Institute for
Information
Infrastructure
Protection

Research Report no. [ ], 2005

Process Control System Security Technical Risk Assessment: Analysis of Problem Domain

Peter Kertzner
The MITRE Corporation

Deborah Bodeau
The MITRE Corporation

Robert Nitschke
Idaho National Laboratory

Jim Watters
The MITRE Corporation

Mary Louise Young
Sandia National Laboratories

Martin Stoddard
Pacific Northwest National Laboratory

December 23, 2005

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.

PREFACE

The Institute for Information Infrastructure Protection (I3P) was founded in 2003 by the Department of Homeland Security (DHS) as a consortium of government, academic, and nonprofit institutions to coordinate research and development efforts in information infrastructure protection. The I3P is managed by Dartmouth College with funding from DHS and the National Institute of Standards and Technology (NIST). Partners include: the University of Illinois Urbana-Champaign, Massachusetts Institute of Technology's Lincoln Laboratory, the MITRE Corporation, New York University, Pacific Northwest National Laboratory, Sandia National Laboratories, SRI International, the University of Tulsa, and the University of Virginia.

The I3P has initiated a Supervisory Control and Data Acquisition (SCADA) research project that is investigating ways to advance the security of Process Control Systems (PCS), which are crucial to many critical infrastructures. Cyber threats against such systems must be addressed to ensure safe and efficient business operations and to support the national goal of critical infrastructure protection. The methodical assessment of risk to the operations of critical infrastructure entities, based on threats to and vulnerabilities of components of their underlying process control systems, will expose technical areas where safeguards may need to be strengthened. The result of a traceable path from exploited component to operational impact should strengthen and provide sufficient argument when making the business case for security improvements.

The I3P project has several tasks, including the development of a risk assessment methodology and tool to support the development of inherently secure process control systems. This methodology and tool will focus narrowly on technical security risks, that is, those associated with vulnerabilities in the design, implementation, and configuration of process control systems. To ensure near-term usefulness of research results, the I3P project is working with representatives of the oil and gas sector. The methodology and tool for PCS technical security risk assessment are being developed in cooperation with a representative industry organization. The risk assessment work is being performed in concert with research into metrics for PCS security. Technical security risks are by no means the only ones relevant to process control systems; other tasks under the I3P project will model security risks to large-scale systems from multiple perspectives, including operational and organizational, and will construct a risk management framework that addresses sector vulnerabilities associated with interdependencies.

This research report describes an initial approach to PCS technical security risk assessment, with attention to the problem of effective risk communication. This document lays the foundation for advancement of a process that focuses on the methodical assessment of risk such that the assessment results will be readily and easily communicable. The intended audience for the concepts and methods presented in this document includes both (1) the risk assessment team who must gather the data at the lowest levels and translate it into a form meaningful to corporate officers; and (2) the corporate officers who must understand and have confidence in the means used to obtain and present the information to them. Being able to communicate risk effectively, e.g., between a PCS LAN security manager and a corporate general manager, is essential to making the business case for improving PCS security.

EXECUTIVE SUMMARY

Process Control Systems (PCS) are crucial to many critical infrastructures, notably those in the oil and gas (O&G) sector. In the past, such systems were effectively isolated from sources of cyber threats external to their owners/operators. However, as enterprise systems evolve towards increasing integration, the need has increased for inherently secure process control systems: those that have been designed, implemented, and configured to minimize vulnerabilities to cyber threats.

Technical security risk analysis – the identification and assessment of risks associated with cyber threats that exploit vulnerabilities in a system's design, implementation, and/or configuration – is key to improving the security of systems throughout the system life-cycle. Technical security risk analysis is performed by technologists, but the results inform risk management decisions by upper management, who must view technical security risks in the larger context of business risks. This implies that connections between risks to processes supporting business operations and vulnerabilities inherent in the underlying process control system be recognized and understood. These connections can be difficult to understand and as a result, recommendations for mitigating vulnerabilities are often disregarded.

Keys to a better understanding of the relationships between vulnerabilities in PCS components and the business processes they support lie in how risk is assessed and how risk is communicated. The American Petroleum Institute (API) Standard 1164 and the National Petrochemical & Refiners Association (API/NPRA) Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries address the security assessment problem space defined by environments where process control systems are used. Targeted and specific refinements to components of these security assessment methods will aid upper management in understanding how technical risks could manifest as adverse impacts to their company's operation and business objectives.

