Process Control Systems Forum

# I3P SCADA Security Research Plan

## Unifying Stakeholders and Security Programs to Address SCADA Vulnerability and Infrastructure Interdependency

Ron Trellue, Team Lead
Sandia National Laboratories

# What is SCADA? What is the I3P?

When you see SCADA in this presentation, it will be used synonymously with the following terms

- SCADA – Supervisory Control and Data Acquisition Systems
- Process Control Systems
- Control Systems
- Digital Control Systems
- Industrial Automation Systems

I3P is the Institute for Information Infrastructure Protection at Dartmouth College (www.thei3p.org)

# What is this research project?

- The objective is to help industry better manage risk by providing additional information on threat characterization, by developing and demonstrating cyber security related tools and technologies, and by contributing to the enhancement of sustainable security practices for SCADA systems.
- Another objective is to provide industry with a mechanism to strengthen applied research by providing guidance and direction to the research team by forming a close partnership.
- The Institute for Information Infrastructure Protection (I3P) recently approved funding for this cyber security research project.

# What does the Research Team plan to do?

- Build upon ongoing cyber security research to apply to the process control arena
- Develop research collaborations with other institutions with cyber security domain expertise
- Develop tools and technology which could enhance the robustness of critical infrastructure process control systems
- Focus on the oil and gas sector primarily
- Demonstrate results of the research
- Communicate the knowledge we learn
- Plan for technology transfer

# Who is on the project ?

- The team is made up of some of the top academic/lab cyber security researchers in the country
- In 2002, the I3P established a research Consortium made up of 24 institutions who meet quarterly to advise the I3P on cyber security research direction
- The current SCADA research team is a subset of the Consortium members
- Government oversight is provided by DHS S&T
- The team will illicit industry guidance through workshops, an advisory board, and direct interaction

# How did this funding come about?

- In January 2003, the I3P released the “2003 Cyber Security Research and Development Agenda” which identified eight underserved research areas
- In 2004, the I3P collected a number of white papers in cyber security research and reviewed them for funding
- This SCADA Security Research Plan was selected as the #1 topical area for funding
- The completed plan was submitted in the Fall of 2004. After it was selected to proceed forward, it was reviewed by a Research Advisory Board, the I3P Executive Committee, and by representatives from the Department of Homeland Security

# What this effort is not

- The Research Team does not develop nor market process control systems
- The Research Team does not own or operate process control systems
- The Research Team does not develop standards, policy, or regulations
- The Research Team will not undertake “science for science’s sake” – this is an applied effort focused on helping address critical industry needs

# What experience does the team have?

- The Research Team has vast experience in security research
- The Research Team has significant experience in addressing enterprise network security solutions
- The Research Team understands the differences between enterprise networks and process control systems
- The Research Team has an understanding of the threat to SCADA systems and their commodity networks

# What has the team accomplished?

- Team members have performed hundreds of assessments on infrastructure systems including process control systems (cyber and physical)
- Team members have published papers on cyber security, SCADA vulnerabilities, best practices, and interdependencies
- Team members have taught classes on SCADA best practices and on doing assessments of SCADA systems
- Each team member has current work in their institutions which will be leveraged for this effort

# Industry is moving in the right direction

- Industry is intent on understanding their risks and investment strategies
- Industry and industry associations are working on standards and best practices guidelines
- Vendors are analyzing security needs and developing mitigation options
- Industry is involved with the growing number of government initiatives with the objective of enhancing the robustness of national critical infrastructure system

# SCADA Security Research Plan Team

- Sandia National Laboratories (SNL), Team Lead
- University of Virginia (UVa)
- Pacific Northwest National Laboratory (PNNL)
- MIT Lincoln Laboratory (MIT/LL)
- MITRE
- SRI International
- New York University (NYU)

# SCADA Security Research Plan Team

- University of Tulsa (Tulsa)
- University of Illinois at Urbana-Champaign (UIUC)
- Dartmouth College
- I3P

# What research is to be done?

## What are some of the results the team hopes to accomplish?

# SCADA Security Research Plan Topic Areas

- 1: Assess dependence on SCADA and its security (risk analysis)
- 2: Model SCADA interdependencies
- 3: Develop metrics for SCADA security
- 4: Research tools to aid in secure design of SCADA systems
- 5: Develop cross domain solutions for information sharing
- 6: Transfer SCADA security technology into industry

