The Vulnerability Assessment of Process Plant in Malaysia

by

Mohd Hafez Bin Mamujalean

Dissertation submitted in partial fulfillment of
the requirements for the
Bachelor of Engineering (Hons)
(Chemical Engineering)

JAN 2009

Universiti Teknologi PETRONAS
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan

CERTIFICATION OF APPROVAL

The Vulnerability Assessment of Process Plant in Malaysia

by

Mohd Hafez Bin Mamujalean

Dissertation submitted in partial fulfillment of
the requirements for the
Bachelor of Engineering (Hons)
(Chemical Engineering)

Approved by,

....
(Assoc.Prof Dr Azmi Bin Mohd Shariff)

UNIVERSITI TEKNOLOGI PETRONAS
TRONOH
PERAK DARUL RIDZUAN

JAN 2009

CERTIFICATION OF ORIGINALITY

This it to certify that I am responsible for the work submitted in the project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons

....

MOHD HAFEZ BIN MAMUJALEAN

ABSTRACT

This report presents a research of a prototype methodology to assess the security of chemical facilities within the Malaysia. The Vulnerability Assessment (VA) do identifies and assesses potential security threats, risks, and vulnerabilities and guides the chemical facility industry in making security improvements. The National Institute of Justice developed the Vulnerability Assessment Methodology (VAM) in collaboration with the Department of Energy's Sandia National Laboratories. Sandia National Laboratories employees are recognized experts in security and counterterrorism and have extensive experience in the protection of nuclear weapons and radiological materials for the process plant. The objectives of the project are to study the vulnerability assessment framework and do the implementation by doing a case study in PETRONAS operation unit. In this project, the Vulnerability Assessment Methodology (VAM) by Sandia National Laboratories is used as guidance to implement vulnerability assessment in PETRONAS plant process. The challenge in this project is do the case study in one of the OPU in which involved collecting the plant data process.

ACKNOWLEDGEMENT

First and foremost I would like to praise to Allah the Almighty which have help and guided us in doing the Final Year Project until it reach to this stage. I would like to thank to various people who helped us a lot in the project

My utmost gratitude goes to my honourable UTP supervisor, Associate Professor Dr. Azmi Bin Mohd Shariff who always found some time in a very busy schedule to guide us, monitoring our progress and answer most of my questions regarding the project. All the experience that I have gained in order to complete the project really teach me to be matured, not just on a thinking skills but also on dealing with working stresses.

My deepest thanks to the Executive Engineer of Vinyl Chloride Malaysia Sdn Bhd (VCMSB), Esa bin Diman, who guide and provide meaningful information in the project. Thank you to Dr. Mohanad M.A.A El-Harbawi for giving a good advice and conduct me in the process of finishing the project.

Last but not least, I would like to thank to my beloved friends and lecturers who support and help me all the time. Thank you

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

1.0 BACKGROUND OF STUDY

Vulnerability assessment (VA) is a mandatory requirement by many countries especially in United States, after 9/11 tragedy. Vulnerability assessment do identifies and assesses potential security threats, risks, and vulnerabilities and guides the chemical facility industry in making security improvements. The use of the vulnerability assessment is limited to preventing or mitigating terrorist or criminal actions that could have significant national impact, such as the loss of chemicals vital to the national defense or economy or could seriously affect localities, such as the release of hazardous chemicals that would compromise the integrity of the facility, contaminate adjoining areas, or injure or kill facility employees or adjoining populations. It's basically to prevent terrorist or criminals actions that can leave a significant impact on the nations by reducing the risks level from being attack [3]

Security threats can come from internal or external adversaries. Internal threats include disgruntled employees and/or contractors, employees forced into cooperation by threat of extortion or violence. External sources include criminals, extremists or terrorists. The most important objective of an adversary, next to successfully completing the mission, is not being detected. Detection usually results in a failed mission. Because the external adversaries may not need to enter your plant, there are few mitigation options for increasing the likelihood of detection prior to the attack. Furthermore, as a recent article "Terrorists focus on simple means (to avoid detection). They are going to use stuff that's available."[USA Today The Forum States] We need to think like terrorists if we want to prevent an attack. "We're looking for this big, magical attack, and the terrorists are looking for stuff that's already in the environment." Some chemical companies have already decided that protecting their assets from attack by armed combatants with military caliber weapons is the responsibility of government and local authorities.[1]

Furthermore, coupled with the terrorist's desire to be unobtrusive, such a scenario is not a high priority for prevention. Given that a chemical plant became the target, a more plausible scenario is the detonation of an ammonium nitrate and distillate fuel oil next to a storage tank. This only requires stuff that is already in the local environment.[1]