Based on analysis of these and other security risk assessment methodologies, it can be concluded that a PCS technical security risk assessment methodology should:

- draw upon and be consistent with overall IT risk assessment methodologies, but avoid the biases of such methodologies towards confidentiality as the primary security goal
- address PCS architectures, technologies, components, and configurations as sources of technical vulnerabilities
- be consistent with the differently-scoped risk models being developed under the I3P project
- be consistent with the Security Vulnerability Assessment (SVA) or Instrumentation, Systems and Automation Society (ISA) methodology (that is, the correspondence between such risk modeling constructs as threats, vulnerabilities, and assets should be clear and comprehensive)
- be useful to those organizations that employ the SVA or ISA methodology, as a drill-down for the analysis and assessment of technical vulnerabilities and risks
- focus on technical risks to process control systems (including process control systems that are interconnected with or interdependent on IT systems), rather than on risks to IT systems
- facilitate the evolution of process control systems toward more inherently secure systems

ACRONYMS AND ABBREVIATIONS

AGA	American Gas Association
AIChE	American Institute of Chemical Engineers
API	American Petroleum Institute
CCPS	Center for Chemical Process Safety
CIDX	Chemical Industry Data Exchange
CMU	Carnegie Mellon University
CSVA	Cyber Security Vulnerability Assessment
DCS	Distributed Control System
DHS	Department of Homeland Security
HMI	Human Machine Interface
I3P	Institute for Information Infrastructure Protection
IAM	InfoSec Assessment Methodology
IED	Intelligent Electronic Device
IP	Internet Protocol
ISA	Instrumentation, Systems and Automation Society
IT	Information technology
LAN	Local Area Network
MMI	Man Machine Interface
MTU	Master Terminal Unit
NIST	National Institute of Standards and Technology
NPRA	National Petrochemical & Refiners Association
O&G	Oil and Gas sector
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
PCS	Process Control System
PLC	Programmable Logic Controller
ROI	Return on Investment
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SVA	Security Vulnerability Assessment
VAM-CF	Vulnerability Assessment Methodology for Chemical Facilities
WAN	Wide Area Network

TABLE OF CONTENTS

SECTION 1: INTRODUCTION

Process Control Systems (PCS) are crucial to many critical infrastructures, notably those in the Oil and Gas (O&G) sector. In the past, such systems were effectively isolated from sources of cyber threats external to their owners/operators. However, as enterprise systems evolve towards increasing integration, the need has increased for inherently secure process control systems: those that have been designed, implemented, and configured to minimize vulnerabilities to cyber threats.

Technical security risk analysis – the identification and assessment of risks associated with cyber threats that exploit vulnerabilities in a system's design, implementation, and/or configuration – is key to improving the security of systems throughout the system life-cycle. Technical security risk analysis is performed by technologists, but the results inform risk management decisions by upper management, who must view technical security risks in the larger context of business risks. This research report describes an initial approach to PCS technical security risk assessment, with attention to the problem of effective risk communication.

Communication of risk involves effectively informing stakeholders at all levels. From the technician performing the most fundamental tasks to the corporate officer charged with maintaining commercial viability, each audience has their own goals and concerns. The risk information must be clearly presented to them in those terms, and must also be consistent, well-founded and defensible. To support development of inherently secure process control systems, risk communication between those who assess risk to process control systems and the physical processes they monitor and control, and owners/operators of facilities to which those physical processes belong, must take place. In particular, plant managers must become aware of their exposure to undesirable business impacts through PCS technical security vulnerabilities. Ideally, this communication would include clear and credible rationale for risk assessment-based assertions of probable business impacts resulting from exploitation of vulnerabilities in PCS components.

A number of assessment methods developed by government, academia, and industry improve risk communication as a side effect of the assessment/reporting process. This paper is not intended to survey such methodologies. Similarly, a large amount of research has been performed on risk communication, particularly in the areas of health, safety, and environmental risks. (See, for example, (NRC 1989)). This report is not intended to survey such work. Rather, this report provides an analysis of impediments to good risk communication and identifies strategies for using technical security risk analysis to improve security in process control systems.

