitoring, encryption, access control, boundary security, and standards for implementation are needed.
Incident Response and Handling	• Response plans are lacking, as well as backup and disaster recovery plans. • Forensic data collection and analysis is needed. • Redundant operational capability is beneficial.

Risk Characterization
Consequences & Resulting Impacts

Consequence	Effect	Impact
Access/Read/ Alter Data	• Theft or alteration of corporate/industry data • Theft or alteration of critical operations data used for future attack • Theft of personnel data • Divulge corporate trading partner info • Billing and purchasing data changed	• Quality of life (i.e. identify theft, negative publicity for corporate and industry) • Physical impacts to equipment
Gain Control of PCS Systems	• Full operation of control systems • Can alter, stop, or destroy equipment and operations	
Denial of Service	• Halt operations on process control, business systems, or telecommunications	
Access Systems as Jump-points	• Use systems as part of a large scale, coordinated attack	
Physical Access to PCS Systems	• Can physically damage systems • Access as a trusted insider if electronic access controls are not in place	
Introduction of a Virus/Worm	• Can slow or halt operations	

Risk Characterization

Potential Business Impacts

- Downtime (production, delivery, network)
- Equipment repair or loss
- Trustworthiness, public perspective
- Environmental damage or fines
- Safety infractions
- Worker or public injury
- Value of stolen corporate trading information
- Value of stolen personnel data
- Value of altered commodity purchasing data
- Value of altered customer billing information

Risk Characterization

Effectiveness of Protective Measures

- Principle of least privilege
- Defense in layers
- Areas to address:
  - Data
  - Applications
  - Platforms and operating systems
  - Networks and communications systems
  - Boundary systems
  - Control systems
  - Physical access
  - Standard operating systems

Risk Characterization

Example Protective Measures

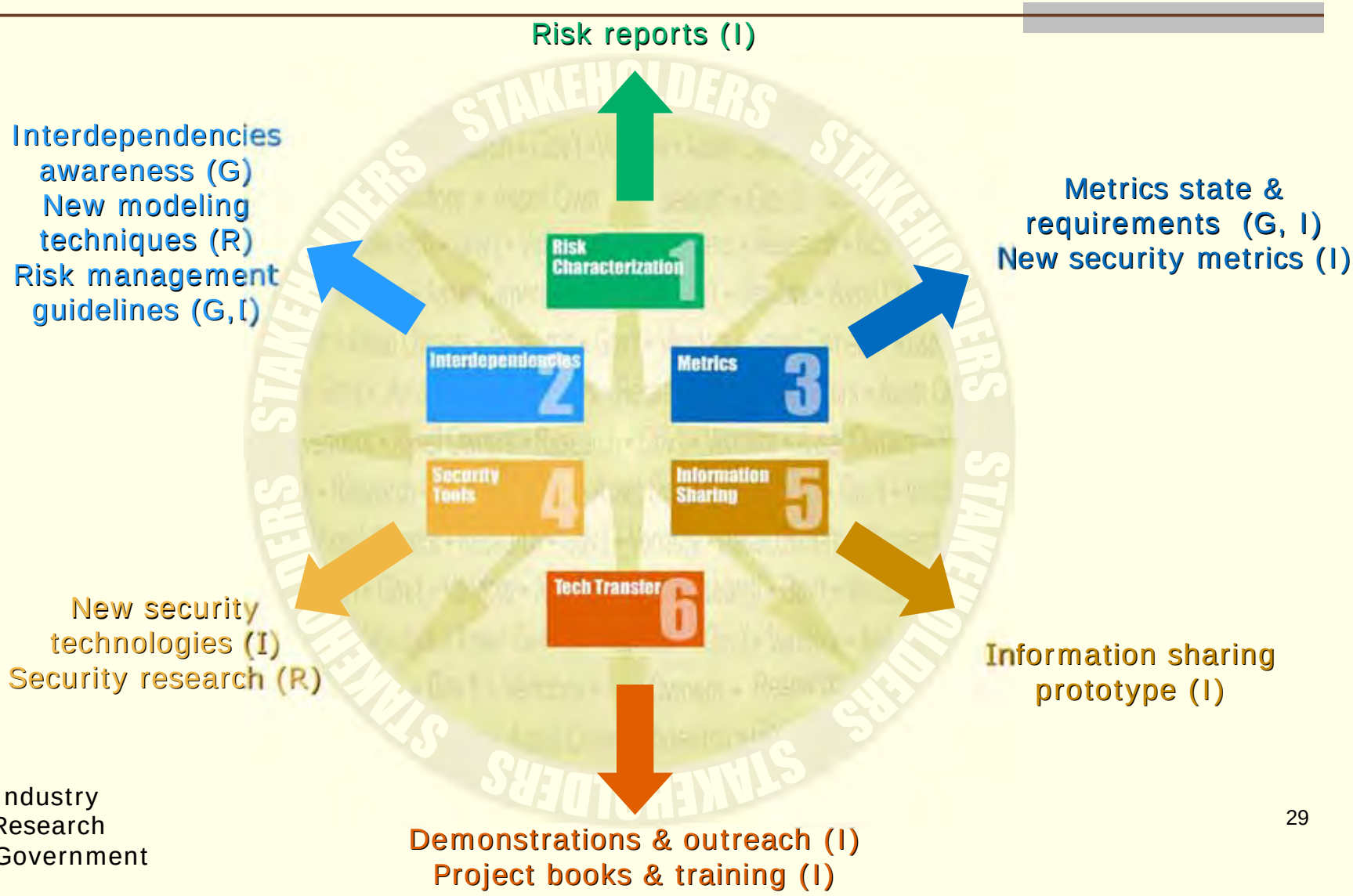
- Access control
- Authentication
- Data separation
- Functional separation
- Encryption
- Patches, upgrades, secure code development
- Monitoring and event correlation
- Backups and disaster recovery
- Alerting mechanisms
- Redundancy
- Perimeter security
- Secure remote access
- Trusted platforms