# Topic 1 - SCADA Risk Analysis

- **Problem: What is the risk to infrastructure caused by potential vulnerabilities of the process control systems?**
- **Deliverables**
  - Year 1 and 2 SCADA risk workshops focused on oil and gas sector to collect data for all tasks in the plan
  - Assembly of knowledge bases from owners, operators, and domain experts including international contacts (UK, Canada)
  - Analysis of the data to determine classes of SCADA systems to include vulnerabilities, threats, consequences, and risks for SCADA security

# Topic 1 - SCADA Risk Analysis

- Development of attack taxonomy and mitigation strategy analysis
- Profiles of security situations, generalized threat and associated metrics, classes of consequences and metrics
- Produce “Best Practices” handbook information for Topic 6

- **Lead – Sandia – Jason Stamp**
- **Team members – Sandia, UVa, PNNL,Tulsa, MIT/LL**

# Topic 2 – Model SCADA Interdependencies

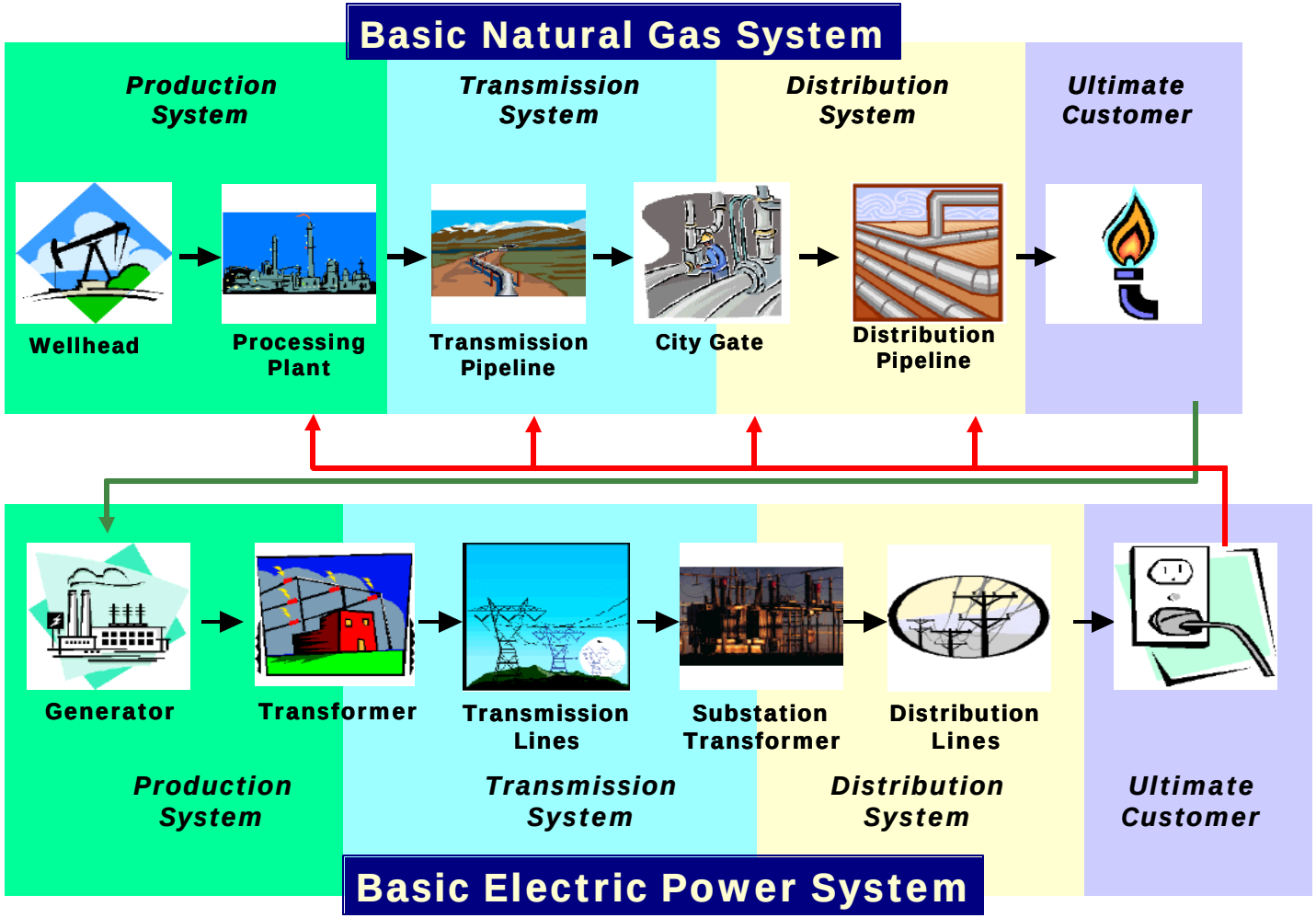
- **Problem: What consequences could vulnerabilities in process control systems cause to the interdependencies between infrastructures?**

