



Institute for
Information
Infrastructure
Protection

Research Report no. 9, May 2007

I3P Risk Characterization Report

Annie McIntyre

Sandia National Laboratories¹

Jason Stamp

Sandia National Laboratories

Ben Cook

Sandia National Laboratories

May 29, 2007

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.

Copyright © 2007. Trustees of Dartmouth College.

¹ Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

TABLE OF CONTENTS

| | |
|--|-----------|
| Table of Contents | 2 |
| Table of Figures | 3 |
| Executive Summary | 4 |
| 1. Introduction | 5 |
| 2. Sources of Input Data | 6 |
| 2.1. Stakeholder Perspectives | 6 |
| 2.2. Gap Analyses and Current States of Practice | 6 |
| 2.3. Control Systems Research | 7 |
| 3. Critical Observations..... | 7 |
| 3.1. Observations from Industry Workshops | 7 |
| 3.2. Observations from Site Visits..... | 9 |
| 4. Risk Characterization Process | 10 |
| 4.1. Threat Assessment..... | 11 |
| 4.2. Vulnerability Analysis | 13 |
| 4.3. Consequences | 15 |
| 4.4. Business Impacts and Return on Investment | 17 |
| 4.5 Effectiveness of Candidate Protective Measures | 18 |
| 5. Summary and Conclusions | 19 |
| 7. Bibliography..... | 20 |
| 8. Further Reading..... | 21 |

TABLE OF FIGURES

| | |
|--|----|
| Figure 1: Risk Characterization Components | 10 |
| Figure 2: Control System Exploit Model..... | 12 |

EXECUTIVE SUMMARY

Developed under the Institute for Information Infrastructure Protection's (I3P) control systems security research project, this white paper discusses risk characterization for control system operations in the oil and gas industry and summarizes major concerns voiced by stakeholders at the I3P workshops held in 2005-2007. The purpose of this risk characterization effort was 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 control systems in critical infrastructure sectors. In this paper, risk is characterized in terms of identifying threats, recognizing common vulnerabilities in control 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 control systems includes technical knowledge from control system researchers, stakeholder perspectives from the workshops, site visits, 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. A well-developed plan and layered approach to security can provide a manageable method to implement protective mechanisms and secure overall operations. 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

Over the past two years, the Institute for Information Infrastructure Protection (I3P) has engaged industry stakeholders to gain an understanding of their perspective on control system security. The objective of engaging industry was to better understand concerns, barriers, needs, and motivators for creating secure operations in a control system environment. To gather this information, the I3P hosted three Control Systems Security Workshops (June 2005, June 2006, and February 2007). These events gathered members of the oil and gas industry including asset owners, vendors, managers, researchers, and government participants. I3P initiatives, security concerns, and cyber risks for automation systems were discussed in briefings, panels, demonstrations, and breakout sessions. In addition to workshops, a series of industry site visits were conducted in 2005-2007. These visits provided important information about realistic control system architectures, challenges, and applications of security solutions.

This white paper discusses the risk characterization aspects for control system operations in the oil and gas industry and summarizes major concerns voiced at the workshops and site visits. All data gathered at the workshops and site visits contributed to the conclusions presented in this paper about control system security and characterization of risk. Risk is characterized in terms of threats, vulnerabilities, and consequences. Protective measures and business impacts are also addressed. 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 control systems in critical infrastructure sectors.

Primary objectives of the workshops and site visits included gaining an understanding from industry segments of the overall security state of control system networks, including:

- Security vulnerabilities and their trends
- The evolution of the industry's control system use leading to the current security state
- Impact of network convergence on security
- In-house capabilities for security
- Owners' expected options for security investment
- Potential consequences for control system tampering and their metrics
- Standards
- Major industry concerns and challenges now and in the future

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, vulnerabilities, and associated operational consequences that can 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 workshops, site visits, and from subsequent research is representative of industry's perspective and includes recognized current and future concerns, rather than speculative ideas, media output, or outsider/third party analysis.

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.

2. 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 workshops, site visits, past assessments on control system networks, trends discussed in industry forums, and technical knowledge of control system threats and vulnerabilities by researchers.

2.1. Stakeholder Perspectives

Industry stakeholders are a diverse group and, as was visible at the workshops and site visits, have different views and priorities. Although many specific issues were discussed at the workshops 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 making a compelling business case for action and also to developing a comprehensive plan for security that mitigates business risk.

