

## *I3P Preliminary Risk Characterization Report*

*Annie McIntyre*  
*Sandia National Laboratories*

*Andrew Lanzone*  
*Sandia National Laboratories*

*Jason Stamp*  
*Sandia National Laboratories*

*Draft*

*March 13, 2006*

This work was supported under grant 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 author(s) and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology. The I3P is managed by Dartmouth College.

*DRAFT*

---

## ACKNOWLEDGEMENTS

---

*The authors would like to thank the Jun2005 I3P Workshop participants for their contribution in providing data to this team ipreparation for this white paper. The team also recognizes Martin Stoddard, P.E., and En Pratt, E.C.F.E., of Pacific Northwest National Laboratory, and Yacov Haimes, PhD., Matthew Henry, Joost Santos, and Kenneth Crowther, of the University of Virginia for their review and comment on this report.*

---

TABLE OF CONTENTS

---

<b>Acknowledgements .....</b>	<b>2</b>
<b>Table of Contents .....</b>	<b>3</b>
<b>Table of Figures .....</b>	<b>4</b>
<b>Executive Summary .....</b>	<b>5</b>
<b>1. Introduction .....</b>	<b>6</b>
<b>2. Critical Observations from the Workshop .....</b>	<b>8</b>
<b>3. Risk Characterization Process .....</b>	<b>10</b>
3.1. Threat Assessment .....	10
3.2. Vulnerability Analysis .....	12
3.3. Consequences .....	15
3.4. Business Impacts and Return on Investment .....	18
3.5. Effectiveness of Candidate Protective Measures .....	19
<b>4. Sources of Input Data .....</b>	<b>21</b>
4.1. Stakeholder Perspectives .....	21
4.2. Gap Analyses .....	21
4.3. SCADA Research .....	21
<b>5. General Analysis .....</b>	<b>22</b>
<b>6. Summary and Conclusions .....</b>	<b>23</b>
<b>7. Appendix: References .....</b>	<b>24</b>

---

**TABLE OF FIGURES**

---

Figure 1: SCADA Attack Model ..... 11  
Figure 2: Cause and Effect of Attack..... 22

---

## EXECUTIVE SUMMARY

---

Developed under Institute for Information Infrastructure Protection (I3P) Risk Characterization Effort, this white paper discusses risk characterization for SCADA operations in the oil and gas industry and summarizes major concerns voiced at the I3P Workshop held in June, 2005. The purpose of this risk characterization effort is to combine experience and viewpoints from industry asset owners, vendors, and government, with known technical threat and vulnerability data in an effort to develop a more comprehensive picture of the risks associated with cyber-threats against SCADA systems in critical infrastructure sectors. In this paper, risk is characterized in terms of identifying threats, recognizing common vulnerabilities in SCADA systems, consequences, and identifying measures effective in protecting these architectures. Impacts on business created by cyber security incidents are recognized, providing a realistic view of effects on operations, personnel, the organization, and the national critical infrastructure. Data utilized in characterizing risks to SCADA systems include technical knowledge from SCADA researchers, stakeholder perspectives from the workshop, and gap analyses performed by I3P activities. Understanding and characterizing this risk enables the development of strategies for preventing, detecting, mitigating, and recovering from cyber-security incidents with focused and defined objectives. This characterization can be used by industry as a starting point to assess major areas of concern in their own operations, the possible consequences of an attack, and the return on investment of implementing defenses, thereby aiding in protection of the national critical infrastructure.

## 1. Introduction

In June 2005, the Institute for Information Infrastructure Protection (I3P) hosted a SCADA Security Workshop in Houston, Texas. This event gathered members of the oil and gas industry including asset owners, vendors, managers, SCADA researchers, and government (Department of Homeland Security) participants. I3P initiatives, SCADA security concerns, and cyber risks for automation systems were discussed in briefings, panels, and breakout sessions. This white paper discusses the risk characterization aspects for SCADA operations in the oil and gas industry and summarizes major concerns voiced at the workshop. Risk is characterized in terms of threats, vulnerabilities, and consequences. Protective measures and business impacts are also addressed.

