

# **Process Security Management: Protecting Plants Against Threats of Terrorism and Criminal Acts**



**For additional copies of this booklet, please contact:**

Primatech Inc.  
50 Northwoods Blvd.  
Columbus, OH 43235  
Phone: 614-841-9800  
Fax: 614-841-9805  
Email: [papers@primatech.com](mailto:papers@primatech.com)  
[www.primatech.com](http://www.primatech.com)

*"I am not fond of expecting catastrophes, but  
there are cracks in the universe."*  
Sydney Smith

**Copyright © 2002, Primatech, Inc. All rights reserved.**

**Process Security Management:  
Protecting Plants Against Threats of Terrorism and Criminal Acts  
September, 2002, Version 1.00**

## Table of Contents

Terms and Acronyms .....	4
Preface .....	5
Introduction .....	6
Process Security Management Program - The Elements .....	7
Management System .....	7
Coordination with Other Organizations .....	7
Employee Involvement and Security Awareness .....	8
Process Security Information .....	8
Risk Assessment .....	8
Security Procedures .....	10
Training .....	10
Contractors .....	10
Security Systems Integrity .....	10
Management of Change .....	11
Incident Reporting and Investigation .....	11
Emergency Response and Crisis Management .....	12
Reviews, Audits and Inspections .....	12
Key Differences Between Managing Process Safety and Process Security .....	13
Model Programs .....	14
Level 1 .....	14
Level 2 .....	14
Level 3 .....	14
Level 4 .....	14
Program Security Measures .....	15
Summary .....	16
Further Information .....	17
About Primatech .....	18

## Terms and Acronyms

---

<b>ERP</b>	Emergency Response Plan
<b>Hazard</b>	A situation or intrinsic property with the potential to create harm. The potential for accidents with undesirable consequences.
<b>LOPA</b>	Layers of Protection Analysis
<b>MI</b>	Mechanical Integrity
<b>MOC</b>	Management of Change
<b>OSHA</b>	Occupational Safety & Health Administration
<b>PHA</b>	Process Hazard Analysis
<b>PSI</b>	Process Safety Information
<b>PSM</b>	Process Safety Management
<b>PSSM</b>	Process Safety and Security Management
<b>PVA</b>	Process Vulnerability Analysis
<b>ROPA</b>	Rings of Protection Analysis
<b>Sabotage</b>	Deliberate destruction or obstruction for political or other advantage.
<b>Safety</b>	Freedom from injury or damage. Protection from accidents.
<b>Safeguard</b>	A measure taken to prevent or protect something. Measures to protect against accidents.
<b>Secureguards</b>	Measures to protect against threats.
<b>Security</b>	Protection against threats.
<b>SI</b>	Systems Integrity
<b>Target</b>	A person, object, facility, or place selected as the aim of an attack.
<b>Terrorism</b>	Threats or actions by individuals or a group against a country, its institutions or people to influence or intimidate for political, religious or ideological reasons.
<b>Threat</b>	The possibility of injury, damage or other hostile action.
<b>Vandalism</b>	The deliberate destruction or damage to property out of malice or ignorance.
<b>Vulnerability</b>	Exposure to injury, damage or other hostile action.

---

## Preface

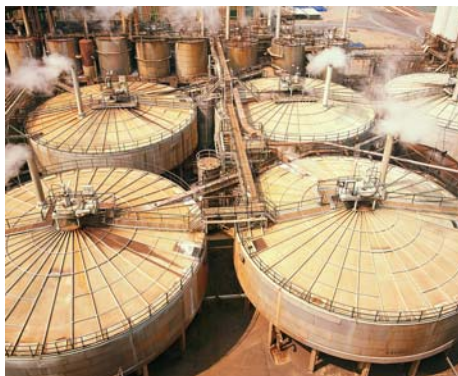
Process security management addresses threats from terrorist and criminal acts against plants that may result in the release of hazardous materials. Its purpose is to manage the risk of such deliberate releases. Recent events have emphasized the need for such programs. Both government and industry are acting to remedy current shortfalls in process security.

This booklet describes a comprehensive program for process security management that parallels process safety management (PSM) programs which address accidental releases of hazardous materials. Such process security management programs can reduce both the likelihood and severity of terrorist and criminal acts.