2.2 Gap Analyses and Current States of Practice

Gap analyses and other research have been performed as part of related I3P activities. These studies determined what technology and processes are available and in use today to secure operations and critical infrastructure. Understanding these gaps from an industry perspective allows control system researchers to determine which technologies should be developed to foster secure operations. Research on other I3P efforts includes cross-domain information sharing, incident taxonomy, efficiency modeling, security metrics, interdependencies, and engineering risks. All research findings and documented results are located on the I3P website (www.thei3p.org) publications page. Knowledge on current states of operation was also gained from site visits. 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 could be applied to address these risks.

2.3. Control Systems Research

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

- Vulnerability assessments on control system architectures
- Red teaming of control systems
- Operations research
- Threat research and threat to consequence modeling
- Discussions with industry experts

3. Critical Observations

Critical observations from industry were gathered at control system security workshops held in 2005-2007 and also from industry site visits.

3.1 Observations from Industry Workshops

Members of the oil and gas industry (primarily represented by pipeline and refining operations) and vendor community voiced their concerns at all workshops. 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 2005 workshop [1].

Operators:

- A need exists for comprehensive security across the spectrum of their control systems, not just patches or rudimentary security controls on individual 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.
- Another need exists for overall intrusion detection and prevention. 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.

Vendors:

- 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 control system engineers are needed. Just as managers and operators must communicate and understand perspectives across the organization when deciding on and implementing security, IT personnel and control 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 at 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 control 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.

The 2006 workshop showcased each research area within the I3P control systems project. Feedback from industry was gathered in each area. Preliminary risk characterization results were presented during a session. In 2007, the workshop showcased tools, technologies, and methodologies resulting from the two-year research project. The 2007 workshop provided an opportunity to discuss specific applications of project results with industry and a means to match solutions with specific needs.

Over the past two years the importance of security and its role in operations has more accepted. A larger number of industry members are evolving their perspective of security and are developing the realization that any control system architecture, no matter the design, should be evaluated for its security. A continued increase in this way of thinking will promote secure operations throughout the industry. Other observations from 2006 [2] and 2007 [3] include:

- Asset owner/operators and vendors can have different expectations. Asset owners often expect security to be addressed by vendors, while vendors often expect a certain level of user awareness and operational security already in place.
- Some industry members still support the idea of industry standards. Many observations at the workshops indicated a desire for baseline security guidance. Industry members consider operational security from different architectures and different approaches. For those who are new to addressing security, a baseline guide with suggested approaches would be very helpful.
- Specific concerns over remote access, wireless, and communications backbones still exist.
- Metrics play an important role to industry. Asset owners/operators have a desire to know their current security posture. Metrics provide data they can analyze to determine where they stand on security and to support decisions on security investments.

3.2. Observations from Site Visits

During the course of the project, members of the I3P research team attempted to visit a representative cross-section of the oil and gas industry. For example, both large and small refineries were visited, along with both liquids and gas pipelines, and vendors. Resource limitations resulted in visits primarily to downstream facilities. Site visits normally consisted of a tour, a review of existing security controls, and a discussion about objectives and future plans. Several key conclusions from the site visits are listed below. This is not a comprehensive list or specific to a single site, but rather an aggregated set of conclusions.

- A secure design is key to many industry members. Implementing a secure design when the opportunity arises for an upgrade can be an effective, cost effective approach to security. Many industry members cannot redesign an architecture solely for security purposes. However, as new hardware, software, and communication mechanisms are added or changed, asset owners are taking this opportunity to employ security.

- Cyber security should be considered in the context of simply one more risk to manage. This risk should be addressed in the same method that environmental, safety, and weather risks are considered.
- Asset owners are often divided on the concept of a “bump-in-the-wire” security control. Some feel this is a solid approach to adding security, while others feel it is another component to consider that makes security even more complex, which could adversely affect reliability.
- Historically, security has been approached in a piecemeal approach, patching only what is needed. This has resulted in many complex and disparate architectures. Securing these architectures now is difficult. There is, however, a general resistance to completely standard architectures as these eventually produce standard vulnerabilities.
- The cost-benefit or return on investment is still extremely important when considering security. Manageability has also become an important consideration.
- The role of organizational communication is critical. Good communication between organizational groups (such as physical security, automation, and control system management) helps in building an effective way to implement and manage security. Understanding the objectives of each group and a collaborative effort ensures a better outcome.
- A balance between physical and cyber security is needed to achieve better operational security. Addressing access control, for example, from both a physical and cyber standpoint can result in a more secure solution.