1.1 Need to Understand Technical Security Risks

Energy company owners/operators need a better understanding of the connection between risks to the production and distribution processes for energy products and vulnerabilities inherent in the process control systems controlling those processes, before they can make the commitment necessary to improve PCS security. No Return-On-Investment (ROI) case can usually be made; rather, enhancing cyber security serves to manage business risks associated with the second-order effects of cyber threats: loss of critical data, equipment malfunction, degraded or denied production or distribution. However, the relationship is typically subtle and complex, especially for large and multi-faceted operations. This often renders even the strongest connections all but invisible to anyone but a trained risk assessment professional.

As a consequence of this connection being difficult to understand, recommendations for mitigating vulnerabilities, or for applying sound design principles to architectures and systems, are frequently discounted, prioritized low, or even disregarded. Further, lack of an approach to illuminating cause-and-effect relationships, i.e., of exploited vulnerabilities, to resultant physical or business consequences, makes it more difficult for front line risk analysts to convey to corporate decision-makers risks to production and distribution operations in terms they would find useful.

Security of process control systems used in the oil and gas industry needs to be improved to safeguard production and distribution operations from intentional harm. Cyber attacks on process control systems, from Master Terminal Units (MTU) in control centers down to the field end devices they manage (e.g., RTUs, PLCs, IEDs), could lead to:

- Endangerment to human life and/or the environment
- Loss of profitability for the affected company
- Harm to the nation's energy production infrastructure

An owner/operator of an oil or natural gas company will appreciate a business case for investing in security when persuaded that without the investment, human life, the environment, or profitability could be harmed—this as a result of vulnerabilities in their process control systems being exploited. Better communication of the impacts compromised process control systems could have on corporate objectives will enable managers to better protect their interests from threats and minimize consequences should PCS vulnerabilities be exploited.

1.2 Keys to Understanding: Risk Assessment and Risk Communication

Understanding technical security risks involves two closely aligned activities—Assessment and Communication. The technical risk assessment involves all the hardware and software associated with the monitoring and control of a system, where, for example, that system could be defined as broadly as being an entire oil refinery, or as narrowly as being a single sensor or actuator attached to a PLC. Risk assessment problems in this dimension are suitably addressed by methods that take into account hardware/software vulnerabilities, threats in the form of exploits to systems possessing vulnerabilities, and consequences stemming from vulnerabilities that are exploited.

Risk communication between groups involves preparing and presenting risk information that is both convincing and motivating in terms that are directly applicable to them. Risk communication between assessment teams and corporate officers is greatly enhanced by risk assessment methods capable of translating *technical risk* into *business risk*, where that translation is via an industry-accepted algorithm and where risk to operations is expressed as *potential business consequences* both in financial terms and in terms that reflect an endangerment to human life and/or the environment. Potential solutions, acknowledging both the benefits and costs they will bring, must be a part of risk communication so that decision makers will have options that can be exercised.

Communication of risk involves effectively informing stakeholders at all levels. From the technician performing the most fundamental tasks to the corporate officer charged with maintaining commercial viability, each audience has their own goals and concerns. The risk information must be clearly presented to them in those terms, and must also be consistent, well-founded and defensible.

SECTION 2: THE PCS TECHNICAL SECURITY RISK ASSESSMENT PROBLEM DOMAIN

The PCS technical security risk assessment problem can be stated as follows:

> How can technical risks to PCS security be assessed, and how can the results of the assessment be communicated meaningfully to corporate decision-makers, so that enterprise process control systems can evolve toward greater inherent security?

Several aspects of the PCS technical security problem domain must be considered, to enable the definition of a methodology, and development of a supporting tool, to address this problem:

- The relationship between PCS technical security and Information Technology (IT) security
- PCS technologies
- The evolution of security risk assessment methodologies for PCS environments
- Sources of technical security risk in PCS environments

2.1 Relevance of IT Risk Assessment Methods

An approach frequently taken to address PCS technical security is to apply concepts and technologies for Information Technology (IT) security. Risk assessment methods and techniques have been devised and developed over the years, primarily within government and academia, in response to security risk management challenges facing IT enterprises. Three such methods are listed below for illustrative purposes. They are:

- The National Security Agency (NSA) InfoSec Assessment Methodology (IAM) (NSA undated)
- The National Institute of Standards and Technology (NIST) Risk Management Guide for Information Technology Systems (NIST 2002)
- The Carnegie Mellon University (CMU) Software Engineering Institute (SEI) Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) (Alberts 1999)

Each of these methods, and other similar methods not listed, has been used in different Department of Defense (DOD), national level agency, and industry settings with varying degrees of usefulness. They attempt to determine the amount of risk faced by enterprises, expressed in the traditional terms of information unavailability, corruption, and disclosure. Also considered by these assessment methods, albeit selectively, is the prospect of unauthorized physical access and its role in facilitating cyber attacks. However, the consequences from attacks on PCS components go beyond damage to information; they include physical process alteration, which could have dramatic operational, financial, and safety ramifications.