Modeling process security management on process safety management offers numerous benefits:

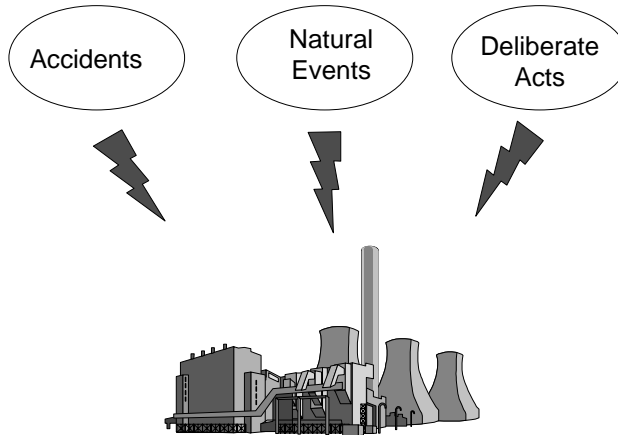
- ◇ Much development work has been performed and experience accumulated on PSM programs since OSHA's PSM standard was enacted in 1992.
- ◇ Most process companies invest significant resources in their PSM programs and value them highly.
- ◇ Modification of an existing program to address process security is easier and more efficient than developing a completely new program.

Furthermore, many companies already have in place elements of process security that can be integrated readily into an overall program. Given the success and acceptance of process safety programs it is logical that an extension of that approach be used for process security.



## Introduction

Many process plants contain hazardous materials that, if released, can adversely impact the health and safety of workers and the public, and damage the environment. Such releases can result from extraordinary events such as *accidents*, *natural events*, or *deliberate acts*. Accidental and natural events are addressed by OSHA's Process Safety Management and EPA's Risk Management Program regulations.



Over the past few years, concern has developed about the risk from deliberate acts performed with the intention of causing harm. They include terrorism, sabotage, vandalism and theft. These acts may arise from individuals or groups inside or outside a facility. While PSM programs provide the framework for a comprehensive process security management program, there are significant differences that require modifications and additions to the PSM framework to accommodate process security.

This booklet outlines a process security management program, describes differences from process safety and provides several model programs.

***“All companies, big and small, should have some measure of site security in place. This is especially true for facilities that handle extremely hazardous substances.”***

**USEPA**

## Process Security Management Program - The Elements

Each element of a process security management program is described below.

### **Management System**

The importance of process safety management systems is well established. A process security management system can parallel and borrow from process safety management. Indeed, both can be integrated in a Process Safety and Security Management (PSSM) program.

Policies, procedures, instructions and documentation must be developed to manage the implementation of process security within an organization. For example, policies are needed for pre-employment screening and access control, and procedures are needed for reporting and responding to threats and incidents.

### **Coordination with Other Organizations**

Process security management requires the involvement of outside organizations. Companies must coordinate activities and communicate proactively with local, state, and federal law enforcement; public safety agencies; government; the community; trade and industry associations; and other companies to share information on:

- ◇ looming threats
- ◇ dangerous trends
- ◇ security breaches
- ◇ and incidents



***“Most security gaps were the result of complacency and lack of awareness of the threat.”***

**ATSDR**

## ***Employee Involvement and Security Awareness***

As with process safety, employees and contractors have a vital role to play in process security. Employee awareness improves process security. Employee involvement improves the design and implementation of the process security management program.

Employees must be alerted to the possibility of attacks and how they could occur so they can assist in their prevention. Employees may also have good ideas on how to address process security issues. Involvement in the process security program can help resolve employee objections to increased security by providing a better understanding of why security measures are being taken.

***“No involvement, no commitment”***

## ***Process Security Information***

Information is needed to support the other elements of a process security program in a similar way to how process safety information (PSI) does so for PSM. Much of the PSI is also needed for process security but, in addition, information is needed on process security equipment and technology. This includes, for example, specifications for acceptable security devices such as closed-circuit television cameras to operate in electrically classified areas.

## ***Risk Assessment***

The risk of deliberate releases of hazardous materials must be evaluated. Risk assessment involves performing a *threat analysis* to identify what could happen, conducting a *vulnerability analysis* to determine how it might happen and its likelihood, and considering what can be done to lower the risk in the form of *security measures* and *safeguards*. Risk assessment is the heart of a process security program.

***Threat analysis*** involves the identification of the source of threats, the study of potential actions of adversaries, and the assessment of the likelihood of the threats by considering the motivations and capabilities of adversaries.

There are various types of threats. They include:

- ◇ Release of hazardous materials on-site
- ◇ Theft of hazardous materials for use/release off-site
- ◇ Interference with production
- ◇ Shutting down the plant

The combination of threat source and type defines specific threats that can be analyzed using vulnerability analysis. Threat likelihoods are assessed and combined with severity to assign threat levels which can be used to decide on the extent of vulnerability analysis that should be performed as well as the levels of safeguards and security measures that should be implemented.