4. Risk Characterization Process

The characterization process includes defining risk in terms of threat, vulnerability, and consequences, within the overarching context of control system operations. Many definitions of risk and contributing factors are presently available. Characterizing risk from an operational standpoint requires consideration of mission and organizational priorities such as safety and reliability. Figure 1 illustrates the relationship among these key pieces of the characterization process. Each component will be discussed in this section.

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

Figure 1: Risk Characterization Components

4.1. Threat Assessment

The goal of a threat assessment is to determine the likelihood of an attack against a given target. Threats to control systems as they pertain to the oil and gas sector 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 control 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 their level of access, motivations, and 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 control 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 control 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, organized crime, or hackers. Although individual hackers may have malicious intent and technical knowledge, organized cyber-terrorist groups may 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" [4]. 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 control system components, 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 control system networks become the primary line of defense. This defense ensures operations are not disrupted or compromised. Because these threats exist today and adversaries continue to gain resources and capability, industry must address this as a present and future issue.

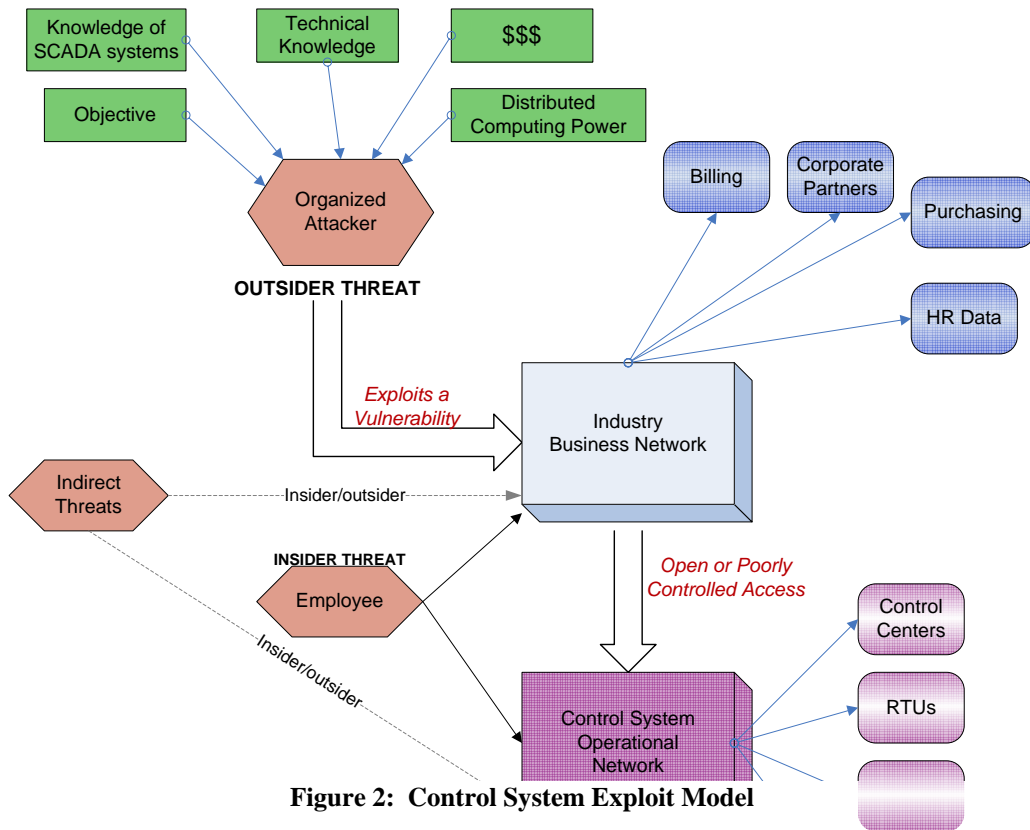


Figure 2: Control System Exploit Model

Figure 2 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 control system, often through a business system, it is 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 systems that manage the lifeblood of the industry.

