

Process Control System Security Technical Risk Assessment Methodology & Technical Implementation

Peter Kertzner

The MITRE Corporation

Jim Watters

The MITRE Corporation

Deborah Bodeau

The MITRE Corporation

May 2006

Approved for Public Release; Distribution Unlimited. 06-0707

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© 2005. Trustees of 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. 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 strengthening safeguards could reduce cyber security, and hence business, risks.

The I3P project has several tasks, including the development of a cyber security 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 approach to PCS technical security risk assessment that facilitates effective risk communication. This document describes a process that focuses on the methodical assessment of cyber security risk as it relates to an organization's primary business objectives. 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. A well-defined methodology to assess technical cyber security risk in a methodical and logical way such that its interpretation as business impacts can be accurately and convincingly communicated to senior management is essential to improving the security posture of critical infrastructures.

EXECUTIVE SUMMARY

Process control systems (PCS) are crucial to many critical infrastructures, notably those in the Oil and Gas sector. In the past, such systems were effectively isolated from outside sources of cyber threats. 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.

An effective risk assessment methodology must improve understanding of the relationships between vulnerabilities in PCS components and the business processes they support. 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.

This paper describes a methodical and self-documenting approach to assessing risk. The approach is methodical in that it decomposes a selected set of business objectives into their constituent activities and then links those activities to potential sources of risk in data processing and control components of an underlying process control system. This assessment process creates as an artifact a multi-level relational matrix that records linkages between vulnerabilities in PCS network components and the business activities in which exploited vulnerabilities could find their expression. This matrix, in essence, serves as a model of an organization’s business functions and the possible risks individual business objectives face due to underlying process control system vulnerabilities. The vulnerability of a PCS network node, when considered with a derived, node-level measure of business value, can be interpreted as a risk measure for business activities that rely on the availability and proper functioning of that node. Adverse impacts to business activities is a concern of top management and the self-archival nature of the method advanced here makes available for inspection by all the analysis supporting, and rationale behind, conclusions reached regarding an organization’s exposure to risk.

This assessment process, with its creation of a comprehensive analytical model of the technical security risk component of business risk, provides needed understanding of the relationships between vulnerabilities in PCS components and the potential, adverse impacts on business processes those vulnerabilities could have when exploited through cyber attack. The I3P SCADA Security Project is currently working with an industry representative to refine and apply this methodology to an operational environment in the Oil and Gas sector. Additional industry partners are invited to participate in the refinement and tailoring of the methodology.

ACRONYMS AND ABBREVIATIONS

AGA	American Gas Association
AIChE	American Institute of Chemical Engineers
ANSI	American National Standards Institute
API	American Petroleum Institute
CCPS	Center for Chemical Process Safety
CDU	Control Distribution Unit
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
HPU	Hydraulic Power Unit
I3P	Institute for Information Infrastructure Protection
I/O	Input / output
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
RiskMAP	Risk-to-Mission Assessment Process
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
VPN	Virtual Private Network
WAN	Wide Area Network

TABLE OF CONTENTS

Preface	ii
Executive Summary	iii
Acronyms and Abbreviations	iv
Table Of Contents	v
List Of Figures	v
Section 1: Introduction	1
Section 2: Technical Security Risk Assessment Approach.....	2
2.1 Business Model Considerations.....	3
2.2 Developing the Business Model.....	4
2.3 Network Risk Model Considerations	4
2.4 Developing the Network Risk Model.....	5
2.5 Linking the Two Models	5
Section 3: RiskMAP Tool Design and Implementation – Description Through Example.....	7
3.1 Creating the Business Model.....	7
3.2 Creating the Network Risk Model	14
3.3 Mapping Risk from Network Nodes to Business Objectives	14
Section 4: Conclusions	21
Appendix: References and Bibliography	22

LIST OF FIGURES

Figure 1. Overview of RiskMAP Process	7
Figure 2. Matrix 1 - Business Objective Relative Weights	8
Figure 3. Business Objectives Arranged by Relative Weight.....	9
Figure 4. Matrix 2 – Task Relative Weight Based on Criticality to Each Business Objective.....	9
Figure 5. Operational Tasks Arranged by Relative Weight.....	10
Figure 6. Matrix 3 – Information Asset Relative Weight Based on Criticality to Each Task.....	11
Figure 7. Information Assets Arranged by Relative Weight (Top 30)	11
Figure 8. Matrix 4 – Network Node Relative Weight Based on Criticality to Each Information Asset	13
Figure 9. Network Nodes Arranged by Relative Weight (Top 30).....	13
Figure 10. Matrix 5 – Assigning Node Risks Due to Vulnerabilities	15
Figure 11. Mapping Risks from Node to Business Objective	16
Figure 12. Node Risks Overlaid on Node Weights.....	17
Figure 13. Matrix 4R – Mapping Node Risk to Asset Risk.....	17
Figure 14. Asset Risks Overlaid on Asset Relative Weights	18
Figure 15. Matrix 3R – Mapping Asset Risk to Task Risk	18
Figure 16. Task Risks Overlaid on Task Relative Weights	19
Figure 17. Matrix 2R – Mapping Task Risk to Business Objective Risk	19
Figure 18. Business Risks Overlaid on Business Objective Weights.....	20

SECTION 1: INTRODUCTION

Process control systems are rapidly evolving: from proprietary to standard protocols, from special-purpose hardware and software to common information technology (IT) products, and from isolation to interconnection with corporate business networks. While this evolution lowers costs and makes organizations that rely on process control systems more agile, it also makes those systems and organizations more vulnerable to cyber attack. Thus, the need to improve PCS security is increasingly urgent. (I3P 2003) To improve the inherent cyber security of process control systems, user organizations need technical risk management techniques. Technical risk management includes

- the identification, analysis, and assessment of risks associated with the design, implementation, and configuration of PCS technologies, components, and systems,
- the analysis of alternative risk mitigation strategies, and
- the communication of the results in non-technical terms to decision-makers who select the strategies that will best help them manage their risks.

The I3P SCADA Security Project is investigating ways to adapt and apply risk management techniques that can enable PCS stakeholders, particularly in the Oil and Gas sector, to improve PCS security in a cost-effective manner. (Lindqvist 2005) This report describes an approach to technical risk assessment of process control systems, to support stakeholders in the Oil and Gas sector – owners, managers, and operators of production and distribution facilities, vendors of PCS technologies and components, and systems integrators – in the improvement of the inherent cyber security of such systems.

As discussed in an earlier report (Kertzner 2006), existing and emerging standards for PCS security address risk assessment to varying degrees. The risk assessment methodologies defined in those standards are not focused on the technical risks associated with process control systems. Thus, the results of applying those methodologies will not guide the architecture, design, implementation, and configuration of process control systems to improve their inherent security. However, as noted in that report, the evolving PCS security standards environment, as well as experience with IT risk management, imply that a technical 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 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; and
- facilitate the evolution of process control systems toward more inherently secure systems.

This report describes such a technical risk assessment methodology for PCS security, and presents an example of its application to an oil refinery.

SECTION 2: TECHNICAL SECURITY RISK ASSESSMENT APPROACH

Security risk management involves the systematic identification, analysis, treatment (e.g., mitigation, acceptance, transfer), monitoring, and communication of risk. Key components of a security risk management process are risk analysis, in which a system, its components, and their relationships are analyzed with respect to threats and vulnerabilities; risk assessment, in which the level of risk is determined based on analysis and a well-defined approach to identifying and assigning values to risk factors, including possible consequences or impacts of threats; and risk communication, in which the results of a risk assessment are translated into terms that are meaningful to decision-makers. This section describes an approach for technical security risk assessment and risk analysis, i.e., for analyzing and assessing risks in which a cyber threat exploits a technical vulnerability in a process control system.

A variety of approaches to system security risk analysis and risk assessment have been taken:

- Policy-based approaches focus on security requirements, as stated in organizational policy documents, or in applicable regulations or standards. Failure to meet a requirement – typically, to implement a specific safeguard – constitutes a potential source of risk. In a policy-based approach, the consequences of such a failure are analyzed and assessed.
- Threat-based approaches focus on how an adversary could exploit technical aspects of a system (e.g., inherent vulnerabilities, poor configuration of key components), as well as non-technical aspects of the system’s operational environment, to produce adverse effects. Analysis, rather than assessment, predominates in a threat-based approach.
- Asset-based approaches focus on the assets that must be protected from threats. An asset-based approach includes identification of system components, as well as analysis of their interconnections and dependencies.
- Mission- or objective-based approaches focus on the missions or business objectives that must be achieved, despite the presence of threats. A mission-based approach includes identification of business functions and how those functions relate to (e.g., depend upon, impose requirements on) systems and their behavior.