The workshop held in June was a specific deliverable under the I3P Program. This task assesses the dependence on SCADA systems and their security. One of the primary objectives of the workshop was to gain an understanding from industry segments of the overall state of SCADA networks, including:

- Security vulnerabilities in SCADA and their trends
- The evolution of the industry's SCADA use leading to the current security state
- Impact of network convergence on SCADA security
- In-house capabilities for security
- Owners' expected options for security investment
- Potential consequences for SCADA tampering and their metrics
- Overall Initiative and program reception
- Standards

Gathering and analyzing this information supports the characterization of risk in terms that provide awareness to industry as well as a basis for mitigating vulnerabilities. In this paper, the characterization of risk was completed by identifying threats and vulnerabilities, and realizing operational consequences that create serious business impacts. This characterization can be used by industry as a starting point to assess major areas of concern in their own operations, the possible consequences of an attack, and the return on investment of implementing defenses. The knowledge and information gathered at the workshop and from subsequent research is representative of the industry's perspective and includes recognized current and future concerns, rather than speculative ideas, media output, or outsider/third party analysis.

The purpose of this risk characterization effort is to combine experience and viewpoints from industry asset owners, vendors, and government, with known technical vulnerability data in an effort to develop a more comprehensive picture of the risks associated with cyber-threats against SCADA systems in critical infrastructure sectors. The I3P Program and the I3P SCADA Security Workshop address the oil and gas sectors specifically. The

## DRAFT

topics in this paper were discussed by industry and SCADA researchers at the workshop and in subsequent meetings. This paper lists the derived, main components of risk and approaches industry can utilize to protect their organizations.

Objectives for completing this white paper included:

- Present information obtained from key critical infrastructure sectors, in this case oil and gas, on experiences, common operating events, concerns, stumbling blocks, and main priorities.
- Identify and categorize main SCADA vulnerabilities.
- Match industry experience and priorities with known technical vulnerabilities.
- Utilize this information for this and other I3P research areas. For example, to:
  - Assess the overall state of SCADA security
  - Suggest a mitigation plan
  - Understand implementation hurdles
  - Build SCADA security analyses
  - Develop qualitative and quantitative metrics for SCADA security
  - Address security with operations as a frame of reference

Understanding and characterizing this risk will enable the development of strategies for preventing, detecting, mitigating, and recovering from cyber-security incidents with focused and defined objectives. Input from industry collectively provides a strong basis for both decision making and improvements with realizable, specific outcomes. It also helps to clarify and prioritize security concerns for the industry, making implementation less overwhelming. The results of this effort also support the cross-domain information sharing effort and gap analysis and foster collaboration with other I3P activities.

## 2. Critical Observations from the Workshop

Members of industry segments voiced their concerns at the workshop. Many of these concerns are discussed in detail in later sections of this white paper. Below is a list of many of the primary points that were raised during the workshop.

### Operator Panel Highlights:

- A need for comprehensive security across spectrum of control systems exists, not just patches or rudimentary security controls on systems. The architecture must be addressed as a whole.
- Interdependencies exist on other critical infrastructures, such as telecommunications. These interdependencies should be considered when implementing security in the architecture.
- A need for overall intrusion detection and prevention exists. Employing a system that provides monitoring, event correlation, first-day intrusion awareness, and alarm processing is necessary.
- Facilitating an understanding of security needs and implementing a solution requires engaging stakeholders at all levels of an organization, including asset owners and managers. An approach to a solution should include buy-in from across the organization.
- Industry stakeholders in any position must be aware that the oil and gas, and national critical infrastructure as a whole, is considered a “target of opportunity” to threats. This means security must be considered now and included in life-cycle planning for the future.

### Vendor Panel Highlights:

- Management must be engaged early in decisions about obtaining and implementing security controls. This must create an understanding by management and asset owners of vulnerabilities and threats that produce real and actual risks. This understanding should include an economic justification for implementing security. Operators then receive support to implement security technologies.
- Awareness and training amongst operators and integrators on security controls, such as firewalls, is generally inadequate, which increases common implementation problems that create vulnerabilities in the architecture.
- An industrial plant network should be considered a multi-layered enterprise rather than a collection of individual nodes. This view allows for security controls to be employed at various levels within the architecture for layered, comprehensive protection.
- Clearly defined roles and relationships between Information Technology (IT) personnel and SCADA engineers are needed. Just as managers and operators must communicate and understand perspectives across the organization when

## DRAFT

deciding on and implementing security, IT personnel and SCADA engineers must be cross-educated to understand priorities and goals. This understanding will allow vendors and operators to approach security throughout the system life-cycle and the enterprise's security plan.