**Vulnerability analysis** is the assessment of the degree to which a facility is exposed to injury, damage or other hostile action. It includes identifying ways in which attacks could happen. Process vulnerability analysis (PVA) focuses on an individual process and identifies ways specific threats identified in the threat analysis can be realized. PVA identifies *threat scenarios* in a similar way to identifying hazard scenarios in a PHA. Process design and layout, security, safeguards, and information, computer and other support systems are considered. Recommendations for improvements are made based on the nature of the threat, process vulnerabilities, possible consequences, and existing security measures and safeguards.

### PVA WORKSHEET

PVAWorks - [PVA EXAMPLE: System 1]					
SECTOR: (1) TANK FARM					
THREATS	VULNERABILITIES	CONSEQUENCES	SAFEGUARDS	S L R	RECOMMENDATIONS
Hazardous material release by terrorists	Tank farm is close to fence line, tanks are labeled and visible from the road, only single fence, explosive charge could be placed	Mass fatalities within the plant and the community	Roving guards	4 2 D	Consider installing double fence with barbed-wire top guard  Consider installing CCTV monitoring
	Projectile could be fired	Mass fatalities within the plant and the community	None	4 2 D	Discuss scenario with local law enforcement

## ***Security Procedures***

Procedures embody the most appropriate way of performing a task. They remove the need for improvisation that can lead to problems. They provide guidance for task performance to those who need it and ensure that tasks are always performed the same way by different people. When coupled with policies and documentation requirements, they help ensure that tasks are not only performed but also carried out correctly. Written procedures should be developed for various security activities, including materials tracking and accounting, personnel screening, access control, information protection, document control, computer access, etc.

## ***Training***

All affected employees should be trained in security-related matters, as appropriate. Failure to train personnel in addressing terrorism and criminal acts increases the vulnerability of facilities. Employees may need training in various areas, including security awareness, security procedures, emergency shutdown and response, etc.

## ***Contractors***

Contractors often perform maintenance and other work at process plants. The PSM standard contains a Contractors element that addresses their impact on process safety. Similarly, a process security management program must address the possible impact of contractors on security. However, it is not unusual for aspects of site security to be provided by contractors, e.g. the guard force, so this element may include the additional aspect of the involvement of the security contractor in the process security program.

## ***Security Systems Integrity***

Security systems will work correctly only if they are properly designed, fabricated, installed, operated, maintained, inspected and tested. This requires a *systems integrity* (SI) or *quality assurance and maintenance program* to ensure the continued integrity of security systems. Such a program is the security equivalent of a PSM mechanical integrity (MI) program.

A security integrity program includes requirements for written specifications for security-critical materials, equipment and systems; procedures to ensure they function as intended; employee training; maintenance; inspection and testing; periodic tests to challenge the security program; and quality assurance.

### ***Management of Change***

Conditions at many plants change constantly. Employees come and go, processes change, and threats wax and wane. Even apparently simple and straightforward changes can lead to increased risk if the process security program is not modified to accommodate the change.

Certain types of changes should trigger a review of the process security management program in a similar way that PSM uses a Management of Change (MOC) program to address changes that affect a covered process. Indeed, the framework and procedures established for MOC in PSM can be adapted for process security, although it is important that additional types of change be addressed, including changes in security devices, equipment or systems; computer and information systems; security procedures; threat level; etc.

### ***Incident Reporting and Investigation***

Incidents include suspicious events, breaches of the process security program and actual attacks. Suspicious events and breaches of the process security program may be precursors to an attack and must be reported so they may be investigated and any applicable corrective actions taken. Actual attacks may be forestalled by proper incident reporting and investigations.



Incidents must be investigated to understand their causes so that actions can be taken to eliminate their recurrence. This contributes to the continual improvement of the process security program.

## ***Emergency Response and Crisis Management***

Plans must be made to respond to attacks. They will overlap with the accident emergency response plan (ERP). However, the plan must address some special issues for threat scenarios, including coordination with law enforcement and Federal agencies, the need for law enforcement personnel to operate in contaminated or hazardous environments, possible attacks on responders prior to or during the event, preservation of evidence, etc. Specialized training for response teams may include recognizing explosive and anti-personnel devices and understanding triggering mechanisms.

Companies may have an existing crisis management plan to deal with accidental releases. Such plans address communicating information to the public, the government, news media and any other affected parties on health risks, casualties, impacts on traffic, etc. The plan should be revised to include threat scenarios. If a plan does not exist, one should be created.