Policy-based and threat-based approaches are of limited usefulness to technical risk assessment intended to improve the inherent security of process control systems against cyber threats. Policy-based approaches are most useful in a stable risk environment, i.e., when system architectures, designs, and configurations are standardized, threats are well known, and use of specific safeguards has been established as best practice. IT system risk assessment methodologies are frequently policy-based. As noted previously (Kertzner 2006), existing and emerging industry standards for PCS security that include system risk assessment methodologies build on IT risk methodologies. However, the risk environment for process control systems is not yet stable. Thus, a technical risk assessment methodology for PCS security should consider the safeguards identified in the documents

- Security Vulnerability Assessment (SVA) Methodology for the Petroleum and Petrochemical Industries (API, NPRA 2004c), which is an adjunct to the vulnerability assessment process defined in the Security Guidelines for the Petroleum Industry (API 2005)
- The American Petroleum Institute (API) standard on Pipeline SCADA Security (API 2004b)
- Guidance, developed with the goal of evolving to a standard, on integrating electronic security into the manufacturing and control systems environment (ISA 2004b)

as proposed rather than established practice. Threat-based approaches to cyber security are embodied in methodologies for penetration testing and Red Teams. However, such methodologies involve interaction

with, and possible destabilization of, operational systems. In the oil and gas sector, the potential impacts on operations make such approaches undesirable or infeasible, or impose constraints that limit the scope of such approaches. (Duggan 2005)

In 1997, The MITRE Corporation began developing a hybrid asset-based and mission-based risk assessment methodology. (Watters 1997) The RiskMAP (Risk-to-Mission Assessment Process) methodology has been applied to a variety of Air Force systems and can be applied to process control systems quite directly. When RiskMAP is applied to an organization, two models are developed, and then linked together to enable risk assessment and risk communication with business decision-makers:

- A business (or mission) model. In this model, organizational objectives (e.g., military missions, business objectives) are identified and their relative importance assessed. Operational tasks (or mission functions) are identified, mapped to the organizational objectives, and the relative importance of each task to each objective is assessed. Finally, information assets are identified, and the relative importance of each information asset to each operational task in which it is used is assessed. (An information asset is a discretely identifiable set of information (e.g., a database, a message or control signal), and is usually closely associated with one or more system components.) When completely developed, the business model identifies and assesses the value of the organization's information assets in a way that allows business decision-makers to understand how the relative values are assessed.
- A system (or network) risk model. In this model, technical assets are identified, and their associated vulnerabilities and threats are assessed, thus producing a risk measure for each technical asset. Technical assets include systems, subsystems, and components (as-configured hardware, software, and telecommunications), as well as instances of information assets that are created by, stored on, transmitted by or via, processed by, or otherwise handled by systems, subsystems, or components. Identification of technical assets can be done manually (e.g., by examining network diagrams and inventories of equipment and software licenses) and/or by using automated tools (e.g., network scanning, vulnerability scanning, configuration checking). Note that identification and assessment of technical assets can be performed manually, or supported by system design tools, for a system that is being designed or developed, and thus can improve the inherent security of such a system.

Using a business model in conjunction with a network risk model allows risk assessors to establish and demonstrate a mapping between risk to individual business objects and risk to operational, business, and safety objectives.

2.1 Business Model Considerations

The major goal of the business model is to ensure that the results of the technical security risk assessment can be expressed in terms of risks to business objectives. The RiskMAP technique organizes a company's activities and PCS/SCADA components in such a way that risks detected at the component level can be expressed as risks at the operations level. Operational risk can then, in turn, be expressed as business risk. This facilitates making the business case for improvements to PCS/SCADA security.

Whether the values assigned during the assessment are qualitative or quantitative depends on what is customary to the organization doing the assessment, the resources the organization can bring to bear, and the time available to do the assessment. Note that numeric values can be qualitative; for example, in the API 1164 risk assessment methodology, the benefit (or value) of a connection to a SCADA/control system is ranked from 1 to 5, while applications are assigned criticality values of low, moderate, significant, and mission-critical. Whether the assessment is qualitative or quantitative, the analysis and presentation must be clear, credible and meaningful to stakeholders at all levels.

For the Oil and Gas sector, a useful business model will identify corporate-level objectives such as:

1. Avoid injury to, or loss of, human life (from industrial accident)

2. Avoid damage to the health environment (e.g., from violation of safety and environmental law)
3. Secure profitability (especially over the long term)

Note that these outcomes are not unique to the Oil and Gas sector, but are also applicable to other critical infrastructure sectors such as chemical processing and electric power generation.

2.2 Developing the Business Model

Development of a business model of an organization involves interaction within that organization between managerial personnel and technical staff. These types of interaction in an oil refining or natural gas production setting could involve vice presidents, process/operations managers, network systems managers/ engineers, application analysts/users, PCS network/SCADA system operators, etc. The steps necessary to construct a business model that can be linked to a model representing risk in the supporting PCS/SCADA network are as follows:

1. Identify and assess the relative importance of organizational business objectives. For example, if the objectives are operate the refinery safely, comply with environmental regulations, and supply oil/gas reliably, assigned weightings would distinguish each objective from each of the others as being “more” or “less” important. It is possible for two objectives to be equally important.
2. Identify operational tasks (e.g., distill oil into useful products, deliver products to customers) and assess the relative importance of each task with respect to the organizational business objective(s) it supports. A task’s “importance” rating depends on whether the objective(s) it supports would be impacted should the task not be completed.
3. Identify information assets (e.g., databases, electronic status boards, control signals) and assess the relative criticality of each asset with respect to the operational task(s) it supports. An asset’s criticality rating depends on whether the task(s) it supports would be impacted should the asset not be available for use in the manner intended.
4. Identify the network nodes and assess the relative criticality of each node with respect to the information asset(s) it supports, be that in producing, storing, manipulating, or transferring the information asset(s). A node’s criticality rating depends on whether the asset(s) it supports would be impacted should the node not be available for use in the manner intended. Note that identification of network nodes is based on the network model, in which systems, sub-systems, and components are identified.

This mapping creates a way to express the impact of not having or not being able to use each network node in its intended manner, in terms of risk to organizational business objectives. For example, a refinery network might include a particular Input/Output device, a Control Processor, and an Operator’s Work Station, all needed to support information assets needed to perform the task of Performing Fractional Distillation. In this case, the information assets include key parameters like vessel pressures and temperatures, as well as flow rates of the products in and out of the vessel. These are operational parameters, but there should also be state-of-health indicators for each of the SCADA devices. All of the foregoing need to be available to keep the task from being degraded.

If any one of these information assets were to not be available for use in the manner intended, then the task of Perform Fractional Distillation would be degraded. Any risk of degradation in this task would show up as risk to one or more of the refinery’s business objectives.

2.3 Network Risk Model Considerations

The network risk model assesses the risk that a cyber threat will exploit a vulnerability in the system (usually, a vulnerability local to a node) to alter the behavior of, damage, or incapacitate a node. The network risk model must be based on a complete and accurate network model, which identifies network nodes (systems, sub-systems, and components) and their connectivity and functional dependencies. RiskMAP enables a mapping from network node risk to business objective risk. When RiskMAP is applied to process control systems, a

node is considered to be an electronic component (e.g., a computer, router, I/O device, PLC) supporting operations involving use of PCS technology, as described in Table 1 of an earlier report (Kertzner 2006).

In oil refining and natural gas production, fault-tree analysis techniques are regularly used for designing safe and reliable systems. Where fault-tree analyses have been performed, their results can and should be used to define, refine, or validate the network risk model. One result of mapping network node risk to business objective risk is the identification of “fault paths,” similar in concept to those resulting from application of fault-tree analysis to an appropriate system. Using RiskMAP, the relationships among, and logical connections between, PCS network nodes and the electro-mechanical devices they manage are evaluated for their criticality to the achievement of stated business objectives. These criticality measures play a prominent role in the calculation of overall risk posed by the PCS/SCADA network to an organization’s business objectives.

2.4 Developing the Network Risk Model

As previously discussed, risk can be expressed quantitatively or qualitatively. The RiskMAP methodology accommodates risk expressed in either form at the network node level, and generates results expressed in the same form at the business objective level. In either case, the risk model starts with a picture of the PCS/SCADA network that accurately shows all nodes with their connectivity, their identity, and their configuration including any safeguards already associated with them.

The steps necessary to construct a model of technical risk that will be linked to the organization’s business model are as follows:

1. List all of the vulnerabilities likely to apply to the components in the network, using whatever data source is deemed credible and appropriate by the organization.
2. Develop a consensus threat measure for each vulnerability, again using whatever data source is deemed credible and appropriate by the organization. Some analysts may choose to use a single, generalized threat measure for all vulnerabilities.
3. For each vulnerability identified, combine the vulnerability and threat measures to establish the risk level (high, medium or low) imposed by the vulnerability on each node in the network. Since this can be a daunting task, some analysts may choose to focus on the most important nodes as identified in the business model.
4. Identify safeguards that exist in the PCS/SCADA network environment applicable to the nodes identified but not taken into account in the previous steps.
5. For each applicable node, adjust the risk imposed by each vulnerability, based on the effectiveness of the safeguard(s) in the previous step, to produce a final risk measure for the node.
6. If a node is put at risk by more than one vulnerability, use the highest risk imposed as the value for Node Risk. As the application of safeguards reduces that risk below the level imposed by other vulnerabilities, use the highest remaining risk imposed on the node as the value for Node Risk.

2.5 Linking the Two Models

The development of the business model has produced a list of network nodes, rank ordered from most to least critical to business objectives. The analyst has identified the vulnerabilities associated with each node and entered a level of risk for each node. The risk model now uses the relationships established in the business model to map the risks from the node to each information asset the node supports, and to each operational task the asset supports, and to each business objective the task supports. A complete, combined-model risk map provides traceable paths from business risk (and projected impacts) at the business objective level back to, or down to, culprit technical risks existing within the PCS/SCADA network. This is illustrated in Figure 1, in the next section.

A basic outline for completion of the method is described below.