### Shared/Common Concerns:

- Wireless connectivity is becoming an integral part of many of the industry's architectures. Securing wireless capabilities as part of the network's overall security plan is necessary.
- A set of widely accepted standards, guidelines, and best practices would be very useful to industry in planning and implementing security across architectures.
- An understanding of how interoperability affects security within the enterprise by various levels within an organization is necessary. This includes remote connectivity, connecting business and operational networks, and connection to outside infrastructures such as trading partners or telecommunication backbones.
- Security should be addressed by including it in the overall life-cycle of SCADA systems and network architectures. Users and vendors should be encouraged to include security in life-cycle planning.
- Legacy systems will continue to operate in the oil and gas infrastructure and must be considered when securing architectures. A plan must be created to secure these systems without disrupting operations and maintaining security controls on these systems throughout their life-cycle.
- Realization of economic justification for implementing security throughout the enterprise. This will require awareness and communication throughout layers of the organization.

### 3. Risk Characterization Process

#### 3.1. Threat Assessment

The goal of a threat assessment is to determine the likelihood of an attack against a given target. Threats to SCADA systems as they pertain to the oil and gas sectors can be derived based on access, intent, and system vulnerabilities. A typical threat assessment includes:

- Identification of known and potential adversaries
- Analysis of each adversary's motivations, goals, and capabilities
- Assessment of the threat posed by each adversary to critical system assets

When applied to a specific SCADA system or set of systems, a threat assessment is normally quite detailed and specific. However, the scope of this paper is broad and its analyses encompass a generalized view of the entire oil and gas industry. As such, this threat assessment is necessarily broad and generalized.

Adversaries can be characterized by both their level of access, motivations, and their capabilities. A threat implies that an individual or group has the ability and access to carry out a process that creates damage to a system or exploits the system for a specific gain. Threats to SCADA systems can come from both insiders and outsiders. For example, a disgruntled employee sympathetic to a terrorist cause will have more direct access to the SCADA systems than a corresponding outsider.

Threats can vary in capability. Capability is a function of resources such as time, money, computing power, technical knowledge, and intelligence resources. Threats and their capabilities are often divided into several specific categories such as nation-state, international terrorists, domestic terrorists, or hackers. Although individual hackers may have malicious intent and technical knowledge, organized cyber-terrorist groups often possess the resources necessary to carry out an effective, distributed attack that produces severe consequences. Characteristics that can affect a threat's success in an attack include:

- Funding
- Goal intensity
- Stealth capability
- Access
- Cyber skills
- Implementation time
- Cyber-organization size

These characteristics are detailed in a report entitled "Generic Threat Profiles" (SAND 2005-5411) by Sandia National Laboratories. A targeted organization has no capability of controlling these characteristics with the exception of access. Therefore an

organization's physical and cyber defenses are critical. Access to information about SCADA systems, including design details, weaknesses, and protective measures, are often available on the Internet. Likewise, industry and corporate-specific data can easily be gathered from basic Web investigative techniques. In combination, this information can be very useful to a threat planning a coordinated attack, and because this information is readily available, increased protections implemented on SCADA networks become the primary line of defense. This defense ensures operations are not disrupted or compromised. Because these threats exist today and organized cyber-terrorists continue to gain resources and capability, industry must address this as a present and future issue.