## ***Reviews, Audits and Inspections***

Various types of reviews, audits and inspections are needed as part of a process security program. They provide a control function. A baseline review can be conducted at any time existing programs and practices need to be compared to best practices or new practices. Periodic reviews are used, often annually, to assess compliance with established requirements. They provide assurance that reasonable measures have been taken and they are functioning.

Audits are used to examine the design and implementation of the process security program to confirm compliance with requirements and current practices. Usually, they are performed every few years.

Plant conditions change constantly. Many changes will trigger an MOC review and modifications to the process security program. However, even such mundane changes as growth of vegetation and trees around a facility's exterior may affect process security, since it provides cover for intruders. Such subtle changes should be monitored by regular checks of the facility and inspections of security devices such as fences, barriers, locks and alarms.

## Key Differences Between Managing Process Safety and Process Security

Most of the elements described above are present in a PSM program. However, their application to process security requires some modifications and additional considerations:

- ◇ Threats wax and wane. Therefore, process security programs should be capable of accommodating varying threat levels.
- ◇ Process security management requires the involvement of law enforcement.
- ◇ A threat analysis is required to identify the sources, types and likelihoods of threats. The closest parallel in process safety is deciding what hazards should be considered in a process hazards analysis (PHA) study.
- ◇ Risk analysis for accidents involves evaluating hazard scenarios that originate with equipment or human failures, or external events or a combination thereof. Risk analysis for terrorism and criminal acts involves evaluating threat scenarios that originate with deliberate acts.
- ◇ Credible threat scenarios must be identified. It is not sufficient to rely on a PHA. PHA scenarios may overlap with threat scenarios but they are not the same.
- ◇ Safeguards against accident or hazard scenarios may not be sufficient against threat scenarios.
- ◇ Process information and computer systems must be protected from misuse.
- ◇ The existing emergency response program will likely need revisions to handle threat scenarios.

***“Decisions about improving site security should be made after evaluating how vulnerable your site is to threats.”***

**USEPA**

## Model Programs

Most companies do not need to be convinced that security improvements are needed. They want to know what specific measures they should take and what other companies are doing. To that end, four programs are described below providing increasing levels of protection.

### **Level 1**

Provides a combination of security measures and safeguards that should be considered by all facilities handling hazardous materials. Most plants should implement these measures or their equivalent. Typically, justification should be provided to exclude any of them from a basic security program.

### **Level 2**

Can be used to protect facilities containing more hazardous materials or larger quantities, or for which the threat level is higher, or when a company wants to take a more conservative risk management approach.

### **Level 3**

Provides measures for increased security that may be appropriate when large populations are at risk, for example, close to major metropolitan areas.

### **Level 4**

Offers all reasonable available measures short of creating an armed encampment.

No one program will be right for every facility since each facility is unique and these programs do not necessarily provide all the measures that may be needed by a facility. However, they do provide reference points for facilities that wish to improve their current process security programs.

***40 million people live near chemical facilities  
in the US***

<b>Program Levels</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>
<b>Security Measures</b>				
Coordination and secure communications with law enforcement	✓	✓	✓	✓
Screening of employees and contractors	✓	✓	✓	✓
Security awareness program	✓	✓	✓	✓
Document control for sensitive information	✓	✓	✓	✓
Restrictions on in-plant signage	✓	✓	✓	✓
Perimeter fence with top guard	✓	✓	✓	✓
Gates with locks, key and lock management program, and guards	✓	✓	✓	✓
Secure points of intrusion	✓	✓	✓	✓
Personnel identification on entry, ID badges and visitor escorts	✓	✓	✓	✓
Visual inspection of bags/parcels	✓	✓	✓	✓
Appropriate employee/contractor termination procedures	✓	✓	✓	✓
Cyber security	✓	✓	✓	✓
Inventory control	✓	✓	✓	✓
Monitoring process parameters	✓	✓	✓	✓
Good housekeeping practices	✓	✓	✓	✓
Release detection and containment	✓	✓	✓	✓
Vapor cloud suppression	✓	✓	✓	✓
Emergency procedures for shutdown, response and evacuation	✓	✓	✓	✓
Retractable vehicle booms at gates		✓	✓	✓
Restrict facility access to employees and contractors		✓	✓	✓
Guard patrols		✓	✓	✓
Random checks of incoming and outgoing vehicles		✓	✓	✓
Enhanced area lighting		✓	✓	✓
Stricter restrictions on vehicle access		✓	✓	✓
Locking manual valves		✓	✓	✓
Vehicle blocking system at entries			✓	✓
Double perimeter fence with tanglefoot			✓	✓
Checks of all incoming and outgoing vehicles			✓	✓
Surveillance system			✓	✓
Perimeter intrusion detection and alarms			✓	✓
Use of smart keys			✓	✓
Guards stationed at interior locations			✓	✓
Access control to sensitive areas and panic alarms			✓	✓
Communications security			✓	✓
Cyber intrusion detection			✓	✓
Additional excess flow, check valves and automatic shutoff valves			✓	✓
Secondary containment for releases			✓	✓
Vehicle barriers around the site perimeter				✓
Secondary fences around hazardous materials and other sensitive areas				✓
Armed guards and guard dogs				✓
X-ray screening of bags/parcels/packages				✓
Radio voice encryption				✓
Counter-surveillance to detect information gathering				✓
Hardening of control rooms, utilities and other critical support systems				✓
Backup computer and critical support systems				✓
Vehicle barriers for sensitive and hazardous materials areas				✓
Projectile shields				✓
Interior area intrusion detection and alarms				✓
Stockpiles of chemical antidotes				✓