1. Map PCS/SCADA network system-level impacts (e.g., loss of a control device or of vital information) to major production activities and possible consequences (e.g., reduced refining capacity) making use of real-world examples.
2. Prioritize results (severity of consequences) based on the relative importance of business objectives, their supporting operational tasks, and their required information assets.
3. Use the risk model to identify the source(s) of any unacceptably high risk to business objectives, tasks, or assets. Next, select potential safeguards to apply to the network nodes, to mitigate the vulnerabilities imposing the excessive risk. When applying a safeguard to a node, adjust the node risk to reflect the application of the safeguard and then view the effect on the asset, task, and business objective risks. Repeat this process until the remaining risks are at an acceptable level, keeping a running total of the costs of using the various safeguards. Use the same approach to investigate alternative sets of safeguards and their comparative costs.
4. Ensure that the expression of assessment results includes the risk facing all of the corporate business objectives, and also includes the costs and the risk reduction for each recommended set of safeguards.

A tool-based implementation of this method will enable facility owners and operators to collaborate with their risk assessment specialists in value weighting their plant processes and information assets. With that in hand, they can identify the true critical nodes in their process control system and develop a cost-effective risk mitigation strategy. The MITRE Corporation has prototyped for use in the oil and gas sector a RiskMAP tool based on a system of linked, Excel¹ spreadsheets with embedded calculating formulas.

¹ Excel is a registered name of the Microsoft Corporation.

SECTION 3: RISKMAP TOOL DESIGN AND IMPLEMENTATION – DESCRIPTION THROUGH EXAMPLE

Owners and operators of oil refining and gas production/pipelining businesses are seeking ways to improve the assessment of risks to operations posed by vulnerabilities in their process control systems. Improvements to the assessment of business risk will be aided by a process that maps risks associated with underlying PCS network nodes to the production processes they support. The rigor necessary for performance of a risk mapping function will at the same time provide needed credibility for consideration and acceptance of results. An assessment begins with development of a business model for an organization and a risk model for the network; it concludes with the combining of the two models to enable mapping between network risks and business interests. Figure 1 below illustrates the use of the combined business and risk models in the RiskMAP process.

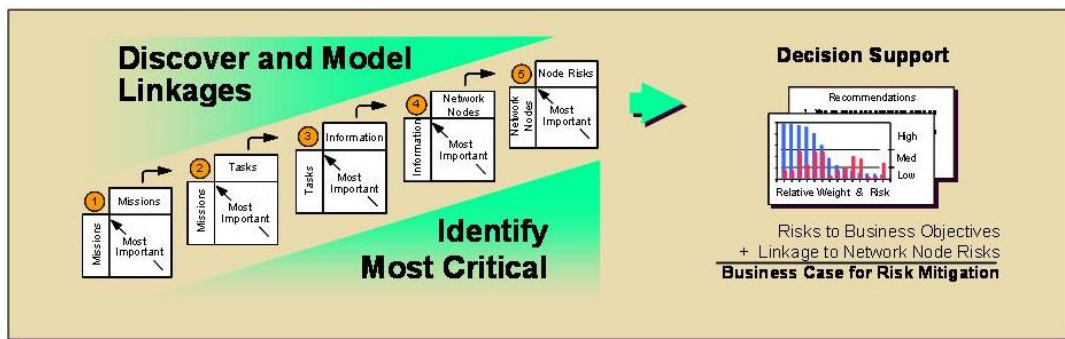


Figure 1. Overview of RiskMAP Process

The example that follows demonstrates an application of the RiskMAP assessment method to the operation of a company whose business is to refine crude oil into useful consumer products. The business objectives of oil refiners may vary across the industry, owing to special market niches and unique business relationships. For the purpose of this example, it is assumed that the business objectives shown below are common to most oil refiners. They serve to represent the overall goals of an operation to which the RiskMAP assessment method is being applied.

3.1 Creating the Business Model

To create a business model, a series of four matrices are used to capture and relate organizational objectives, supportive operational tasks, essential information assets (electronic in form) and network nodes that support them. The matrices developed for this project are applicable to most commercial refineries and are sufficiently complete so as to allow their use as templates, requiring only minor adjustments by individual users. A similar set of matrices will be developed for companies that produce and pipeline natural gas.

The business model presented below was developed up through Matrix 3 in collaboration with an industry representative oil refiner. Matrix 4 will be completed as part of the ongoing risk assessment of that refiner's operation. Matrix 4 in this report contains hypothetical data. It organizes a typical refining operation into a set of high-level business objectives, a larger set of supportive operational tasks, and a still larger set of information assets upon which operational tasks depend. Establishing relationships between entities at successive levels gives rise to a multi-dimensional criticality model of production processes common to refiners. Later, according to the RiskMAP method, measures of risk associated with the PCS/SCADA network components that monitor and control production processes, will be applied to the business model.

In constructing a business model, top-level business objectives are identified and rank ordered with respect to the overall goals of the organization. This process usually involves plant management, but may also involve plant operations personnel. Business objectives identified and their relative significance weightings are

entered into the non-shaded cells of Matrix 1. (Values that appear in shaded cells are the result of an auto-fill encoding embedded in the spreadsheet-based matrix.) The objectives used are those found to be common to oil refining companies:

- Operate safely,
- Improve profitability,
- Stay in compliance (with environmental regulations), and
- Supply customers well.

Figure 2 shows these objectives in a completed example of Matrix 1, after cognizant corporate representatives have considered the relative importance of each objective with respect to the others (an exercise which frequently reveals previously-unarticulated differences in the perspectives of the representatives, and which is also vital to the eventual credibility of the final results of the risk assessment). The weighting scale shown in Matrix 1 is only a guide. As evident in Figure 2, other values may be inserted in the non-shaded cells. The formulas embedded in the shaded cells calculate the remaining quantities as functions of the values entered by the analyst.

SCALE:							
1 = Row is EQUALLY IMPORTANT to Column							
2 = Row is SLIGHTLY MORE IMPORTANT than Column							
4 = Row is SIGNIFICANTLY MORE IMPORTANT than Column							
8 = Row is FAR MORE IMPORTANT than Column							
(Use reciprocals for LESS IMPORTANT cases)							
		Stay safe	Stay profitable	Stay in compliance	Supply customers well	Sums	Normalized Relative Weights
Stay safe		1	1.25	1.75	2	6.000	0.348
Stay profitable		0.8	1	1.4	1.6	4.800	0.279
Stay in compliance		0.571	0.714	1	1.143	3.429	0.199
Supply customers well		0.5	0.625	0.875	1	3.000	0.174
Total >>						17.229	1.000

Figure 2. Matrix 1 - Business Objective Relative Weights

Figure 3 is the Pareto graphical view of the business objectives and their relative weights, sorted left-to-right from most important to least important. The Pareto view has proven to be an important visual aid during the process of assigning the relative weights. Corporate executives find the visual representation helpful when making sure that the assigned weights correctly represent the corporate values. By personally fine-tuning the entries in Matrix 1, corporate executives are able to satisfy themselves that the RiskMAP business model has a valid starting point. This is crucial to corporate buy-in and also sets the tone for the rest of the assessment.

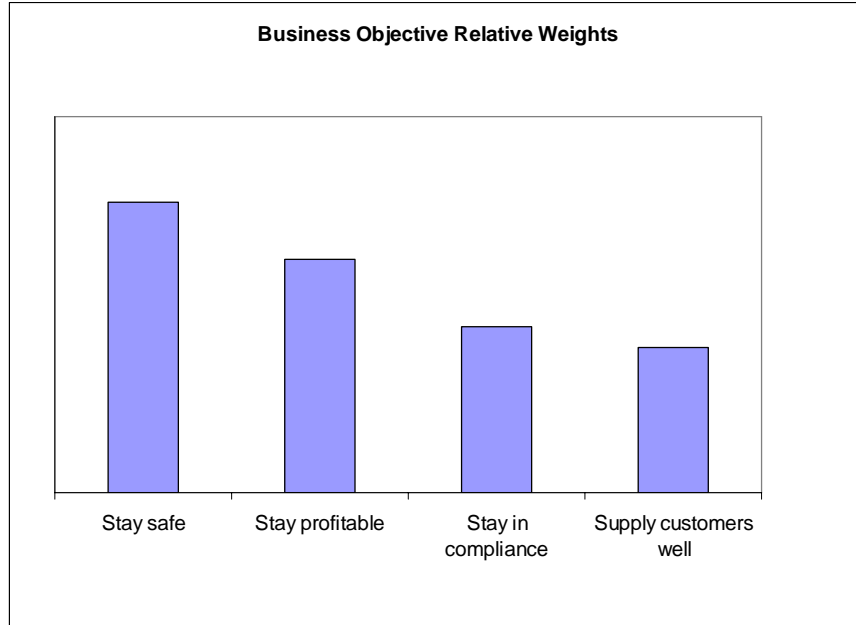


Figure 3. Business Objectives Arranged by Relative Weight

In the second step of developing the business model, operational tasks are identified and mapped to business objectives. Thus, the business objectives appearing in Matrix 1 become row headings in Matrix 2. The assessment team identifies the major operational tasks and uses them as column headings. This process involves collaboration between operations personnel and process engineers. Each operational task is evaluated against each business objective for criticality, with the end result being a list of weighted operational tasks.