Nowadays, VA is a mandatory requirement for the chemical plants in Europe and America but not in Asia. In the future, the VA will set the foot in Asia to be implemented more vigorously[9] For the Oil and Gas industry in Malaysia, it is important to conduct a study on the risk assessment of vulnerability impacts against the predicted variations from the national and international models, [Dr. Foo Say Moo, PETRONAS][9]

1.1 PROBLEM STATEMENT

The vulnerability assessment is usually used by the European and American companies. However, it is not yet implemented in Asia, especially Malaysia. As the time goes on, the vulnerability assessment will be one of the mandatory requirements in the Asian. PETRONAS, as one of the Oil and Gas Company in the world, have been looking to these issues seriously [9]. The application of vulnerability assessment in Asian especially Malaysia will face some difficulties since there are no exact framework to be as example or guidance. There are three vulnerability assessments available in which the applications depend on its suitability to the company. Each of the assessments does have the advantages and disadvantages. Proper research is needed to determine which assessment suit to PETRONAS. As the pioneer of this assessment, case study is needed to be the example for the future use.

1.2 OBJECTIVES

The main objectives of this research are:

- To study the vulnerability assessment framework
- To apply the vulnerability assessment framework by doing a case study in one of the PETRONAS Operation Unit(OPU)

1.3 SCOPE OF STUDY

- Vulnerability Assessment Method (VAM) by Sandia National Laboratories

  Sandia VAM method can be said as the complete set of vulnerability assessment since it include all the process that are needed in this project such as site survey for a case study. There was an attempt to make the Sandia VAM as a regulated standard for vulnerability assessment but this appears to be less likely due to the changes in the Congress, Washington Update, *Passage of Chemical Security Act Seems Unlikely,* CEP November 2002. The VAM was chose due to it completeness [R. Peter Stickles et-al][1]

- Considered only the worse case scenario [3]
- Adversary type of attack is terrorist attack [3]
- Case study on Vinyl Chloride Malaysia Sdn Bhd (VCMSB)
- Has significant impact on the nation [3]
- Has a tool onsite inventory of threshold quantities (TQ) or greater of chemical covered under Federal regulation 40 CFR 68.130 [3][7]

1.4 THE RELEVANCY AND FEASIBILITY OF THE PROJECT

The wars in the middle-east have increased the possibility of Malaysia to be attack by the terrorist. The terrorist might chose the PETRONAS process plant as a target to break down the economic since PETRONAS is the major economic contributor to the Malaysia. As the economic sector collapse, other foreign country will use this opportunity to get involve with Malaysia, hence controlling the country. Vulnerability assessment seems to be very important to the Malaysia due to the PETRONAS plant process presence.

CHAPTER 2
LITERATURE REVIEW

2.0 VULNERABILITY ASSESSMENT

The use of vulnerability assessment (VA) is to prevent or mitigate the terrorist or criminal action that could have a significant impact on the nation, such as the lose of chemicals vital to the national defense or economy, or seriously effect the localities. Basically there are three methods to start the vulnerability assessment which are:

1. Vulnerability Assessment Methodology (VAM)
2. American Chemical Council (ACC)
3. Chemical Engineers Center for Chemical Process Safety (CCPS).

The U.S. Department of Justice, Office of Justice Programs has already supported the development of the Chemical Facility. Vulnerability Assessment Methodology (VAM), which was prepared by Sandia National Laboratories, Chemical industry groups including the American Chemical Council (ACC) and The American Institute of Chemical Engineers Center for Chemical Process Safety (CCPS) have also responded with their own guidelines and methodologies for assessing treats of attack from internal and external activities. [4]

TABLE 3: Summary Of The Features Of Three Public Domain Methodologies

Element	ACC SSG	CCPS SVA	Sandia VAM
Screening	Step 1: Chemical Hazard Evaluation: • How likely is a chemical release, and • How harmful would it be?	Enterprise Level Screening • Relative Difficulty of Attack factor considers ease of access and complexity of logistical support • Relative Severity factor considers population density within the radius of impact of RMP "worst case" scenario.	1.0 Screening • Specify undesired events • Evaluate consequences of Undesired Events
Threat Identification Assessment	Step 2: Process Hazard Analysis Step 3: Consequence Assessment Step 4: Physical Factors Assessment	Step 2: Facility Characterization: • Assets/hazard ID, Consequence analysis Attractiveness analysis, Layers of protection review Step 3: Threats Assessment: • Adversary ID/ characterization	3.0 Planning: • Characterize facility • Derive severity levels • Threat Assessment 4.0 Site Survey
Risk Analysis		Step 4: Vulnerability Analysis • Target classification or Site security review and scenario development • Risk analysis	5.0 Analysis • Systems effectiveness analysis • Risk Analysis
Mitigation	Step 5: Mitigation Assessment	Step 5: Identify Countermeasures	6.0 Risk Reduction
LESS	⇦ Formalized Methodology ⇨		MORE