Although the illustrated attack may seem large in scale and comprehensive in scope, even just one technical consequence of this attack could have severe impacts. 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 cause 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 control system operations in addition to threats with targeted, malicious intent.

4.2. 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 [5]:

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

Vulnerabilities discussed at the I3P workshops included descriptions of broad categories as well as specific examples. These categories are outlined in Table 1.

Table 1: Characterized Vulnerabilities

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

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 control systems and the organization. Consideration must also be given as to whether the estimated threat will exploit the vulnerability, and if exploited, and the possible resulting impact. 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 [6, 7]. The Candidate Protective Measures section of this report discusses a layered approach to applying a comprehensive security plan.

4.3. Consequences

Consequence is the 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 control 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 the potential 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 protective mechanisms. The consequences of an attack can have direct impacts on the organization or on the industry as a whole. These impacts include [5]:

- Physical impacts that encompass the set of direct consequences of control system misoperation. The most devastating potential effects include personal injury or loss of life. Other effects include damage to or 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.
- 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 plausible objective of an adversary and one that could be attempted via a cyber attack. These impacts can often lead to economic impacts as well.
- Impact on National Critical Infrastructure
The oil and gas sector represents an essential part of the whole national infrastructure. Product shortages, outages, and delayed purchasing and transportation create secondary effects on other segments of the national infrastructure. Likewise, attacks on other industries in the national infrastructure can affect the oil and gas sectors. An example reiterated at the workshops is the reliance on the telecommunications industry.

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

Table 2: Technical Effects and Resulting Impacts

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

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 operations. 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.

4.4. 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 control system networks. However, it was recognized at the workshops and site visits 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. Implementation of security within an architecture is often compared to the purchase of insurance. The probability of attack is unknown and 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 as well as the potential impacts of a successful cyber attack. Downtime and the halted processing or 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 control system network is utilized as an entry point or active node in a coordinated attack on the national infrastructure, it can have devastating economic consequences in addition to the infrastructure damage. This scenario is not unlike that of airline companies who have suffered a business loss or even 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 the implementation of effective security measures.

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, prediction and measurement of likelihood of an attack are unrealistic. When evaluating critical assets and processes, management must determine an acceptable level of risk. Although not quantifiable, managers should consider potential business impacts when determining this acceptable risk. These include [5]:

- 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

The use of security metrics in control system environments can assist in making the business case. Metrics that provide ongoing data, such as a dashboard, or metrics used in a snapshot assessment can provide valuable information. This includes the identification of critical assets, the valuation of processes, and the effectiveness of existing security controls. Analysis of this data can assist in implementing controls and security technology in the most critical operational or architectural areas. More information on security metrics for control systems can be found at the I3P publications website.

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

4.5 Effectiveness of Candidate Protective Measures

Defenses against cyber attacks are most effective when applied in several layers of security integrated into the overall system design. Unfortunately, observations suggest that security is often being approached by piecemeal efforts. Often, specific controls are implemented that only partially address protection, such as firewalls. The result is complex networks with separate protective measures that can require burdensome management. Protection and defense must be viewed as a comprehensive task approached one layer at a time. Vulnerabilities can be mitigated and threats deterred by using a layered approach that groups areas of concern [5][7]. The areas that require defense include:

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

Identifying these areas within architecture assist and asset owner in mapping their processes and determining exactly what needs to be protected and how to defend it. These defenses and protective measures could include:

- | | |
|------------------------------------|------------------------------------|
| • Access control | • Functional separation |
| • Authentication | • Network design |
| • Applied OS and platform security | • Encryption |
| • Data separation | • Patches, upgrades |
| | • Monitoring and event correlation |

- Backups and disaster recovery plans
- Alerting mechanisms to discover coordinated attacks
- Redundancy in connectivity
- Firewalls and perimeter security
- Secure remote access
- Trusted computing platforms
- Accepted metrics for risk characterization elements

Such an approach offers a comprehensive solution while addressing security in each critical area. This approach is often easier and more cost effective than applying a quick, point solution to an immediate problem, satisfying just one specific need. Understanding the architecture in place and matching this approach with the overall objectives of the organization can lead to a better application of protective measures. This also makes the task more manageable and can provide better return on investment.