2.1.1 Risk Communication Issues

Because risk concepts of the IT domain are difficult to understand, they are also difficult to communicate effectively to non-IT professionals. Expanding the IT enterprise to now include computerized, network-ready physical control devices unfamiliar to IT risk professionals (e.g., physical sensors and actuators connected to programmable logic controllers) only compounds the risk communication problem. It is difficult for an organization to manage risks without everyone fully understanding what they are.

When assessing risk in PCS networks, the end focus should not be on abstract consequences such as a denial of service, but rather on tangible consequences from cyber attacks (e.g., the intentional malfunction of a PLC and its sensor and how that would affect an oil refining production step). There is a difference between the temporary unavailability of a network information server and a maliciously manipulated plant process that allows a volatile material to enter an unstable state. The difference between these two types of consequences is not lost on plant operators and must be effectively communicated with a credible basis for all assertions and consequences.

The seriousness of potential consequences from cyber attacks on process control systems argues that technical vulnerabilities in process control system components be unambiguously mapped to specific physical consequences that could manifest themselves should those vulnerabilities be exploited. Development of inherently secure process control systems will be facilitated by use of risk assessment tools and techniques that express risk in terms of impact on operations and then on business objectives. Communicating a better understanding of the likely consequences, given the prevailing threat environment of not developing inherently secure process control systems, will motivate greater consideration of recommendations for making these systems more secure. Obstacles to effective risk communication, such as the use of technical terms and abstract concepts when presenting assessment results to upper management, and not adequately explaining cause-and-effect relationships involving exploited components and their resultant impacts on operations, must be overcome in order to help justify needed security investments indicated through risk assessment and analysis.

2.2 PCS Technologies

A PCS technical security risk assessment methodology must facilitate analysis of a process control system throughout its life-cycle. It must identify and facilitate the identification of vulnerabilities in the PCS architecture and its underlying technologies and components, as designed, built, and operationally configured. The PCS architecture includes specification of the functionality of PCS components (increasingly in terms of standards) and of how components are assembled in interdependent ways. Within the O&G sector enterprises, process control systems evolve (rather than being replaced by new turn-key systems); changes are implemented gradually to minimize operational impacts. An organization's PCS architecture can be expected to change slowly. Therefore, in the near term, evolution toward inherently secure process control systems must focus on addressing vulnerabilities in components, their configurations, and their interdependencies.

Considerable guidance exists for security of IT components. However, that guidance is frequently irrelevant to the PCS environment in which real-time response is crucial to safety and operational performance. Security configuration guidance for the PCS environment is limited (see, for example, (NISCC 2005)). However, the development of more guidance can be expected. A PCS technical security risk assessment methodology must thus be capable of including or using such guidance.

Table 1 below identifies major PCS hardware and software components typically used in the monitoring and control of equipment within energy producing enterprises. Their likelihood of presence/use in control centers, remote stations, and plants is noted in the table. Together, they represent a core of potential sources of vulnerabilities and must be considered when modeling risk in energy production operations that use process control systems.

Table 1 PCS Technologies/Components

PCS Technology/Component:	PCS Point of Presence		
	Control Center	Remote Station	Plant
PCS / WAN interfaces	D	D	D
HMI/MMI (MTU/RTU)	D	M	D
Alarm subsystems	D		
Data archiving (database server)	P		
Links to operation's business network	P		
FEPs (front end processor/local data storage)	M	M	M
Internet connectivity	M		
Global control loops	M		
RTUs/IEDs/PLCs		D	D
Sensors		D	D
Control equipment and actuators		P	D
Local control loops		P	D
Comm protocols (e.g., ModBus, TCP/IP)	D	D	D
SCADA/PCS system software	D	P	D
Business network interface			M

Source: Sandia National Laboratories

Key: D = definitely have P = probably have M = may have

The PCS components described in Table 1 are used for monitoring and controlling business objects. A business object, as defined in the O&G sector, is typically hardware in substance (equipment) and is used to facilitate business objectives of an organization. In the case of an oil production enterprise, high-level business objects include:

- Platforms (sea-based)
- Wells (land-based)
- Pipelines (well to tanker/refinery, refinery to distributors/outlets)
- Tankers (transportation of oil (crude))
- Facilities (petroleum terminal (dock), storage, refinery, pumping/distribution)
- Retail outlets (gasoline, heating oil, jet fuel)
- PCS network

Business processes that rely on the availability and correct operation of these high-level business objects could be adversely affected through the exploitation of vulnerabilities in process control systems. Together, these objects represent potential business-level areas of impact that must be considered when constructing a process control system-centric model of business risk.