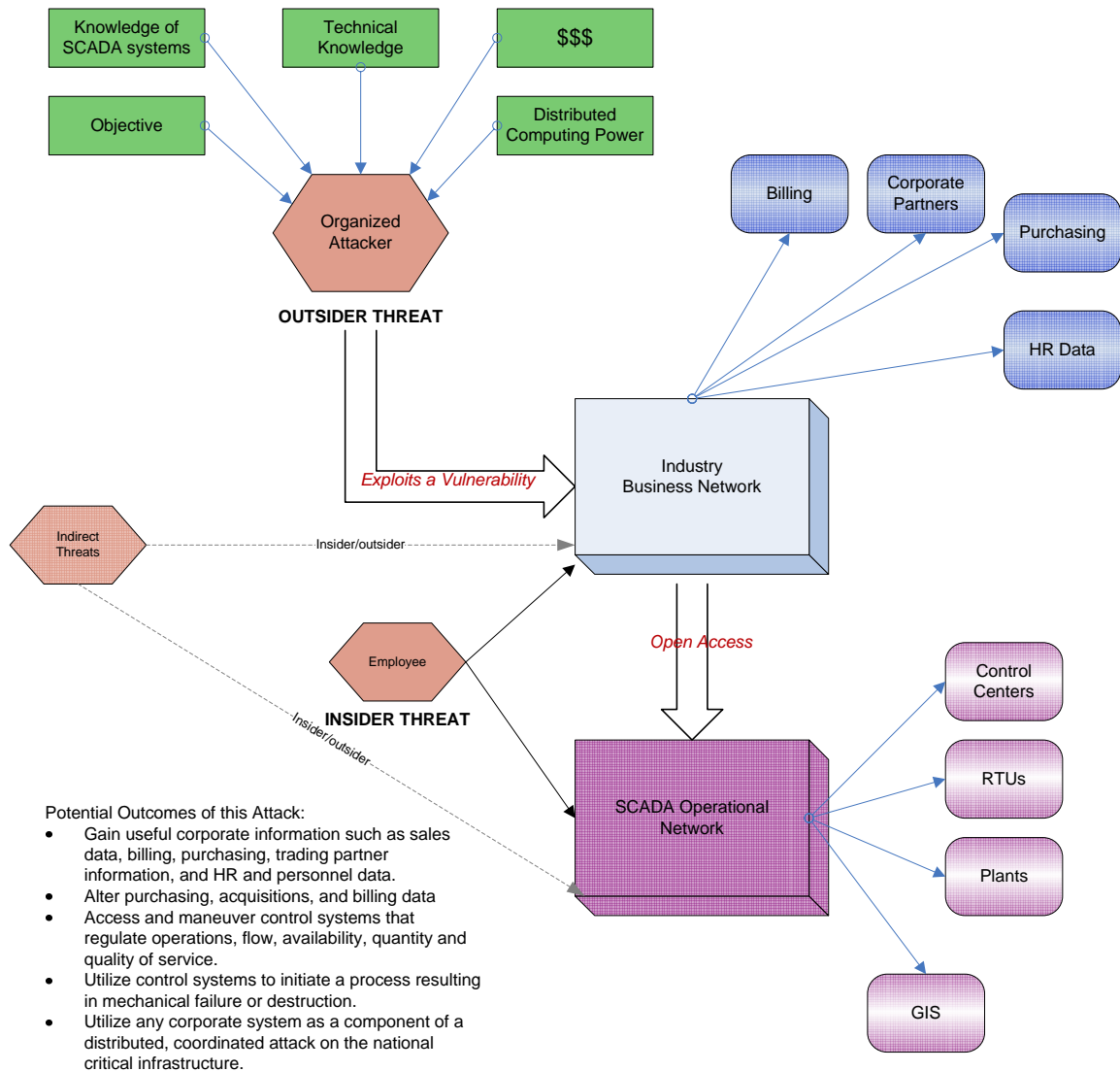


Figure 1: SCADA Attack Model

Figure 1 illustrates an attack and lists its potential effects, which include downtime, exploited information for financial gain, damaged trading or strategic partnerships, safety issues, and damage to infrastructure. Consequences and impact on business are addressed in later sections of this white paper.

As an example, once a threat accesses a SCADA system, often through a business system, it can be possible for the attacker to assume privileges as though they were a trusted insider. This control could potentially reach far beyond the business network into full control of SCADA systems that manage the lifeblood of the industry.

Although the illustrated attack may seem large in scale and comprehensive in scope, even one effect of this attack could have severe consequences. The motivation, resources, methods, and timeframe to carry out the attack are all determining factors in the success of the attack. Understanding that a threat exists and knowing the factors that can contribute to the success of an attack can provide industry with an awareness that leads to proper defenses and mitigations to reduce vulnerabilities and protect critical infrastructures.

In some instances, threats are not targeted toward an organization or one specific goal. For example, widespread worms and viruses can create overall slow-down and damage, but are generally not used to produce a specific effect on one organization. Likewise, untrained employees or accidents by employees can pose a threat to the organization by inadvertently creating security holes. These indirect threats should be considered when addressing security in SCADA operations in addition to threats with targeted, malicious intent.

### *3.2. Vulnerability Analysis*

A vulnerability is a weakness that exists in a system, network, application, or process that can be exploited by a threat to create an adverse effect. Examples of vulnerabilities can include open ports, unpatched software, dated virus protection, or exploitable system services. Vulnerabilities can be identified through a frequent assessment process or review and can be reduced by a variety of mechanisms. These mechanisms can include:

- Patches
- Access controls
- Secure designs
- Boundary and network controls
- Network protocols
- Monitoring
- Security plans and policies
- Physical controls

Vulnerabilities discussed at the I3P workshop include descriptions of broad categories as well as specific examples. These categories are outlined in the following table.