It has also been agreed that industry standards, government security guidelines, and information sharing would assist in implementing and maintaining protective controls. In combination, these measures can provide the best defense against attack. Applying only random or minimal security controls may do little to prevent or even slow down an attacker, perhaps leading to increased risk. Industry should also require that protective measures be applied with control system operations as the focus. This means utilizing operational knowledge as the basis for implementing the best, most effective controls that promote operations while ensuring security. A close collaboration between IT, control system engineers, and management is required. A reiteration by industry throughout the project is the need for intra-organization communication. Historically, the most effective security exists in organizations with good communication and a clear understanding of each group's objectives. Finally, for details on the protection tools developed under the I3P project, fact sheets are available for review on the I3P website.

5. Summary and Conclusions

Risk can be considered in terms of threat, vulnerability, and consequence. To better characterize cyber risks to control systems, comments and concerns from asset owners, vendors, and researchers were gathered at I3P workshops and site visits. Defining potential threats, the range of possible technical vulnerabilities, and resulting impacts and consequences can provide a picture of overall risk. Consequences can have numerous outcomes for the organization. Business impacts translated from consequences are of particular interest to stakeholders. This multi-faceted view of risk can appear daunting. However, this approach to security (including identification of critical areas and processes, followed by dividing these areas into secure domains, and subsequently applying protective mechanisms or structure to these areas) creates a manageable method to address operations. Many tools are available that can assist stakeholders in securing operations. Methodologies, tools, metrics information, and other I3P products are available on the I3P website.

Applying appropriate security controls to critical areas and data types is essential for a comprehensive defense [8]. 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, control system 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 more 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 security plan. These plans often include monitoring, disaster planning, and recovery. These or other industries could be used as models for creating or revising guidelines and standards for the oil and gas industry. An approach must be taken, however, that includes an operational focus, and avoids 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.

The consideration of potential economic and safety impacts 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 are necessary. To effectively secure operations and manage business risks, it is essential that all members of an organization understand the relevant threats, vulnerabilities, and consequences outlined in this paper.

7. Bibliography

[1] Institute for Infrastructure Information Protection, "PCS Workshop," June 2005, Available at <http://www.thei3p.org/about/PCSworkshop05.html>.

[2] Institute for Infrastructure Information Protection, "PCS Workshop," June 2006, Available at <http://www.thei3p.org/about/pcspresentations0606.html>.

DRAFT

[3] Institute for Infrastructure Information Protection, “PCS Workshop,” February 2007, Available at <http://www.thei3p.org/about/pcspresentations0606.html>.

[4] D. Duggan, *Generic Threat Profiles*, Sandia National Laboratories Report, SAND2005-5411, July 2005.

[5] J. Stamp, “Drivers and Concerns for SCADA Security,” I3P 2005 Workshop Presentation, June 2, 2005.

[6] D. Duggan, *Common Vulnerabilities in Critical Infrastructure Control Systems*,” Sandia National Laboratories Report, SAND2003-4117P, November 2003.

[7] A. Baker, et al., *A Scalable Systems Approach for Critical Infrastructure Security*,” Sandia National Laboratories Report, SAND2002-0877, April 2002.

[8] J. Stamp, M. Berg, and M. Baca, *A Reference Model for Control Automation Systems in Electrical Power*,” Sandia National Laboratories Report, SAND2005-6286P, November 2005.

8. Further Reading

D. Kilman and J. Stamp, *Framework for SCADA Security Policy*, Sandia National Laboratories Report, SAND2005-1002C, 2005.

J. Stamp, et al., *Sustainable Security for Infrastructure SCADA*, Sandia National Laboratories Report, SAND2003-4670C, December 2003.

I3P National Cyber Infrastructure Bulletins, Various Issues, Available at http://www.thei3p.org/publications/nci_bulletin.html

American Petroleum Institute, “Security Guidelines for the Petroleum Industry”, 3rd Edition, API Publishing Services, Washington, DC, 2005. Available at <http://api-ec.api.org/filelibrary/Security.pdf>

American Petroleum Institute and National Petrochemical Refiners Association, “Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition,” API Publishing Services, Washington, DC, 2004. Available at http://api-ec.api.org/filelibrary/SVA_E2.pdf

A. McIntyre, J. Stamp, B. Cook, and A. Lanzone, “Workshops Identify Threats to Process Control Systems,” *Oil and Gas Journal*, October 2006.