High-level business objects are not directly monitored and controlled by process control systems; rather, it is the underlying electro-mechanical business objects such as pumps, valves, switches and heaters that are. These objects are representative of the class of objects that mechanically instrument platforms, wells, refineries, etc., and are essential to production operations. Thus, they must also be considered when modeling risk in process control systems and to the high-level operations they support. These lower level business objects are what interface to PCS end devices (e.g., IEDs, PLCs, RTUs) and are therefore susceptible to malicious manipulation.

2.3 Security Risk Management Methodologies for Process Control Systems

Existing and emerging industry standards for PCS security address risk management to varying degrees.

- Security Vulnerability Assessment (SVA) Methodology for the Petroleum and Petrochemical Industries (API 2004c), which is an adjunct to the vulnerability assessment process defined in the Security Guidelines for the Petroleum Industry (API 2005)
- Risk analysis methodology described in Appendix B of API 1164 (API 2004b)
- Risk analysis methodology for integrating electronic security into the manufacturing and control systems environment (ISA 2004b)

Each of these methods is based, explicitly or implicitly, on IT security risk management methods. The National Institute of Standards and Technology *Risk Management Guide for Information Technology Systems* (NIST 2002) serves as a risk assessment/risk management framework from which the assessment/analysis methods cited above draw some of their techniques.

The Security Guidelines for the Petroleum Industry (API 2005) identify the following security vulnerability assessment methodologies, but allow for the use of other methodologies:

- the SVA methodology (API 2004c)
- API RP 70 *Security for Offshore Oil & Natural Gas Operations* (API 2003)
- API RP 70I *Security for International Oil and Natural Gas Operations* (API 2004a)
- USCG NVIC 11-02, relevant solely to specific types of facilities (USCG 2004)
- the American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS®) “Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites
- the Sandia National Laboratories Vulnerability Assessment Methodology for Chemical Facilities (VAM-CF)

No guidance is given on selecting a methodology, and these methodologies are scoped more broadly than cyber security. However, the Chemical Industry Data Exchange (CIDX) has defined a process for comparing Cyber Security Vulnerability Assessment (CSVA) methodologies, and applied this to nine methodologies (CIDX 2003). The comparison is based on (17) basic criteria, (11) desirable properties, and (4) nice-to-have properties for the methodology. One of the basic criteria is that the CSVA be “applicable to all types of computer systems (DCS, PLC, SCADA, Enterprise Network, Business LAN/WAN), and their support systems (Utilities, rack room, fire protection, environmental control and network connections), used at process plants.” While some of the methodologies CIDX compared met this criterion, the focus is not on technical security risks. Thus, it is unclear whether the existing methodologies compared by CIDX could be used to guide the development or evolution of process control systems toward inherent security.

Overall, the API Security Guidelines and SVA provide a useful structure for security risk assessment. The Security Guidelines (API 2003) focus on assessing risks associated with possible terrorist attacks. However, the SVA methodology defines four classes of threat sources:

- Terrorists (international or domestic)
- Activists, pressure groups, single-issue zealots
- Disgruntled employees or contractors
- Criminals (e.g., white collar, cyber hacker, organized, opportunists)

The SVA methodology also defines three threat types:

- Insider threats
- External threats
- Insiders working as colluders with external threats

The SVA methodology identifies critical assets; identifies, for each asset, critical functions and interdependencies; and assesses asset attractiveness to adversary. The SVA methodology provides blank forms for identifying and assessing assets, threats, asset attractiveness to threats, and for vulnerability identification, risk ranking, and countermeasure identification.