**Table 1: Characterized Vulnerabilities**

Vulnerability Category	Description and Examples
System Data	<ul style="list-style-type: none"> <li>• Lack of understanding of what data is considered sensitive, how it should be separated and protected.</li> </ul>
Security Administration	<ul style="list-style-type: none"> <li>• Lacking policies, standard procedures, training, and corporate/industry security plans.</li> <li>• Formal configuration management needed for upgrades, legacy plans, and patching.</li> </ul>
Architecture and Design	<ul style="list-style-type: none"> <li>• No integrated security in SCADA designs. Security must be an add-on.</li> <li>• Centralized storage or control mechanisms are single points of failure.</li> </ul>
Platforms	<ul style="list-style-type: none"> <li>• Patching, backups, passwords, OS security, application security, and security policies for access control and file sharing are needed.</li> <li>• Physical access control is lacking.</li> </ul>
Networks and Communications	<ul style="list-style-type: none"> <li>• Wireless security, monitoring, encryption, access control, boundary security, and standards for implementation are all needed.</li> </ul>
Incident Response and Handling	<ul style="list-style-type: none"> <li>• Response plans are lacking, as well as backup and disaster recovery plans.</li> <li>• Forensic data collection and analysis is needed.</li> <li>• Redundant operational capability is beneficial.</li> </ul>

Industry representatives reiterated specific vulnerabilities at the workshop. Below, these concerns are listed in no particular level of importance. However, these vulnerabilities could be used to begin a checklist for industry members in considering their own organization’s security posture. This list is not comprehensive, but may help identify main areas that create vulnerabilities or points of failure.

Industry Concerns:

- *Wireless Security*  
Lack of security in wireless connectivity and remote access to enterprise systems. Wireless security must be addressed as part of the enterprise architecture. There is 802.11 protocol in production fields, but a more secure, capable solution is needed across the infrastructure and in remote areas.

## DRAFT

- *Intrusion Detection*  
Lack of basic intrusion detection to include monitoring, event correlation, and alarms. This security control is essential to detecting and preventing attacks.
- *Understanding and Implementation of Security*  
Lack of a comprehensive view and implementation of security. Currently, there is sporadic or little implementation of controls across the system. One layer, such as a firewall, or physical security, is not enough to prevent an attack. A layered, comprehensive approach is necessary.
- *Legacy Systems*  
Many legacy systems that have interoperability issues or hardware and software constraints are still in use. These systems have minimal security controls and an inability to upgrade resulting in vulnerabilities without clear mitigation strategies and a weakening of the overall architecture. Addressing these legacy systems and developing a solution for protection is needed.
- *Standards*  
No widely accepted standard for security implementation in control systems exists. Therefore non-standard security controls are applied over a variety of domains, including business systems, process controls systems, and physical (site) security. A comprehensive, layered approach is needed. Guidelines for an enterprise approach to security would be useful.
- *Training and Awareness*  
Training and awareness of security configurations is necessary to prevent the incorrect implementation of security controls, such as firewalls.
- *Design*  
Basic security is not designed into SCADA systems, such as authentication, access control, and encryption. The need for add-on security can create implementation difficulties. Upgrades and added functionality to aging SCADA systems can result in the introduction of commercial technology that can add new vulnerabilities. Considering security at the beginning and through-out the SCADA system life-cycle is critical in continual, secure operations.
- *Network Structure*  
Many SCADA operational systems are connected to business networks within the enterprise. Without separation or controls placed between the architectures, attackers have a potentially exploitable access path to gain control over operations. Thus, the risk to business operations increases.
- *Policies and Plans*  
In addition to guidelines and standards in the approach to and implementation of security, enterprise level security policies and plans are needed to ensure security is implemented at the necessary levels of protection.
- *Incident Handling*  
Part of robust security includes data backups as well as the preservation and analysis of forensic data. Developing a plan for maintaining this data is important to understand and mitigate future attacks.

Understanding vulnerabilities and how they exist and evolve within an architecture is necessary when selecting and applying security protective measures. Vulnerabilities can be identified and reduced, but continual maintenance is required to safeguard elements of the architecture and operations as a whole. Vulnerability assessments are particularly useful in determining the current state and robustness of an organization's architecture. Identified technical vulnerabilities, however, are often not meaningful to management when making choices to invest in security. Vulnerabilities must be viewed as only one part of a whole when considering risk to SCADA systems and the organization. Different members of the organization, and of the industry, may have differing priorities. Awareness and communication is required to create a comprehensive security plan that prioritizes assets and provides guidelines for applying protective measures. Patches, maintenance and upgrades, virus protection, and application of basic security controls, are common methods of reducing vulnerabilities. To ensure the best protection, methods for identifying and eliminating vulnerabilities should be addressed at all stages of the life-cycle, with plans developed for on-going maintenance. The Effectiveness of Candidate Protective Measures section of this white paper discusses a layered approach to applying a comprehensive security plan.