Figure 4 below is a completed example of Matrix 2, showing the operational tasks determined by industry experts to be common to oil refining companies. Task relative weights are calculated as the sum of the products of the row Relative Weights with the column Criticality entries. For example, as shown in the highlight in Figure 3 below: $(0.348 * 4) + (0.279 * 6) + (0.199 * 4) + (0.174 * 4) = 4.56$.

Mission Impact from Loss of Task: 0 = No Impact on Achievement 2 = Objective Achievable Using Work Around 4 = Objective Degraded Even With Work Around 6 = Objective Not Achievable at all		Task Rel	1	2	3	4	5	6	7	8	9	10	11	12	13	14
		Wt	4.56	4.56	3.49	3.30	2.61	2.59	2.16	1.81	1.81	1.81	1.65	1.30	0.91	0.56
Task	Acquire Natural Gas															
	Acquire Water															
	Receive Causitic															
	Acquire Electrical Power															
	Quality Test During Loading															
	Impurity Removal															
	Blend & Load Lube Oils															
	Perform Fractional Distillation															
	Perform Hydro-Treating															
	Quality Test During Processing															
	Load Other Products															
	Unload & Store Crude															
	Bill for Product															
	Acceptance Test Crude															
Mission Objective		M.O. Rel Wt														
1	Stay safe	0.348	4	4	4	2	0	4	0	0	0	0	0	0	0	0
2	Stay profitable	0.279	6	6	2	4	4	0	4	4	4	4	2	2	2	2
3	Stay in compliance	0.199	4	4	6	4	4	6	0	0	0	0	2	2	0	0
4	Supply customers well	0.174	4	4	2	4	4	0	6	4	4	4	2	2	2	0

Figure 4. Matrix 2 – Task Relative Weight Based on Criticality to Each Business Objective

Figure 5 below is the Pareto view of the operational tasks of Matrix 2. The representation gives an immediate impression of which refining tasks are considered to be most critical to achieving business objectives. In this example the two most critical tasks are the acquisition of natural gas and the acquisition of water. As in the case of Matrix 1, developing this view helps the refinery team members to identify, validate or refine, and reach consensus on assumptions that had previously been unspoken or incomplete.

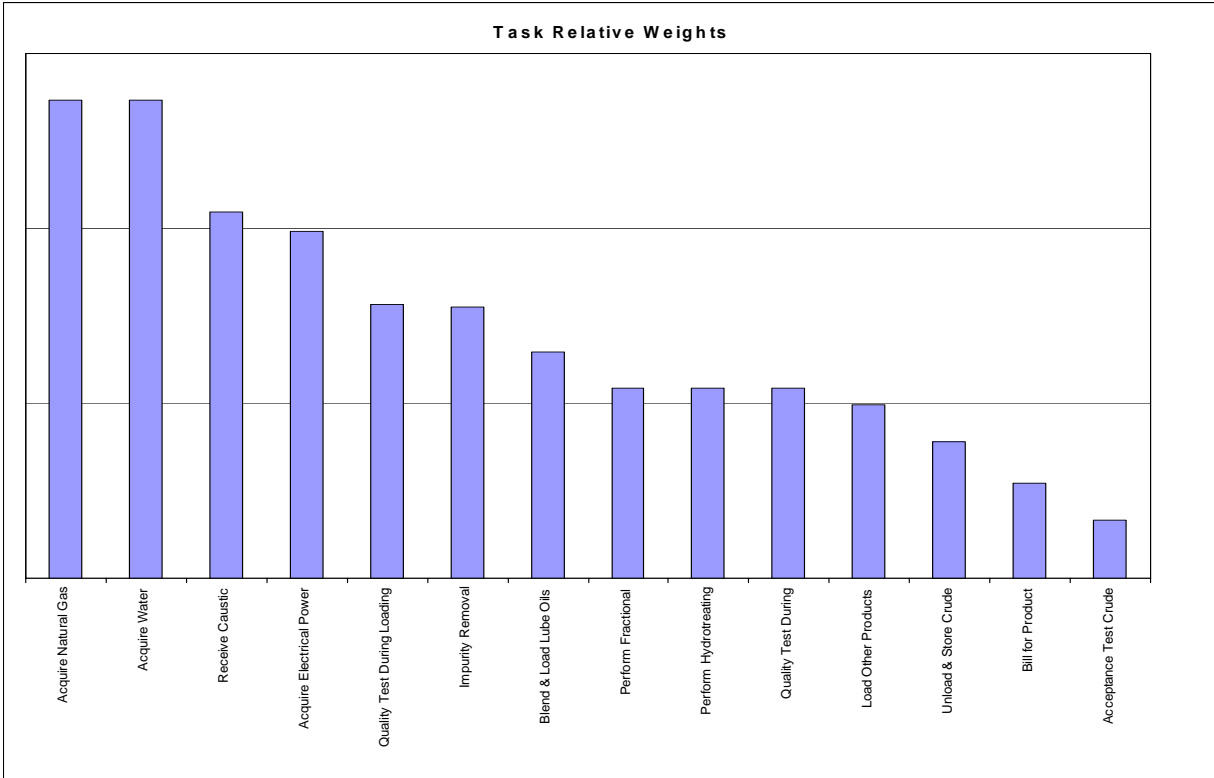


Figure 5. Operational Tasks Arranged by Relative Weight

In the third step of developing the business model, information assets are identified and assessed. Thus, the prioritized operational tasks appearing in Matrix 2 become row headings in Matrix 3 and column headings are filled in with the names of information assets. Information assets that support each task are identified through a collaborative process involving process engineers, applications analysts, and operators. Each information asset is evaluated against each operational task for criticality, with the end result being a list of weighted information assets ordered left to right from most critical to least.

Where large numbers of like information assets are present (e.g., several hundred control commands) they are grouped by system (e.g., CDU, HPU, Utilities) and then by equipment type (e.g., columns, pumps). That allows the representation of thousands of individual information assets in far fewer entries in Matrix 3.

For the example model described in this paper, information assets identified by industry professionals include the following types:

- *<system> <equipment>* Safety Sensor Output
- *<system> <equipment>* Safety Command
- *<system> <equipment>* Control Sensor Output
- *<system> <equipment>* Control Command
- Load Test Outcome
- Clerk Instructions To Loading Rack
- *<system> <equipment>* History Sensor Output
- Product(S) Order

- Natural Gas Incoming Pressure
- Water Incoming Pressure

Figure 6 below is a partial representation of a completed Matrix 3. It shows the operational tasks from Matrix 2 on the left side and some of the identified information assets arrayed across columns in a left to right descending order of criticality to tasks. The weights are calculated as shown for Matrix 2.

Task Impact from Loss of Asset:		Asset Rel Wt																													
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
0 = No Impact on Task																															
2 = Task Completable Using Work Around																															
4 = Task Degraded Even With Work Around																															
6 = Task Cannot Be Done At All																															
	Information Assets	Util Pump Safety Sensor Output	Util Pump Safety Command	Util Storage Safety Sensor Output	Util Storage Safety Command	Util Separators Control Sensor Output	Util Separators Control Command	Util Compressors Safety Sensor Output	Util Compressors Safety Command	Lead Test Outcome (pass, fail)	HPU Pump Safety Sensor Output	HPU Pump Safety Command	HPU Fired Heater Safety Sensor Output	HPU Fired Heater Safety Command	HPU Special Safety Sensor Output	HPU Special Safety Command	HPU Compressors Safety Sensor Output	HPU Compressors Safety Command	Util Fired Heater Safety Sensor Output	Util Fired Heater Safety Command	Util Fired Heater Control Sensor Output	Util Fired Heater Control Command	Util Electrical Safety Sensor Output	Util Electrical Safety Command	Util Pump Control Sensor Output	Util Pump Control Command	Util Storage Control Sensor Output	Util Storage Control Command	Util Compressors Control Sensor Output	Util Compressors Control Command	HPU Pump Control Sensor Output
	Tasks	Task Rel Wt																													
1	Acquire Natural Gas	4.557																													
2	Acquire Water	4.557																													
3	Receive Caustic	3.493																													
4	Acquire Electrical Power	3.303																													
5	Quality Test During Loading	2.807								6													6	6							
6	Impurity Removal	2.587	4	4	4	4	4	4	4	4																					
7	Blend & Load Lube Oils	2.159								4																2	2	2	2	2	2
8	Perform Fractional Distillation	1.811	6	6	4	4	4	4	4	4																4	4	4	4	4	4
9	Perform Hydrotreating	1.811	6	6	4	4	4	4	4	4																4	4	4	4	4	4
10	Quality Test During Processing	1.811									6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	
11	Load Other Products	1.652																													
12	Unload & Store Crude	1.303																													
13	Bill for Product	0.905																													
14	Acceptance Test Crude	0.557																													

Figure 6. Matrix 3 – Information Asset Relative Weight Based on Criticality to Each Task

Figure 7 below shows the Pareto view of the top 30 Information Assets, as calculated in Matrix 3. Again, this view serves to help the viewer identify the most critical items as those on the left side of the chart. Because the information assets were classed by system and by equipment, it is possible to see patterns emerging.