The scope of the SVA methodology is broad; cyber security is addressed as one area. Cyber countermeasures involve application of good IT security practices and do not address the cyber security concerns specific to process control systems. The SVA methodology "has been used extensively at a wide variety of facilities involving all aspects of the petroleum and petrochemical industry." (API 2004a) Thus, a PCS technical security risk assessment methodology should:

- be consistent with the SVA methodology (that is, the correspondence between such risk modeling constructs as threats, vulnerabilities, and assets should be clear and comprehensive)
- be useful to those organizations that employ the SVA methodology, as a drill-down for the analysis and assessment of technical vulnerabilities and risks.

In addition, however, a PCS technical security risk assessment methodology should:

- focus on technical risks to process control systems (including process control systems that are interconnected with or interdependent on IT systems), rather than on risks to IT systems
- facilitate the evolution of process control systems toward more inherently secure systems

ISA Technical Report 99.00.02, Integrating Electronic Security into the Manufacturing and Control Systems Environment (ISA 2004b), presents an asset-based methodology for performing security vulnerability and risk assessment for such systems. This methodology, like the accompanying technical report on security technologies (ISA 2004a), focuses on IT security technologies and vulnerabilities. However, a PCS technical security risk assessment methodology could use, or draw from, the assessment measures defined in this methodology.

The Natural Gas Security Committee of the American Gas Association (NGSC/AGA) references the NIPC Risk Management Guide (NIPC 2002) for an overall framework. The AGA's specific security guidance (AGA 2004) describes a high-level risk assessment process, consisting of Three Layer Analysis, Security Architecture Analysis, and Successive Compromise Analysis. However, this guidance does not address assessment or risk communication.

The risk models (risks to the infrastructure due to potential vulnerabilities in process control systems, risks of cascading effects resulting from system interdependencies and cyber attacks) being developed under other

I3P tasks (Lindqvist 2005) are not focused on technical security risks alone. However, a PCS technical security risk assessment methodology should be consistent with these models.

2.4 Sources of Technical Security Risk in Process Control Systems

Process Control Systems (PCS) used in past decades to instrument energy production facilities were by today's standards less prone to cyber attack. This was due largely to the use of proprietary communication methods to exchange information between field locations and the operations center as well as the PCS LAN's isolation from the corporate business LAN. Modern process control systems use open (i.e., standards-based rather than proprietary) technologies. While open technologies have helped improve Oil and Gas operations, they have also made those same operations less secure due to their newly acquired exposure to vulnerabilities exhibited by the open technologies being embraced.

Internet Protocol (IP) -based networks are examples of open technologies currently being used within a number of critical infrastructure sectors. Because IP-based PCS networks can be implemented easily and interconnect with corporate networks, they, in some cases, allow business users and corporate clients to gain access to field data directly. However, the connection of PCS networks to corporate networks and the Internet also exposes them to many more risks of attack and sabotage through viruses and other forms of malicious code. (Zonneveld 2004)

SECTION 3: CONCLUSION

This paper has described the problem of assessing and communicating technical security risks facing process control systems used in the Oil and Gas (O&G) sector. It has described the challenges facing a risk assessment team in making their results meaningful to a variety of corporate stake holders. It has identified desirable characteristics of a PCS technical security risk assessment methodology. Such a methodology should:

- draw upon and be consistent with overall IT risk assessment methodologies, but avoid the biases of such methodologies towards confidentiality as the primary security goal
- address PCS architectures, technologies, components, and configurations as sources of technical vulnerabilities
- be consistent with the differently-scoped risk models being developed under the I3P project
- be consistent with the SVA or ISA methodology (that is, the correspondence between such risk modeling constructs as threats, vulnerabilities, and assets should be clear and comprehensive)
- be useful to those organizations that employ the SVA or ISA methodology, as a drill-down for the analysis and assessment of technical vulnerabilities and risks
- focus on technical risks to process control systems (including process control systems that are interconnected with or interdependent on IT systems), rather than on risks to IT systems
- facilitate the evolution of process control systems toward more inherently secure systems

Risk assessment methods developed by the Oil and Gas Sector go a long way toward standardizing processes used within the sector to determine residual risks where there is a security program already in place. A standardization of risk metrics used in conjunction with the assessment methods, and a component-to-process risk mapping framework within which those metrics can be applied, will serve to strengthen business cases made for improving security for process control systems.