### *3.3. Consequences*

Consequence is the resulting loss, damage, or impact resulting from a threat successfully exploiting a vulnerability. Consequences can include access and alteration of data, disruption of service, destruction of the system, and severe environmental and public health results of an attack. Based on the threats and vulnerabilities discussed, consequences to SCADA systems could potentially be severe due to physical and operational effects. Some consequences can have serious effects on business operations, to the industry as a whole, and to the national critical infrastructure.

Understanding consequences of a successful attack can help an asset owner identify areas of the architecture that need higher levels of protection and prioritize the deployment of protection mechanisms. The consequences of an attack have direct impacts on the organization or industry as a whole. These impacts include:

- Physical impacts that encompass the set of direct consequences of SCADA misoperation. The most devastating potential effects include personal injury or loss of life. Other effects include the loss of property (including data) or damage to the environment.
- Economic impacts are the resulting side effects of the physical impacts ensuing from an attack. Physical impacts could result in repercussions to system operations, which in turn inflict a greater economic loss on the facility or company. On a larger scale, these impacts could negatively affect the local, regional, national, or possibly global economy.

## DRAFT

- **Social Impacts or “Quality of Life”**  
Another side effect that is often overlooked is the consequence of losing national or public confidence in an organization or industry. It is, however, a very real objective and one that can be accomplished via a cyber attack.
- **Impact on National Critical Infrastructure**  
Industry sectors provide a part of the whole national infrastructure. Load adjustment, outages, and delayed purchasing and transportation, create secondary effects on the national infrastructure. Likewise, attacks on other industries in the national infrastructure can affect the oil and gas sectors. An example reiterated at the workshop is the reliance on the telecommunications industry.

The table below breaks down example consequences, effects, and overall impacts. If a threat exists that can exploit an existing vulnerability, any number of these consequences can occur.

**Table 2: Technical Effects and Resulting Impacts**

Technical Consequence	Effect	Impact
Access/ Read/Alter Data	<ul style="list-style-type: none"> <li>• Theft or alteration of corporate/industry data</li> <li>• Theft or alteration of critical operations data used for future attack</li> <li>• Theft of personnel data</li> <li>• Divulge corporate trading partner info</li> <li>• Billing and purchasing data changed</li> </ul>	<ul style="list-style-type: none"> <li>• Economic (i.e. loss of trading partner, market instability, downtime)</li> <li>• National Critical Infrastructure (i.e. weaknesses in operations may be exploited, downtime, unavailability)</li> <li>• Quality of Life (i.e. identify theft, negative publicity for corporate and industry)</li> <li>• Safety issues</li> <li>• Physical impacts to equipment</li> </ul>
Gain Control of SCADA Systems	<ul style="list-style-type: none"> <li>• Full operation of control systems</li> <li>• Can alter, stop, or destroy equipment and operations</li> </ul>	
Denial of Service	<ul style="list-style-type: none"> <li>• Halt operations on process control, business systems, or telecommunications</li> </ul>	
Access Systems as Jump-points	<ul style="list-style-type: none"> <li>• Use systems as part of a large scale, coordinated attack</li> </ul>	
Physical Access to SCADA Systems	<ul style="list-style-type: none"> <li>• Can physically damage systems</li> <li>• Access as a trusted insider if electronic access controls are not in place</li> </ul>	
Introduction of a Virus/Worm	<ul style="list-style-type: none"> <li>• Can slow or halt operations</li> </ul>	

While the table does not contain every potential consequence, it is important to understand how a threat with an opportunity can create negative consequences. For example, if a system that houses critical operational data is connected to the Internet via a business network and has no password requirement, an attacker can more easily gain access and alter data, halt or change operations, or possibly even cause destruction of critical components. Although this is a simplified example, this scenario has physical and economic effects to the organization and the industry. It can affect quality of life, create safety issues, and generally weaken the national critical infrastructure. As stated before, implementing defenses and designing secure operations are the proactive steps that industry members can take to prevent damage to their operational ability. Understanding components such as the network, the platforms, the system data, and operational policies can help in creating a layered approach to protecting the infrastructure.

### *3.4. Business Impacts and Return on Investment*

Determining the consequences of an attack based on analysis of threats and vulnerabilities is useful to understanding exactly what to protect on SCADA networks. However, it was recognized at the workshop that implementation of security controls is often an expensive task. There must be a visible return on investment to justify the expense of deploying additional security technology such as hardware, software, or physical controls. It is probably most analogous to insurance, although the financial benefit to stopping attacks on a daily basis is rarely quantifiable. Therefore an asset owner must consider the potential cost of not employing these controls. Downtime and the halted movement of oil and gas can be directly translated to loss of profit. To some extent, safety can also be quantified in the number and cost of accidents and injury. However, the social impacts such as quality of life and the effect on critical infrastructure at a national level are not easily measured.