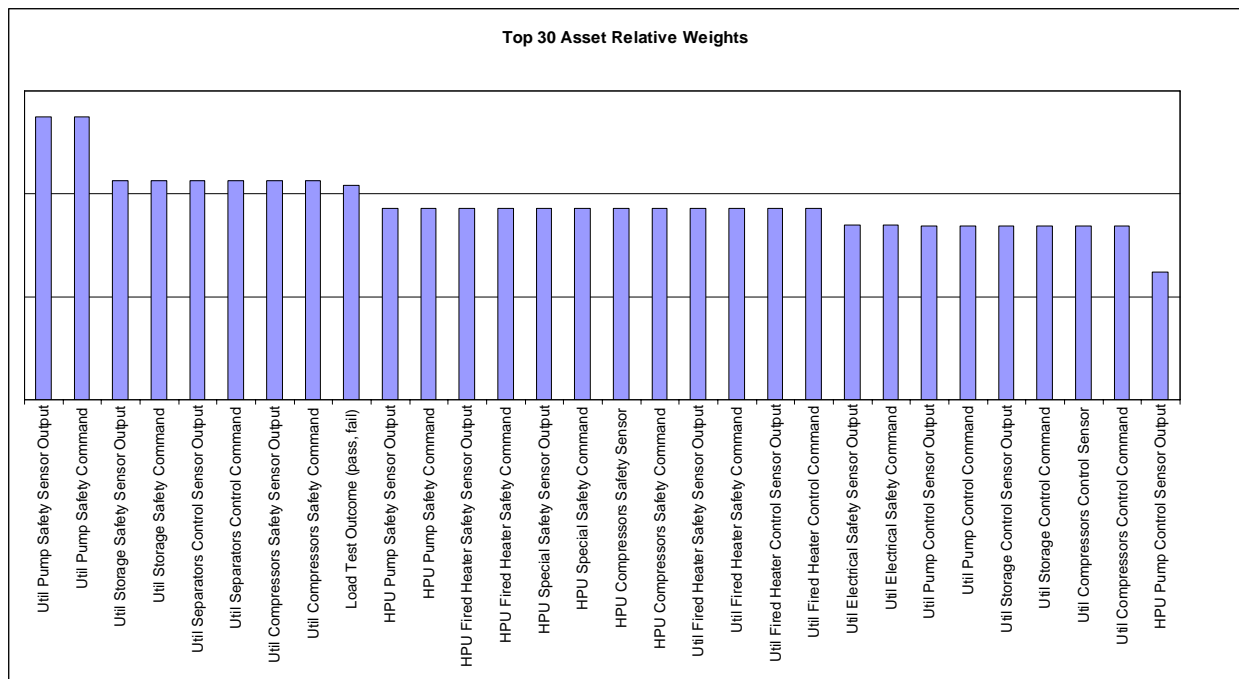


Figure 7. Information Assets Arranged by Relative Weight (Top 30)

The information assets on the left side of the chart are clearly the ones most vital to the operation of the refinery. But protecting those key information assets still depends on securing the network nodes that are involved in producing, manipulating, storing and transmitting those information assets. Identifying the key network nodes requires development of the network model and of the next matrix, Matrix 4.

The network model consists of a full inventory of network components (nodes), together with a representation of connectivity and functional dependencies. An accurate network diagram provides a basis for the network model. It is vital that all devices be identified, down to the individual PLC or I/O device. Individual sensors and actuators may be grouped in the same way as their signals, i.e.,

- *<system> <equipment>* Safety Sensor
- *<system> <equipment>* Safety Actuator
- *<system> <equipment>* Control Sensor
- *<system> <equipment>* Control Actuator
- *<system> <equipment>* History Sensor

All connectivity must be represented, including modems, network printers, and VPNs. Subnets and connections between PCS and corporate LANs must also be included. Existing fault tree analyses can provide useful information about connectivity and functional dependencies. Finally, the make, model, operating system and patch level of each device must be included. The latter information is needed to identify vulnerabilities known to exist in specific devices. Once the diagram is completely documented, it serves as a canvas on which to trace the path(s) traveled by each information asset. Tracing the path(s) aids in discovering all network nodes involved with an information asset, even if the involvement is only in transporting the asset from one point to another. Any network node involved with an asset brings with it the vulnerabilities, connectivity and dependencies that it may possess, including exposure to attack launched from other nodes.

Once all of the associations between nodes and assets have been identified, Matrix 4 is used to capture each node's criticality to each information asset. That is, a scale value is used to reflect the impact on each asset, should a network node not be available as it was intended.

Note that the gathering of this information about the device/component inventory and network connectivity is frequently useful and illuminating to refinery team members from the standpoint of network management. In an operational environment, network diagrams can quickly become outdated. Use of network scanning tools (a commonplace in IT network management as well as IT risk assessment) to gather and maintain such information requires caution in a PCS environment, to avoid degrading performance.

Figure 8 below is a partial representation of a completed Matrix 4. It shows the information assets from Matrix 3 on the left hand side and some of the identified network nodes arrayed across columns in a left to right descending order of criticality to asset. The weights are calculated as shown for Matrix 2. Figure 9 shows the Pareto view of the top 30 network nodes, as calculated in Matrix 4. The nodes appearing on the left are most critical to the organization. Any risks associated with them should be mitigated first.

3.2 Creating the Network Risk Model

The first step in creating a risk model of a PCS/SCADA network is to determine vulnerability ratings for its various processing components – not only those that provide the means for monitoring and controlling their connected PCS/SCADA devices, but also those performing other functions which are connected to a common network. As discussed in section 2.4, this step is facilitated by working from an accurate diagram of the network, so that each node listed in Matrix 4 can be fully evaluated.

Devices on the corporate portions of a refiner's network may be scanned for vulnerabilities using a number of available tools. However, because technical vulnerability scanning is not advised on operational PCS/SCADA networks, a non-intrusive approach is needed to develop the vulnerability information required by the method. One such approach is to list the devices used in the PCS/SCADA network and then to manually enter into the risk model any vulnerabilities known to exist in those devices. Knowledge of such vulnerabilities may come from several sources, any of which may be used as long as the organization considers them credible and the risk assessment team treats their results consistently.

- Sandia National Laboratories has assembled a list of vulnerabilities commonly found in critical infrastructure control systems. (Stamp 2005) These vulnerabilities organize into three distinct categories: those related to PCS administration, those related to PCS networks, and those related to PCS platforms.
- PlantData Technologies, Inc. has developed a list of the Top 10 Security Issues for PCS networks. (Pollet 2005) Because a security issue can acknowledge possible existence of a vulnerability, the ten security issues cited by PlantData should, in addition to the vulnerabilities recognized by Sandia, be included in vulnerability evaluations of a PCS networks.
- There are also a number of vulnerability discovery tools that could be used at different points in a PCS product's life cycle. (Byers 2006) Some are intended for use by the product vendor, and others by the asset owner.

The vulnerabilities discovered in the development of the network model provide the first input for developing the risk model.

The second step is to evaluate the threat. Some organizations use threat assessment methods developed by government and/or industry for describing specific to more general threat scenarios that can result in harm to their operation and/or business. An analysis of trends in terrorist threats to the oil and gas sector has been performed under the auspices of the I3P SCADA Security Project. (Simonoff 2005) However, in the absence of such specific measures, a general, uniform threat measure can be assumed for the environment and associated with all nodes.

However derived, the next step is to combine the vulnerability and threat values to arrive at node-by-node risk values. This is best done using scale values such as High/Medium/Low. The next section explains how these are mapped from Node to Business Objective.

If any safeguards exist in the network that have not already been accounted for, those are identified next, and then finally, the node risks are adjusted based on the effectiveness of the safeguards.

3.3 Mapping Risk from Network Nodes to Business Objectives

A low risk at the network node contributes only low risk to any business objective that relies upon it. However, a high node risk does not necessarily imply a high business risk. Criticality of node to asset, of asset to task, and of task to business objective must be considered; thus, the risks must be mapped one step at a time in order to avoid overlooking any of the relationships that the business model provides.

Figure 9 below illustrates the possible paths the mapping of a risk can take when progressing from node to asset, asset to task, and task to business objective. At each step, the word pictures given for impact come

from the matrices in the business model. For simplicity, the trivial paths for “no impact” are omitted since they would transmit no risk at all.

As can be seen in the illustration, Low risks at the node beget Low risks to the business objective. The situation is nearly the same for Medium or High risks, although for both of those the risk transmitted to the next step is lower when the impact is merely having to resort to a common work around with no degradation involved.

The terms Node Loss, Asset Loss, etc. are very curtly defined in Figure 11. Certainly there are cases where a node, asset, task or business objective can be partially compromised. Those cases are best reviewed in detail once attention is brought to them by means of the all-or-nothing definitions used to map the risks.

Another hurdle to mapping risk from node to business objective is the problem of showing the combined effect of multiple risk factors. There are a number of opinions and approaches to this problem. Rather than examine the merits of any one of them, the project team simply recommends mapping the maximum risk from each node. As mitigation measures are considered for reducing these risks, the next-greatest, remaining risks come into play. Mitigating these brings up the next, and so on until there are no unacceptable risks remaining.