- **Deliverables**
  - Report on risk management of SCADA interdependency using the UVa Inoperability Input-Output Model (IIM) addressing the posed research questions
  - Database of case characterization for use by I3P researchers and others
  - Reports on qualitative and quantitative analysis of cases of SCADA and infrastructure interdependencies
  - Impact of SCADA disruptions derived from DHS NISAC interdependencies simulation scenarios

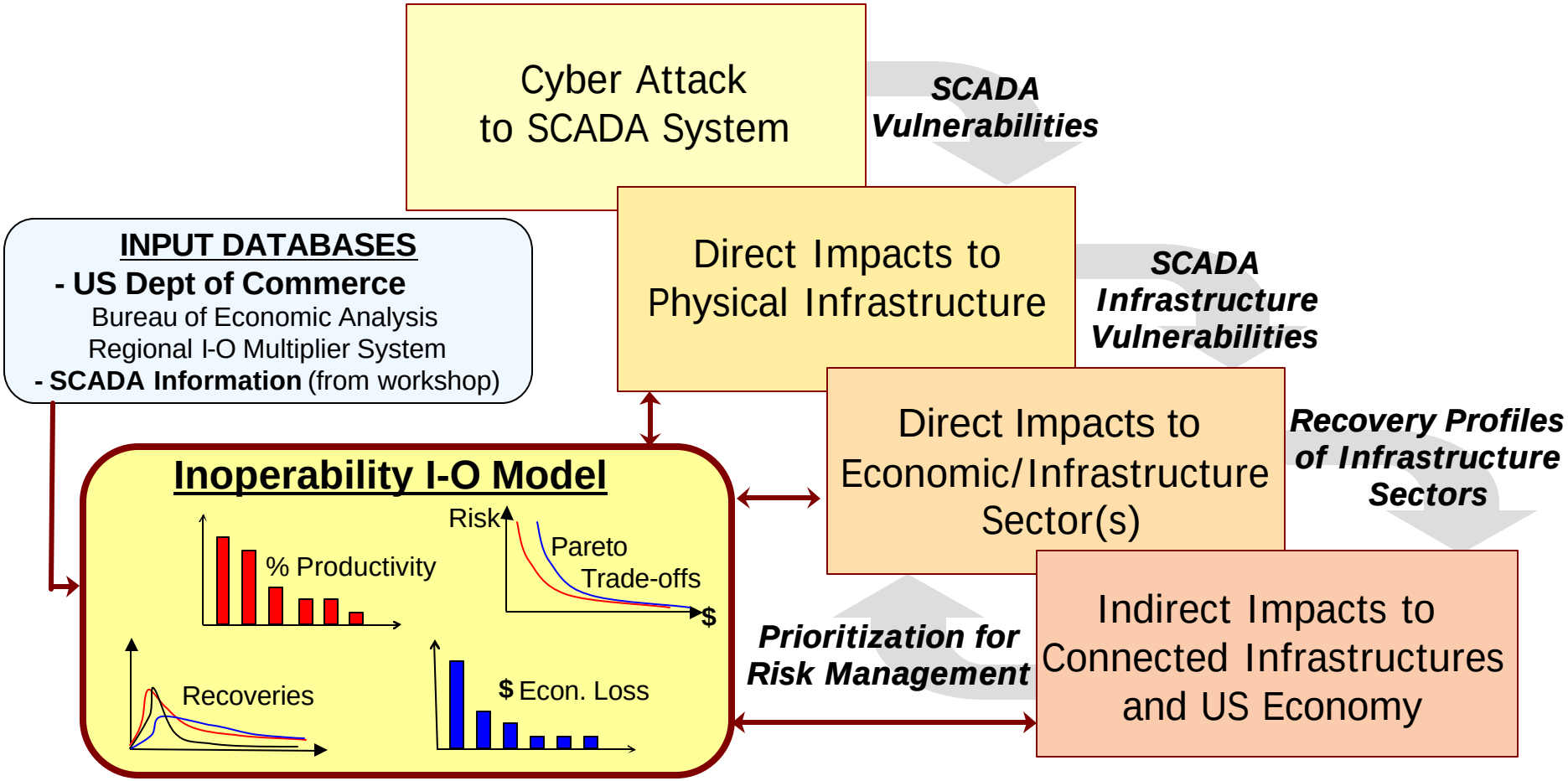
# Topic 2 – Model SCADA Interdependencies