APPENDIX: REFERENCES AND BIBLIOGRAPHY

Alberts, Christopher J., Sandra G. Behrens, Richard D. Pethia, and William R. Wilson. September 1999. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), Framework, Version 1.0. Technical Report CMU/SEI-99-TR-017. Available at http://www.sei.cmu.edu/publications/documents/99.reports/99tr017/99tr017abstract.html

American Gas Association (AGA). August 2004. Cryptographic Protection of SCADA Communications: General Recommendations, Draft 3, AGA Report No. 12. Available at http://www.gtiservices.org/security/AGA12Draft3r6.pdf

American Institute of Chemical Engineers (AIChE), Center for Chemical Process Safety (CCPS). August 2002. Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites.

American Petroleum Institute (API). April 2005. Security Guidelines for the Petroleum Industry. Available at http://api-ec.api.org/filelibrary/Security.pdf

American Petroleum Institute (API). March 2003. API RP 70 *Security for Offshore Oil & Natural Gas Operations*, 1st Ed.

American Petroleum Institute (API). April 2004a. API RP 70I *Security for International Oil and Natural Gas Operations*, 1st Ed.

American Petroleum Institute (API). September 2004b. API Standard 1164 – Pipeline SCADA Security, First Edition.

American Petroleum Institute (API) and National Petrochemical Refiners Association. October 2004c. Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition. Available at http://www.npra.org/publications/general/SVA_2nd_Edition.pdf.

DOJ's - National Institute of Justice, EPA's - Chemical Emergency Preparedness and Prevention Office, Sandia National Laboratories, 2003, (VAM-CF) Vulnerability Assessment Methodology - Chemical Facilities. Developed in cooperation with the chemical industry and government agencies

ISA – The Instrumentation, System, and Automation Society and American National Standards Institute (ANSI). 2004a. Security Technologies for Manufacturing and Control Systems. ANSI/ISA-TR99.00.01-2004, ANSI, Washington, D.C.

ISA – The Instrumentation, System, and Automation Society and American National Standards Institute (ANSI). 2004b. Integrating Electronic Security into the Manufacturing and Control Systems Environment. ANSI/ISA-TR99.00.02-2004, ANSI, Washington, D.C.

Keimele M., S. Schmidt, R. Berdine, Basic Statistics – Tools for Continuous Improvement (Fourth Edition), Air Academy Press, ISBN 1-880156-06-7.

Ulf Lindqvist, SRI International. November 17, 2005. Securing Control Systems in the Oil and Gas Infrastructure: The I3P SCADA Security Research Project. Available at http://trust.eecs.berkeley.edu/pubs/11.html

National Infrastructure Protection Center (NIPC). November 2002. Risk Management: An Essential Guide to Protecting Critical Assets. Available at http://www.iwar.org.uk/comsec/resources/risk/risk-mgmt.pdf

National Infrastructure Security Co-ordination Centre (NISCC). February 15, 2005. NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, Rev. 1.4. Prepared for the United Kingdom NISCC by the British Columbia Institute of Technology (BCIT) and available at http://www.niscc.gov.uk/niscc/docs/re-20050223-00157.pdf

National Institute of Standards and Technology (NIST). July 2002. Risk Management Guide for Information Technology Systems. Available at http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

National Research Council (NRC). 1989. Improving Risk Communication. National Academy Press, Washington D.C.

National Security Agency (NSA). Undated. INFOSEC Assessment Methodology modules. Available at http://www.iatrp.com/modules.cfm

Stamp Jason, Phil Campbell, Jennifer DePoy, John Dillinger, and William Young, "Sustainable Security for Infrastructure SCADA", Sandia National Laboratories, May 17, 2004.

Stamp Jason, John Dillinger, William Young, and Jennifer DePoy, "Common Vulnerabilities in Critical Infrastructure Control Systems", Sandia National Laboratories, 2nd edition 11 November 2003.

Stoddard Martin, Deborah Bodeau, Rolf Carlson, Cliff Glantz, Yacov Haimes, Chenyang Lian, Joost Santos, James Shaw, Process Control System Security Metrics – State of Practice, I3P Research Report No. 1, August 2005. Available at https://www.thei3p.org/about/researchreport1.pdf

U.S. Coast Guard (USCG), August 6, 2004. CH-1 to NVIC 11-02, Recommended Security Guidelines for Facilities, COMDTPUB P 16700.4, NVIC 11-02 Change 1. Available at http://www.uscg.mil/hq/g-m/nvic/02/NVIC%2011-02%20CHANGE%201.pdf

Zonneveld Paul, Deloitte & Touche's Enterprise Security Risk Group. September 2004. "Taking Homeland Security to the Oil Field", Upstream CIO magazine.