For example, an organization must consider how they will be viewed by customers and the market if they suffer a publicized attack. Likewise, if a corporation's unsecured SCADA network is utilized as an entry point or active node in a coordinated attack on the national infrastructure, it can have devastating business consequences in addition to the infrastructure damage. This scenario is not unlike that of airline companies who have suffered a business loss or faced near bankruptcy due to eroding public confidence caused by a hijacking or safety-related crash. The price of inaction can be far costlier than implementation of security to the architecture.

A common argument is one of statistics. In wrestling with the cost of implementing security, many managers question the probability of a successful attack. However, media reports inform the public daily about terrorist cells attempting to gain more information on US infrastructures and of US intelligence agencies monitoring and quantifying reconnaissance attempts by known threats. Therefore acceptable risk determined by management must include consideration of any current or future threat of this kind. Some of the business impacts that should be considered in determining risk include:

- Downtime (production, delivery, and 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

Just as layered security can address complex technical weaknesses, a robust and well-rounded plan is needed to address business risk. This plan can assist in understanding why to implement security controls. Just as the technical aspects are multi-faceted, determining business risk can be equally complex, and conclusions can often be different based on an organization's function and priorities.

### *3.5. Effectiveness of Candidate Protective Measures*

Defenses against cyber attacks are most effective when applied in multiple layers of security. Currently, as can be seen in the industry concerns (see Section 3.2), security is being approached by piecemeal efforts. Often specific controls are implemented that only partially address protection, such as firewalls. Protection and defense must be viewed as a comprehensive task. Vulnerabilities can be mitigated and threats deterred by using a layered approach that groups areas of concern. These areas which require defense include:

- Data
- Applications
- Platforms and operating systems
- Networks and communications systems
- Boundary systems
- Control systems
- Physical access
- Standard operating procedures

Breaking apart these layers, organizations can map their processes and determine exactly what needs to be protected and how to defend it. These defenses and protective measures could include:

- |                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Access control</li><li>• Authentication</li><li>• Applied OS and platform security</li><li>• Data separation</li><li>• Functional separation</li><li>• Network design</li><li>• Encryption</li><li>• Patches, upgrades</li><li>• Monitoring and event correlation</li></ul> | <ul style="list-style-type: none"><li>• Backups and disaster recovery plans</li><li>• Alerting mechanisms to discover coordinated attacks</li><li>• Redundancy in connectivity</li><li>• Firewalls and perimeter security</li><li>• Secure remote access</li><li>• Trusted computing platforms</li><li>• Accepted metrics for risk characterization elements</li></ul> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

It has also been agreed that industry standards, government security guidelines, and information sharing would all assist in implementing and maintaining protective controls. In combination, these measures can provide the best defense against attack. Applying only one security control may do little to prevent or even slow down an attacker, perhaps increasing risk logarithmically. Industry should also require that protective measures be applied with SCADA operations as the focus. This means utilizing SCADA operational

## DRAFT

knowledge as the basis for implementing the best, most effect controls that promote operations while ensuring security. A close collaboration between IT, SCADA engineers, and management is required.

## 4. Sources of Input Data

The data used to develop threats, vulnerabilities, consequences, and business impacts was derived from several sources. These sources include industry perspectives voiced at the workshop, past assessments on SCADA networks, trends discussed in industry forums, and technical knowledge of SCADA threats and vulnerabilities by researchers.

### 4.1. Stakeholder Perspectives

Industry stakeholders are a diverse group and, as was seen at the workshop, have different views and priorities. Although many specific issues were discussed at the workshop such as firewall implementation and access control, a common theme was the need for understanding security across the organization and implementation across the enterprise as a whole. Awareness and understanding of threats, vulnerabilities, and consequences across different levels of the industry, including management, asset owners, engineers, and vendors, is critical to developing a comprehensive plan for security that mitigates business risk.

### 4.2 Gap Analyses

Gap Analyses have been performed as part of other I3P activities. These studies determine what technology and processes are available and in use today to secure operations and critical infrastructure. Understanding these gaps within an industry perspective allows SCADA researchers to determine which technologies developed to foster secure operations. Research on other I3P efforts includes cross-domain information sharing, metrics, and engineering risks. Knowledge on current states of operation was also gained from initial site visits, which will be continued throughout the I3P project. This data, leveraged from other I3P activities and workshop feedback, assisted the team in determining an overall picture of security within operations and how threats and vulnerabilities create business consequences and which mitigations should be applied.