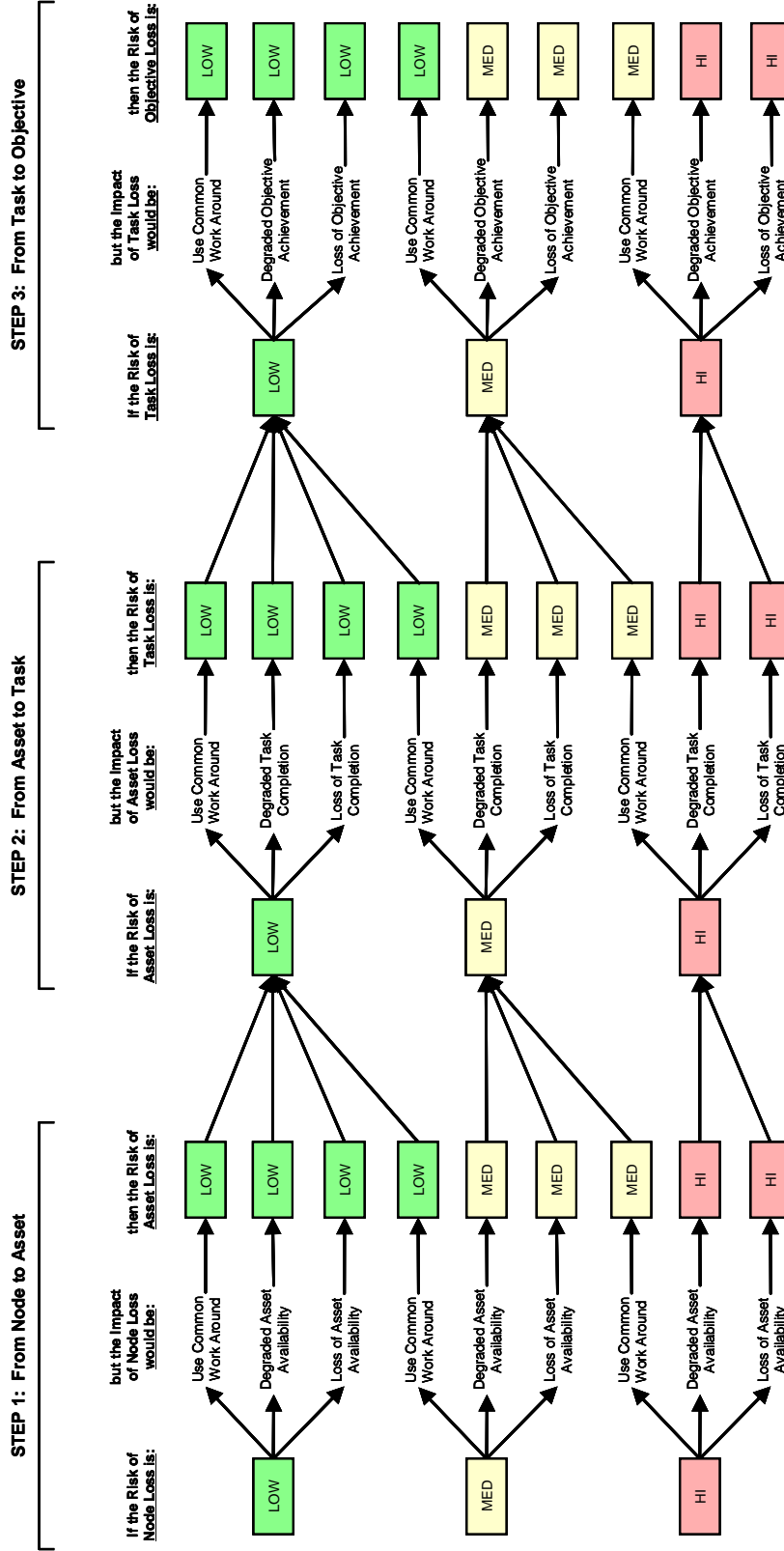
For the sake of illustration, hypothetical risk values will be assigned to several of the nodes identified in Matrix 4 and mapped to asset, task and business objective. Figure 10 below shows how Matrix 5 is used to assign risk values to hypothetical vulnerabilities and to associate them with network nodes.

Risk of Node Loss: 1 = Low 3 = Medium 5 = High		Vulnerabilities																									Max Node Risk	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25		
Network Nodes		Node Rel Wt	Vulnerability 5	Vulnerability 3	Vulnerability 13	Vulnerability 1	Vulnerability 2	Vulnerability 27	Vulnerability 22	Vulnerability 6	Vulnerability 10	Vulnerability 11	Vulnerability 14	Vulnerability 7	Vulnerability 15	Vulnerability 18	Vulnerability 12	Vulnerability 19	Vulnerability 20	Vulnerability 23	Vulnerability 24	Vulnerability 28	Vulnerability 4	Vulnerability 8	Vulnerability 16	Vulnerability 21	Vulnerability 29	
1	Network Interface	3,059	5	3		1																						5
2	PLC Config Server	2,541					1																					1
3	OPC Server	2,541						1																				1
4	< brand z > Server 2	1,791				3				3																		3
5	< brand x > Server	1,730			5		1						3	1									1					5
6	< brand x > Operator Station 1	1,730												1	1													1
7	< brand x > Operator Station 2	1,730									3	3			1	1							1					3
8	Work Station 2	1,529							1								3	1	3						1			3
9	Printer 2	1,529												1					1									1
10	DCS Switch 1	1,529													1		1							1	1			1
11	DCS Switch 2	1,529																1										1
12	DCS Comm Processor	1,529								3										1	3							3
13	Work Station 3	1,416																		1								1
14	Work Station 1	1,258						5													1							5
15	DCS Control Processor 9	1,155																				1						1
16	< brand x > PLC 4	956																									1	1

Figure 10. Matrix 5 – Assigning Node Risks Due to Vulnerabilities

Using the logic shown in Figure 11, the max values for node risk are mapped from node to asset, from asset to task, and from task to objective working backward through Matrices 4, 3, and 2 but replacing criticality and weight values with risk and max risk values. This is accomplished by filling the cells with logical expressions rather than with static values. Then, as node risks are mitigated, the corresponding changes are propagated to asset, task, and business objective risks. To distinguish these modified matrices in the risk model from the original matrices in the business model, we number them 4R, 3R and 2R. Figures 13, 15, and 17 below show Matrices 4R, 3R and 2R as they are used to map the max risk values from node to objective. Figures 12, 14, 16 and 18 show the Node, Asset, Task and Business Objective Risks overlaid on the Node, Asset, Task and Business Objective Pareto charts seen earlier in this section. These risk-augmented Pareto views provide the starting point for presenting a business case for mitigating specific technical risks. The matrices 2R, 3R and 4R provide the tools to instantly identify the root causes for any elevated level of risk at the task or business objective level. This will be explained in the paragraphs that follow Figure 18.

Logically Mapping Risk from Node to Objective



Node Loss = Not having the node functioning in the manner needed (in terms of timeliness or quality) to support asset availability.
 Asset Loss = Not having the asset available for use in the manner intended (in terms of timeliness or quality) to support task completion.
 Task Loss = Not having the task completed in the manner intended (in terms of timeliness or quality) to support objective achievement.
 Objective Loss = Not having the business objective achieved (in terms of timeliness or quality) to support corporate needs.