Risk Characterization

Conclusions

- Common themes among industry and researchers
- Need for a layered approach to security
- Understanding critical functions, data types, and required protection levels is essential
- Have a security plan
- Employ security in design and with technology controls
- Keep an operational focus
- Develop standards and guidelines
- Facilitate organizational and industry communication

Significant Products and Results



I = Industry
R = Research
G = Government

Accomplishments: Situational awareness/business case

- **RiskMAP**, the proven Risk-to-Mission Assessment Process, provides decision support information tailored to company needs. RiskMAP translates between the technical terms of network risk and the business terms of corporate risk so that all can understand and decide on risk mitigation strategies.

- An **educational awareness seminar** has been developed addressing risk characterization for the gas and oil sector.

- **Interdependency models** have been developed to assess the consequences of potential cyber disruption to local, regional, and infrastructure business.

Accomplishments: Metrics and Tools

- **Metric Reports** document the gaps in using enterprise security metrics for process control system environments. Requirements for PCS security metrics are analyzed.
- A **metrics technology evaluation tool** is under development to be used to evaluate the security of new PCS products.
- A prototype **Security Dashboard** has been developed that converts the *DOE 21 Steps for Improving Cyber Security of SCADA Networks* into a security evaluation tool.

Accomplishments: Secure Design Tools

- Operator tools
  - APT: The Access Policy Tool assesses the system of firewalls and their rule-sets and host policy enforcement mechanisms to determine whether the rule-sets accurately implements the desired policy.
  - Emerald: Emerald is a system for intrusion detection and alert correlation that has been adapted from enterprise systems for use in control systems.

These tools have been developed and are currently undergoing further testing and evaluation.

Accomplishments: Secure Design Tools

- Vendor tools
  - DEADBOLT is an effective, scalable and practical automated testing framework that facilitates the discovery of buffer overflows in C and C++ software before deployment.
  - SecSS: The Security Services Suite is intended to serve as a technical solution for securing communications networks used in industrial control systems with five approaches: message monitoring, protocol-based solutions, tunneling services, middleware components, and key management.
  - SHARP: The Security Hardened Attack Resistant Platform provides a vendor an infrastructure independent high security environment for process control system networks as a drop-in component.

Project Success

- Demonstrated improved cyber security in the Oil & Gas infrastructure sector
  - New research findings
  - New technologies
- Significantly increased awareness of
  - Security challenges and solutions
  - The capabilities of the I3P and its members

Interested in More Information?

- Visit the project web site, www.thei3p.org/projects/pcs.html
  - Reports on risk characterization, state of metrics, and risk assessment . Fact sheets on the techincal products.
- Contact one of the research teams
  - E.g., RiskMAP is available for evaluation
- Come to the next I3P workshop in Houston
  - February 15, 2007: Demos and presentations
  - February 16, 2007: Security training – customized for the oil & gas industry, based on research findings