### 4.3 SCADA Research

Knowledge and information was also leveraged from activities performed by SCADA researchers at Sandia National Labs. These activities include:

- Vulnerability assessments on SCADA architectures
- Red teaming of SCADA systems
- Operations research
- Threat research
- Coordination with industry

## 5. General Analysis

This paper described threats and factors that contribute to the expanded capability of these threats. Vulnerabilities and weaknesses were discussed along with the consequences that can occur if a threat exploits a vulnerability. A basic model for how these events occur can be illustrated.

$$\begin{array}{ccccccc} \text{THREAT} & \times & \text{VULNERABILITY} & \times & \text{CONSEQUENCE} & = & \text{RISK} \\ \text{Resources} & & \text{Weaknesses} & & \text{Effect} & & \text{Business Impact} \end{array}$$

**Figure 2: Cause and Effect of Attack**

What many feel is most important is the translation of consequences or effects into impacts on the business. If economic and safety effects are realized, it can create a more compelling case for implementing security controls. Because all threats cannot be eliminated and vulnerabilities continue to evolve, a layered approach to security and a comprehensive implementation plan is necessary. In creating a plan, however, it is useful for all those involved to understand the relevant threats, vulnerabilities, and consequences, and how they could affect each organization and the national critical infrastructure.

## 6. Summary and Conclusions

Individual comments made at the workshop were discussed in earlier sections of this paper. Common themes arose both with industry and with SCADA security researchers. For example, the need for a layered approach to security mapped to separated architectural areas is critical. Understanding the critical functions and data types and applying appropriate security controls to these areas according to their needs is essential for a comprehensive defense. The Sandia National Laboratories' paper entitled "A Reference Model for Control and Automation Systems in Electric Power" outlines these data types. In addition to the use of technology in security controls, a comprehensive and well-understood security plan is required. This plan should address physical, personnel, and information security, and should mandate as many controls as required to secure operations. In this plan, it is also necessary to address the life-cycle of technology. As operations and equipment evolve, security must be fluid and provide the functionality required by the current situation. In addition to life-cycle planning, legacy systems must be assessed and a methodology developed for either upgrading or replacing these systems.

In developing a plan and applying controls, forging a common understanding among different industry and organizational groups is paramount. This means creating awareness and discussion among all stakeholders to include asset owners, vendors, IT personnel, SCADA operators, and organizational management. Most industry members agree that problems exist and there is a need for a total solution. Involving and obtaining feedback from members across the enterprise can result in a security plan that is most effective while ensuring continuity of operations. Utilizing feedback from events such as the workshop creates an opportunity to build this solution. Awareness, planning, cooperation, information sharing, and implementation are steps that must continue.

In addition to technology and a security plan, industry members have expressed the need for standards or guidelines that can be used to build a security plan. The defense and financial sectors are examples of those using technology standards with the required supporting plan. These plans often include monitoring, disaster planning, and recovery. Other industries could be used as models for creating guidelines and standards for the oil and gas industry. An approach must be taken, however, that includes an operational focus, and avoid simply adding on technologies built to secure only IT components. Routine assessments and structured security enforcement are continual activities that also ensure effective, secure operations.

I3P will continue to identify and address these identified issues. This I3P effort will coordinate with other I3P activities and industry to develop ideas for comprehensive security. These activities will yield an accurate picture of the most important issues both today and in the future.

## 7. Appendix: References

- [1] *A Reference Model for Control and Automation Systems in Electric Power*, SAND2005-1000C
- [2] *A Scalable Approach for Critical Infrastructure Security*, SAND2002-0877
- [3] *Common Vulnerabilities in Critical Infrastructure Control Systems*, SAND2003-1772C
- [4] *Framework for SCADA Security Policy*, Dominique Kilman and Jason Stamp, SAND2005-1002C
- [5] *Generic Threat Profiles*, SAND2005-5411
- [6] "I3P National Cyber Infrastructure Bulletin," Vol.1, No.1
- [7] "I3P SCADA Security Workshop Raw Data Report"
- [8] "Industry Security Needs/Concerns," PPT Presentation
- [9] *Penetration Testing of Industrial Control Systems*, SAND2005-2846P
- [10] "Security Guidelines for the Petroleum Industry", American Petroleum Institute (April 2005), <http://api-ec.api.org/filelibrary/Security.pdf>
- [11] "Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition," American Petroleum Institute and National Petrochemical & Refiners Association (October 2004), [http://api-ec.api.org/filelibrary/SVA\\_E2.pdf](http://api-ec.api.org/filelibrary/SVA_E2.pdf)
- [12] *Sustainable Security for Infrastructure SCADA*, Jason Stamp et al., SAND2003-4670C