Figure 11. Mapping Risks from Node to Business Objective

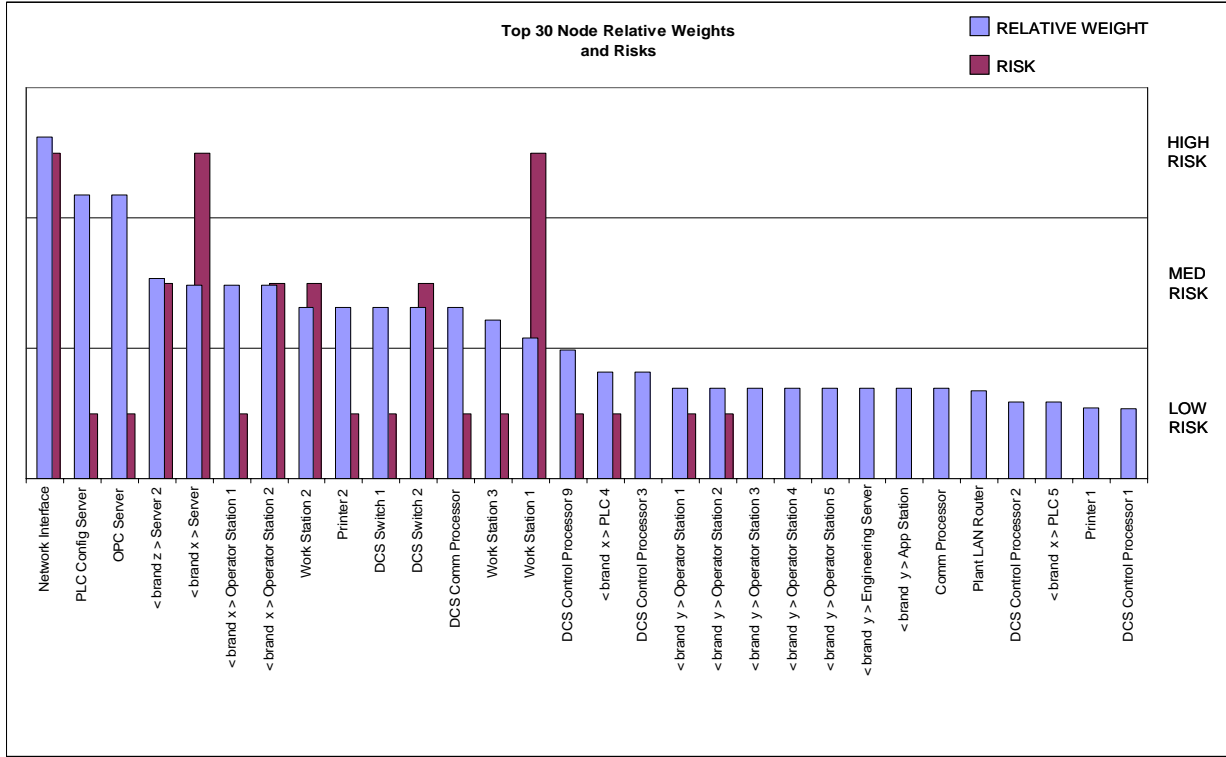


Figure 12. Node Risks Overlaid on Node Weights

Risk of Asset Loss:		Max Node Risk	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30		
Information Assets		Max Asset Risk	Network Nodes																															
1	Util Pump Safety Sensor Output	5	1	1	1	5	1	3																										
2	Util Pump Safety Command	5	1	1	1	5	1	3																										
3	Util Storage Safety Sensor Output	5	1	1	1	5	1	3																										
4	Util Storage Safety Command	5	1	1	1	5	1	3																										
5	Util Separators Control Sensor Output	5	5							1	1	1	1	1		5	1																	
6	Util Separators Control Command	5	5							1	1	1	1	1		5	1																	
7	Util Compressors Safety Sensor Output	1	1	1	1					1	1	1	1	1		5	1				1	1												
8	Util Compressors Safety Command	1	1	1	1					1	1	1	1	1		5	1				1	1												
9	Load Test Outcome (pass, fail)																																	
10	HPU Pump Safety Sensor Output	5	1	1	1	5	1	3																										
11	HPU Pump Safety Command	5	1	1	1	5	1	3																										
12	HPU Fired Heater Safety Sensor Output	5	1	1	1	5	1	3																										
13	HPU Fired Heater Safety Command	5	1	1	1	5	1	3																										
14	HPU Special Safety Sensor Output	5	1	1	1	5	1	3																										
15	HPU Special Safety Command	5	1	1	1	5	1	3																										
16	HPU Compressors Safety Sensor Output	1	1	1	1																1	1												
17	HPU Compressors Safety Command	1	1	1	1																1	1												
18	Util Fired Heater Safety Sensor Output	1	1	1	1																1	1												
19	Util Fired Heater Safety Command	1	1	1	1																1	1												
20	Util Fired Heater Control Sensor Output	5	5							1	1	1	1	1																				
21	Util Fired Heater Control Command	5	5							1	1	1	1	1																				
22	Util Electrical Safety Sensor Output	1	1	1	1																1	1												
23	Util Electrical Safety Command	1	1	1	1																1	1												
24	Util Pump Control Sensor Output	5	5	1	1	1				1	1	1	1	1		5	1																	
25	Util Pump Control Command	5	5	1	1	1				1	1	1	1	1		5	1																	
26	Util Storage Control Sensor Output	5	5							1	1	1	1	1																				
27	Util Storage Control Command	5	5							1	1	1	1	1																				
28	Util Compressors Control Sensor Output	5	5							1	1	1	1	1		5	1																	
29	Util Compressors Control Command	5	5							1	1	1	1	1		5	1																	
30	HPU Pump Control Sensor Output	5	5							1	1	1	1	1																				

Figure 13. Matrix 4R – Mapping Node Risk to Asset Risk



Figure 14. Asset Risks Overlaid on Asset Relative Weights

Risk of Task Loss: 1 = Low 3 = Medium 5 = High	Tasks	Max Task Risk	Information Assets																																	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30				
	1 Acquire Natural Gas																																			
	2 Acquire Water																																			
	3 Receive Caustic	1																																		
	4 Acquire Electrical Power	3																																		
	5 Quality Test During Loading																																			
	6 Impurity Removal	5	5	5	5	5	5	5	5	1	1																									
	7 Blend & Load Lube Oils																																			
	8 Perform Fractional Distillation	5	5	5	5	5	5	5	5	1	1																									
	9 Perform Hydrotreating	5	5	5	5	5	5	5	5	1	1																									
	10 Quality Test During Processing																																			
	11 Load Other Products	3																																		
	12 Unload & Store Crude	3																																		
	13 Bill for Product																																			
	14 Acceptance Test Crude																																			

Figure 15. Matrix 3R – Mapping Asset Risk to Task Risk

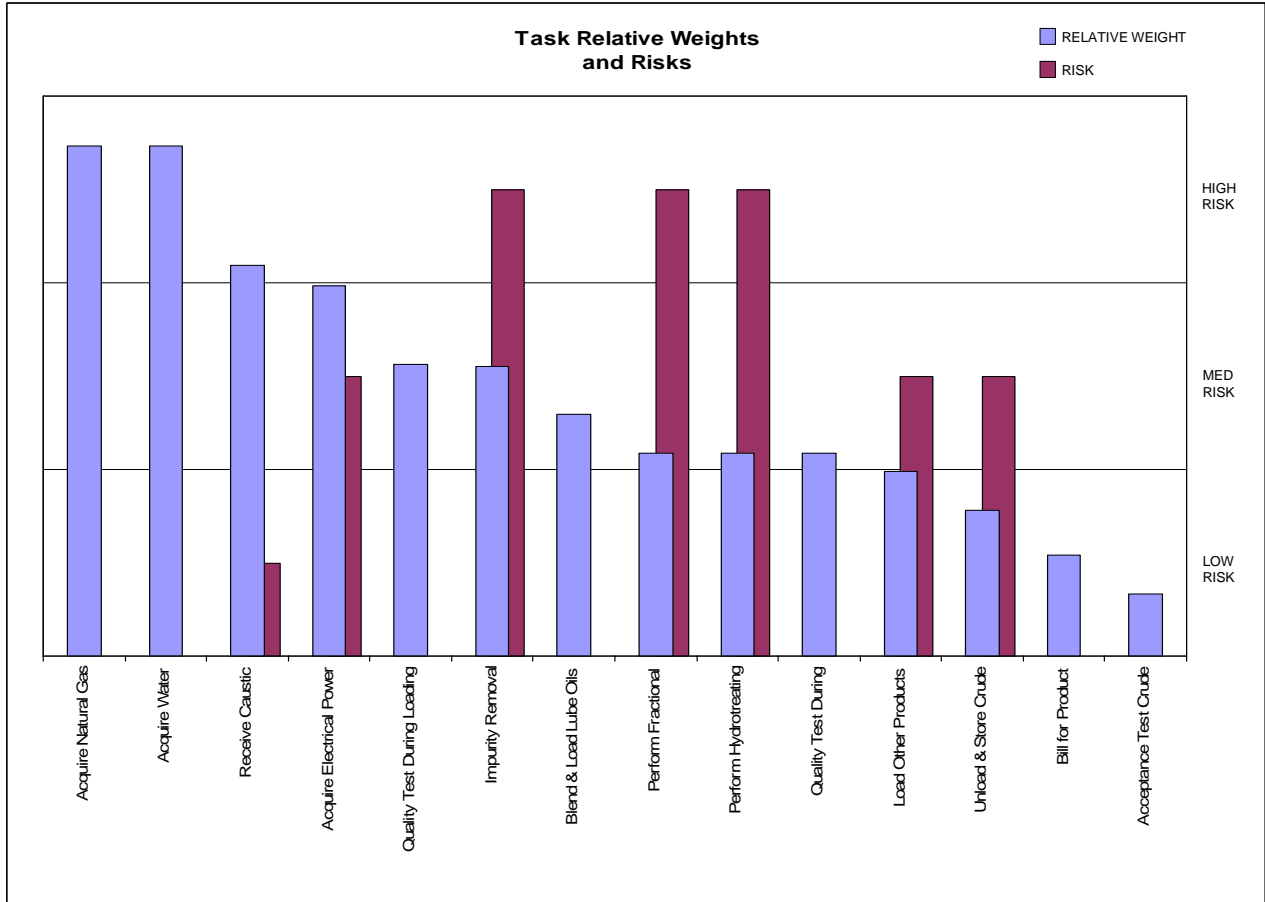


Figure 16. Task Risks Overlaid on Task Relative Weights

Risk of Business Objective Loss: 1 = Low 3 = Medium 5 = High		Max Task Risk	1	2	3	4	5	6	7	8	9	10	11	12	13	14
			Task	Acquire Natural Gas	Acquire Water	Receive Caustic	Acquire Electrical Power	Quality Test During Loading	Impurity Removal	Blend & Load Lube Oils	Perform Fractional Distillation	Perform Hydrotreating	Quality Test During Processing	Load Other Products	Unload & Store Crude	Bill for Product
Business Objective		Max Obj. Risk														
1	Stay safe	5			1	1		5								
2	Stay profitable	5			1	3				5	5		1	1		
3	Stay in compliance	5			1	3		5				1	1	1		
4	Supply customers well	5			1	3				5	5		3	1		
5																