## Summary

---

Process security management is as important as process safety management. It deserves the same attention.

PSM programs are well established at many facilities and their framework can be used to implement a process security management program effectively and efficiently. Such a program provides comprehensive management of threats from terrorist and criminal acts and can be implemented quickly using existing programs.

Swift action is vital. No time should be lost in protecting plants against these threats.



## Further Information

---

Technical details on Process Security Management are available in several papers available from Primatech:

- **“Process Security Management Systems: Protecting Plants Against Threats”** Provides guidelines for implementing a Process Security Management Program.
- **“Assessing Risks from Threats to Process Plants: Threat and Vulnerability Analysis”** Describes the steps involved in assessing the risks from deliberate acts and provides an example of threat and vulnerability analysis.
- **“Process Plant Security Programs For Managing Risks From Deliberate Releases and Diversions of Hazardous Materials”** Provides examples of security programs that can be implemented to manage various risk levels. Also, describes a classification scheme for security measures and safeguards to protect against deliberate acts.
- **“Inherent Security: Protecting Process Plants Against Threats”** Proposes that the first line of defense against threats should be the application of *inherent security* principles in a manner analogous to the application of *inherent safety* principles to prevent accidents in plants. Provides examples of such principles. Additional security measures and safeguards needed to protect against deliberate releases are also discussed.
- **“Rings of Protection Analysis (ROPA): Determining Needed Safeguards and Secureguards to Protect Against Terrorism and Criminal Acts”** Describes and provides an example of the application of ROPA in an analogous way to Layers of Protection Analysis (LOPA) for process safety.

These papers may be obtained by contacting Primatech at 614-841-9800 or via email: [papers@primatech.com](mailto:papers@primatech.com)

## About Primattech

---

Primattech specializes in Process Safety, Security and Risk Management. We offer consulting, training and software to assist our clients in identifying and reducing the risks posed by toxic, flammable, and explosive materials.

Companies in a variety of industries choose Primattech to help them manage the risks posed by such hazardous materials. We help companies reduce the likelihood and consequences of releases, which helps protect employees and the public and prevent damage to equipment and the environment. Reducing these risks also improves productivity and quality. We help companies comply with OSHA's Process Safety Management (PSM) standard, EPA's Risk Management Program (RMP) regulation, and industry guidelines.

Our capabilities include:

- Process Hazard Analysis (PHA)
- Compliance Audits and Program Assessments
- PSM Program Development and Implementation
- RMP Program Development and Implementation
- Release and Spill Assessment
- Process Security Management
- Threat and Vulnerability Analysis for Deliberate Acts Including Terrorism
- S84 - Safety Instrumented Systems
- Layers of Protection Analysis (LOPA)
- Operating and Maintenance Procedures Development
- Mechanical Integrity Program Development and Implementation Guidance
- Human Factors and Human Error Analysis
- Facility Siting Analysis
- Dispersion and Consequence Modeling
- Probability Modeling
- Quantitative Risk Assessment
- Emergency Response Program Development and Implementation Guidance
- Expert Witness Testimony and Litigation Support

Primattech's clients are often Fortune 500 companies but also include medium and smaller sized companies. We specialize in serving the process industries, and have served hundreds of industrial facilities throughout the world.

Our services and products enable our clients to achieve their risk, safety and security objectives faster and easier. Primattech is an independent company with no vested interests and is seen, therefore, to deliver work recognized as objective and unbiased.

**50 Northwoods Boulevard**  
**Columbus, OH 43235 USA**  
**Telephone: 614-841-9800**  
**Fax: 614-841-9805**  
[www.primattech.com](http://www.primattech.com)