- Lead – UVa – Yacov Haimes
- Team members – UVa, NYU, Sandia

# Example Interdependency: Gas-Electric Infrastructures



# Topic 2A: UVa Risk Management of SCADA Interdependency Using the Inoperability Input-Output Model (IIM)



# Topic 2B: NYU Empirically Derived SCADA – Infrastructure Interdependencies

Identify/Compile Events

(From Government, Industry, Academic Databases)

↓

Code/Statistically Diagnose Events

↓

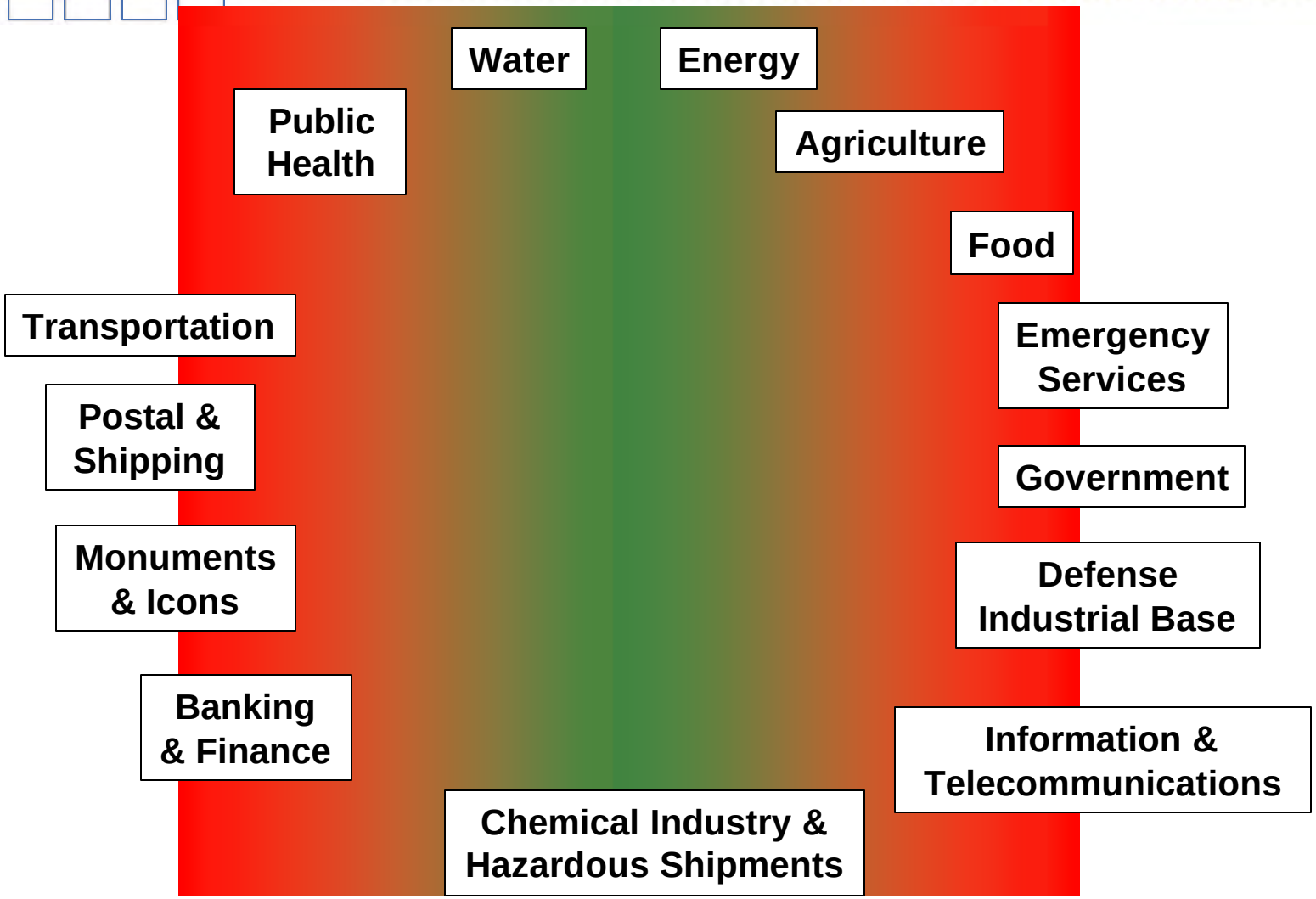
Derive Common Vulnerabilities

↓

Input Event Characteristics Into Macro Models

(Haimes et al. IIM; Influence Diagrams; Risk Models; etc.)

# Topic 2C: NISAC Modeling of Interdependencies (Sandia)



# Topic 3 - Metrics

- **Problem: How can you measure the security robustness of process control systems?**
- **Deliverables**
  - Current state of art/practice report for performance metrics (including standards)
  - Metric requirements for effective risk management of SCADA security
  - New metrics
- **Lead – PNNL - Joe Huffman**
- **Team members – PNNL, Sandia, UVa, MITRE**

# Topic 4 - Secure Design

- **Problem: How do you design and verify trusted process control systems?**
- **Deliverables**
  - SCADA security related tools and products for end-users to help secure existing installations
    - Techniques for integrity verification
    - Intrusion and anomaly detection for SCADA systems
    - Tools for alarm correlation and aggregation
    - Research extending existing tools such as VARM, Mobius, LANscape and others to SCADA systems

# Topic 4 - Secure Design

- Tools developed for SCADA system developers to help design more secure future systems
  - Develop multi-protocol analyzer
  - Apply Symbolic Analysis Lab (SAL) to SCADA system design
  - Develop guidelines for next generation protocols

- **Lead – MIT/LL – Rob Cunningham**