Figure 17. Matrix 2R – Mapping Task Risk to Business Objective Risk

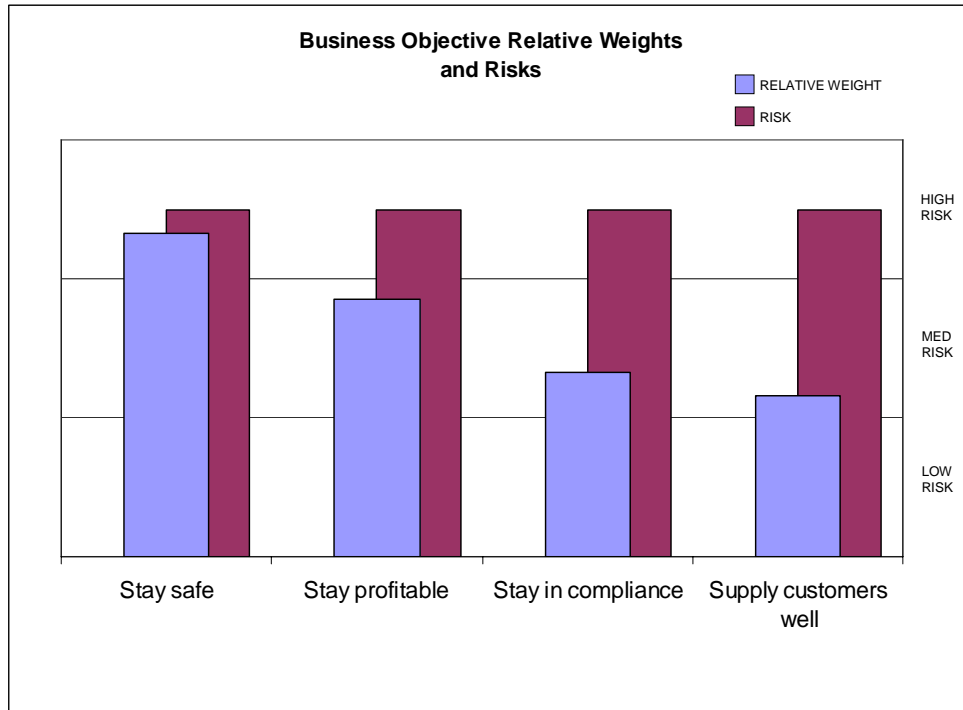


Figure 18. Business Risks Overlaid on Business Objective Weights

When viewing the risks facing the business objectives as seen above, a natural question for the viewer is: What is/are the root cause(s) of the elevated risks? The logical follow-on question is: What is the most cost-effective way to mitigate the elevated risks? RiskMAP provides the means for the assessment team to quickly trace risks to their root causes – specific vulnerabilities in the network nodes.

Since all four business objectives are, in this example, facing high risk, all four risks need to be traced to their sources. However, only the Stay Safe objective will be traced here for illustration. Starting with Matrix 2R (see Figure 17), note the Stay Safe objective has a maximum risk value of high, as indicated by the scale value of 5. Scanning across the row for each objective, it can be seen that for the Stay Safe objective, the only supporting task contributing high risk is task 6: Impurity Removal. Moving to Matrix 3R (see Figure 15) it can be seen that the Impurity Removal task's high risk is contributed by six supporting assets, all associated with the Utilities system. In Matrix 4R (see Figure 13), a single network node, the < brand x > Server, contributes the high risk to four of the assets. Two other nodes, the Network Interface and Work Station 1, each contribute high risk to the other two assets. Matrix 5 (Figure 10) shows that the Network Interface's high risk stems entirely from the hypothetical "Vulnerability 5." The < brand x > Server's high risk comes from "Vulnerability 13," and Work Station 1's high risk comes from "Vulnerability 27." Mitigating those three vulnerabilities to medium risk or below will lower the business risk from high to medium. This can be demonstrated by lowering the risk values for those vulnerabilities in Matrix 5 and observing the corresponding drop in each of the high risk bars to medium at all levels, thanks to the relationships captured in the models.

Additional risk mitigation actions can be considered and the benefits demonstrated, but the costs of each action must also be considered and presented in order to enable a fully-informed decision. But the set of matrices in RiskMAP can be used to clearly show the minimum set of mitigating actions. Once the results are presented to corporate decision makers in terms of risk to business objectives, with immediately-available supporting detail and the means to support what-if excursions, the risk assessment team will have made a compelling case to support their risk mitigation strategy.

SECTION 4: CONCLUSIONS

RiskMAP enables an organization to capture and relate business processes and components in a way that, when combined with component technical vulnerability and cyber threat data, reveals the greatest cyber security risks to organizational objectives. RiskMAP meets the objectives for a technical cyber security risk assessment methodology stated in the earlier report (Kertzner 2006). RiskMAP draws upon and is consistent with the IT risk assessment methodologies used in government, academia, and industry. These techniques are by design oriented toward strengthening systems to resist attacks on information and IT infrastructures. The RiskMAP methodology considers attacks on information and on the PCS (and, as applicable, IT) components that handle process control information, and the possible business impacts that may ensue. RiskMAP is consistent with other differently-scoped models being developed under the auspices of or in conjunction with the I3P SCADA Security project. (Crowther 2005) However, its ability to account for technical vulnerabilities – in PCS architectures, technologies, components, and configurations – as sources of business as well as security risk makes RiskMAP unique in that it can provide business focused rationale for investing in SCADA security.

Oil and gas industry organizations have developed security assessment methodologies that use traditional risk modeling constructs of threats, vulnerabilities, and assets to derive measures of risk to systems. The RiskMAP methodology uses these same constructs, but to derive measures of risk to business operations and objectives. To this end, the RiskMAP methodology can utilize data previously gathered for past or current assessments to build its own business focused models of risk. The consistency of RiskMAP with existing oil & gas industry methodologies makes it a useful tool to those organizations that in particular employ the SVA or ISA methodology. The self-documenting approach of RiskMAP, where analysis elements are linked—from the abstract business objectives to the concrete network platforms, provides a way to drill-down in a completed model for the analysis and assessment of technical vulnerabilities and risks.

In summary, the RiskMAP methodology can be applied directly to technical cyber security risk assessment for process control systems, and specifically to systems in the oil and gas sector. The I3P SCADA security effort is developing risk analysis template matrices specific to the Oil and Gas sector. These matrices will focus the assessment process 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. Application of the RiskMAP method to the process control network/systems problem space will facilitate the evolution of process control systems toward more inherently secure systems. The I3P SCADA Security Project is currently working with an industry representative to refine and apply this methodology to an operational environment in the Oil and Gas sector. Additional industry partners are invited to participate in the refinement and tailoring of the methodology. Those interested in getting involved are encouraged to contact the research team by email at I3P-scadasecurity-metrics@thei3p.org or by contacting the authors.

Peter Kertzner kertzner@mitre.org

Jim Watters jwatters@mitre.org

Deborah Bodeau dbodeau@mitre.org

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.
- Byres, Eric and Matthew Franz. January 2006. “Uncovering Cyber Flaws.” *InTech*, pages 20-25. Available at http://www.isa.org/Content/ContentGroups/InTech2/Features/20061/January27/Uncovering_Cyber_Flaws.htm
- Crowther Kenneth and Yacov Haimes. 2005. “Application of the inoperability input - output model (IIM) for systemic risk assessment and management of interdependent infrastructures.” *Systems Engineering*, Volume 8, Issue 4, pages 323-341.
- Department of Justice (DOJ’s National Institute of Justice), Environmental Protection Agency (EPA’s Chemical Emergency Preparedness and Prevention Office), and Sandia National Laboratories. 2003. (VAM-CF) Vulnerability Assessment Methodology - Chemical Facilities. Developed in cooperation with the chemical industry and government agencies.
- Duggan David. March 2005. Penetration Testing of Industrial Control Systems. Sandia Report SAND2005-2846P. Available at http://www.sandia.gov/scada/documents/sand_2005_2846p.pdf
- I3P (Institute for Information Infrastructure Protection). 2003. Cyber Security Research and Development Agenda. Available at http://www.thei3p.org/about/2003_Cyber_Security_RD_Agenda.pdf
- 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.

Kertzner Peter, Deborah Bodeau, Robert Nitschke, Jim Watters, Mary Louise Young, and Martin Stoddard. January 2006. Process Control System Security Technical Risk Assessment: Analysis of Problem Domain. I3P Research Report No. 3. Available at <https://www.thei3p.org/about/researchreport3r1.pdf>

Lindqvist, Ulf, 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>

Nitschke Robert. 2005. “Appendix C, Risk Reduction Analysis Tool for Control Systems.” Idaho National Laboratories.

Pollet Jonathan. March 14, 2005. Risk Mitigation – Top Ten Security Issues with Securing Real-Time Control and SCADA Systems that Support Critical Infrastructure. Available from <http://www.plantdata.com>

Simonoff Jeffrey, Carlos Restrepo, and Rae Zimmerman. November 30, 2005. Trends for Oil and Gas Terrorist Attacks (DRAFT). I3P Research Report No. 2. Available at <http://www.thei3p.org/research/scada/i3presrep2.pdf>

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

Stamp Jason, John Dillinger, William Young, and Jennifer DePoy. November 11, 2003. “Common Vulnerabilities in Critical Infrastructure Control Systems”, Sandia National Laboratories, 2nd edition. Available at <http://www.oe.netl.doe.gov/docs/prepare/vulnerabilities.pdf>

Stoddard Martin, Deborah Bodeau, Rolf Carlson, Cliff Glantz, Yacov Haimes, Chenyang Lian, Joost Santos, James Shaw. August 2005. Process Control System Security Metrics – State of Practice, I3P Research Report No. 1. 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>

Watters C. J. 1997. Chapter 12 – Case Studies, in Kiemele M., S. Schmidt, R. Berdine, Basic Statistics – Tools for Continuous Improvement (Fourth Edition), Air Academy Press, ISBN 1-880156-06-7.