- **Team members – MIT/LL, SRI, University of Illinois, MITRE, PNNL, Tulsa**

# Topic 5 - Cross Domain Solutions

- **Problem: How do you reliably share sensitive information between critical domains?**
- **Deliverables**
  - Results from workshops and customer interactions on requirements for secure information sharing
  - Adapt ongoing research in the following areas to tailor for SCADA applications
    - Trustworthy information sharing – Sandia
    - Adaptive CDIS Service - Mitre
    - CDIS Protection - Dartmouth
- **Lead – MITRE, Michelle Gosselin**
- **Team members – MITRE, Sandia, Dartmouth**

# Topic 6A – Transfer of Technology

- **Problem: How do we share these research results and products with our industry and government customers?**
- **Deliverables – Transfer of technology**
  - Continuous evaluation of technologies for transition readiness
  - Develop scenario specific Technology Demonstration Programs
  - Coordinate with other efforts being funded by DHS, DoD, DOE and industry
  - Formulate specific technology transfer plans with industry
- **Lead – SRI – Ulf Lindqvist**
- **Team members – SRI, Sandia, UVa, PNNL, Tulsa, MITRE, All**

# Topic 6B – Knowledge Transfer

- **Deliverables – Knowledge transfer**
  - Publish technical reports and papers
  - Collect and publish releasable information in project books through ISA – possible themes:
    - All there is to know about SCADA systems security and where it is going
    - SCADA security in the oil and gas sector –details of our work
    - SCADA security in the other critical sectors – how do we see the transfer of knowledge and technology
  - Establish and manage limited-access web site
  - Establish an electronic SCADA Journal
  - Pursue education and awareness efforts
    - Through conferences
    - Through professional society meetings
  - Conduct SCADA security awareness classes

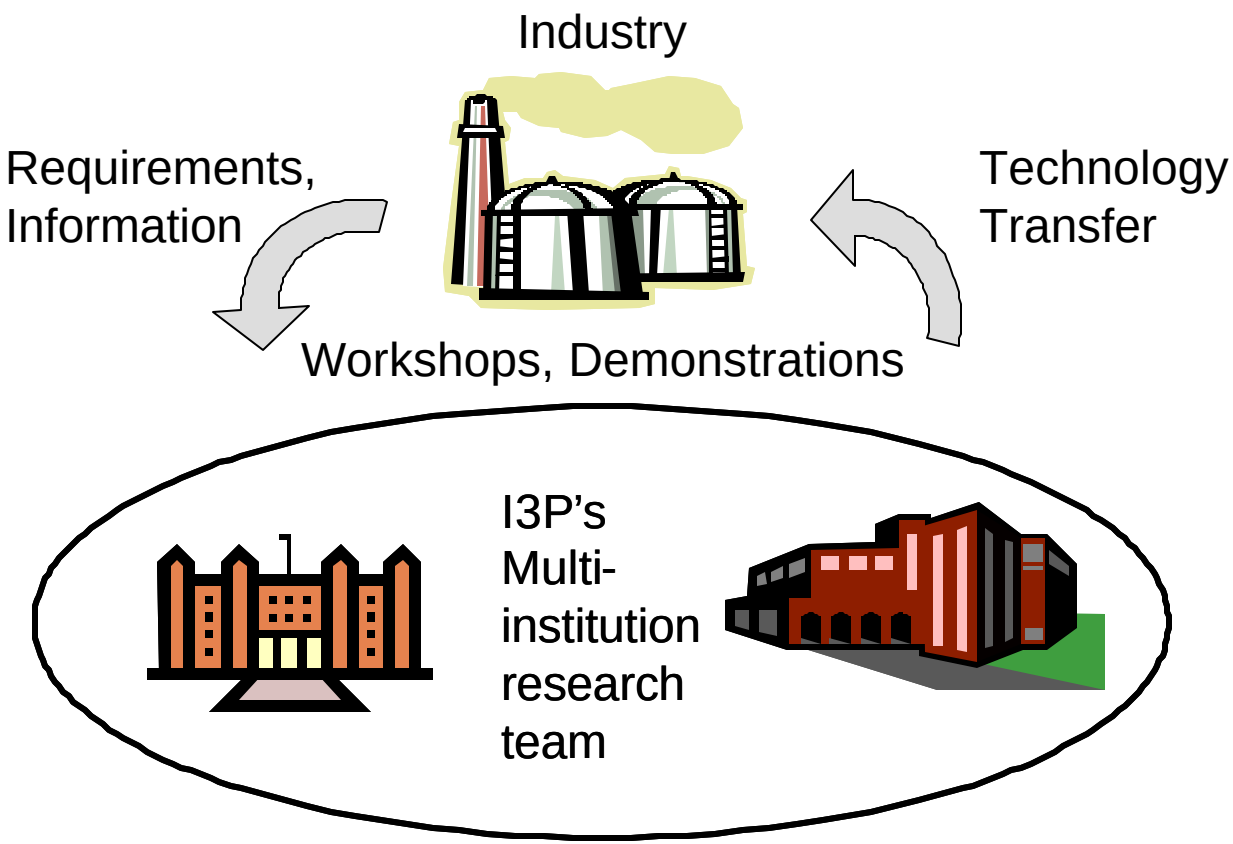
# Recommendations from Independent Review Advisory Board

1: A stronger partnership is needed with SCADA users and vendors in oil and gas industry

2: Clearer steps are needed towards commercialization

3: Staff members with oil and gas SCADA experience must be added to the team

4: Interim performance goals must be set and measured

6: Create a clear mechanism and budget to integrate related research from non-I3P institutions

# I3P SCADA Security Program Overview