Figure 2.0(a) : Summary of the Features of Three Public Domain Methodologies

Figure 2.0(a) does differentiate the three public domain method to do VA. All the three methods can be applied in all countries such as Malaysia. ACC SSG method is the simplest way to do the vulnerability assessment. In the ACC SSG method, the risk analysis is not included in one of the steps. For the CCPS SVA method, the contents do include the risk analysis and more details compare to the ACC SSG. However, in CCPS SVA, the site survey process is not included. [1]

The prototype Vulnerability Assessment Model (VAM) developed for this project is a systematic, risk based approach in which risk is a function of the severity of consequences of an undesired event, the likelihood of adversary attack, and the likelihood of adversary success in causing the undesired event. For the purpose of the VAM analyses:Risk is a function of S, LA, and LAS.[3]

S= severity of consequences of an event.
LA= likelihood of adversary attack.
LS= likelihood of adversary attack and severity of consequences of an event.
LAS= likelihood of adversary success in causing a catastrophic event.

The VAM compares relative security risks. If the risks are deemed unacceptable, recommendations can be developed for measures to reduce the risks. For example, the severity of the consequences can be lowered in several ways, such as reducing the quantity of hazardous material present or siting chemical facilities (CFs) farther from populated areas. Although adversary characteristics generally are outside the control of CFs, they can take steps to make themselves a less attractive target and reduce the likelihood of attack to their facilities. Reducing the quantity of hazardous material present may also make a CF less attractive to attack. The most common approach, however, to reducing the likelihood of adversary success in causing a catastrophic event is increasing protective measures against specific adversary attack scenarios. Because each undesirable event is likely to have its own consequences, adversaries, likelihood of attack, attack scenario, and likelihood of adversary success, it is necessary to determine the risk for each combination of risk factors.[3]

CHAPTER 3
VULNERABILITY ASSESSMENT METHOD FRAMEWORK

3.0 SCREENING FOR THE NEED FOR A VULNERABILITY ASSESSMENT

Screening chemical facilities has two purposes which are, for individual Chemical Facilities (CFs), the screening determines whether or not a vulnerability assessment (VA) should be conducted and for organizations with more than one CF, the screening determines which CFs should undergo Vas and prioritizes them. [3]

3.1 DEFINING THE PROJECT

After a CF has been screened and selected for a VA, the next step is to assign a facilitator trained in the VAM to define the VA project for that facility. Defining the project includes reviewing the purpose of the work to be performed, the tasks to be accomplished, and the resources to be allocated; creating a schedule of activities; and assembling a team to accomplish the work. The team may be the same one that prepared the process hazards analysis (PHA) for the facility, with the addition of one or more employees with security responsibilities. The project definition should be documented in a written statement that may be amended as the VA progresses. [3]

3.2 CHARACTERIZING THE FACILITY

An early step in security system analysis is to describe thoroughly the facility, including the site boundary, building locations, floor plans, access points, and physical protection features; and the processes that take place within the facility. This information can be obtained from several sources, including design blueprints, process descriptions, the PHA report, the RMP, the piping and instrument drawing (P&ID), and site surveys.[3]

3.2.1 The Facility Characterization Matrix

The facility characterization matrix organizes the security factors for each processing activity and provides a framework for determining and prioritizing the critical activities[3]

3.2.2 Process Flow Diagram

A process flow diagram must be created that shows the use of each reportable chemical that can be exploited to create an undesired event. The diagram prepared for the PHA to determine the critical processing activities can be used for the VA as well.[3]

Figure 5 presents a form for recording the use and handling of chemicals and the hazard reduction measures available at each stage in the manufacturing process. The information recorded can then be used to analyze the manufacturing process to determine the critical activities

	Manufacturing Steps				
	Incoming	Staging In	In Process	Staging Out	Outgoing
Use and handling of chemicals					
Manufacturing activities					
Regulated chemicals used*					
Quantity/form/concentration					
Location/duration					
Accessibility					
Recognizability					
Hazard reduction measures					
Physical protection					
Process control protection					
Active mitigation					
Passive mitigation					
Safety procedures					
*Chemicals or other hazardous substances listed in 40 CFR 68.130 or 29 CFR 1910.119.					

Figure 5: Form for Analysis of Operating Activities[3]

3.2.3 Process Control Flow Diagram

A flow diagram can be developed for the process control system for each critical activity. A generic process control flow diagram is provided in Figure 6. Process control is normally a closed cycle in which a sensor provides information to a process control software application through a communications system. The application determines if the sensor information is within the predetermined (or calculated) data parameters and constraints. The results of this comparison are fed to an actuator, which controls the critical component. [3]

This feedback may control the component electronically or may indicate the need for a manual action. This closed-cycle process has many checks and balances to ensure that it stays safe. The investigation of how the process control can be subverted is likely to be extensive because all or part of the process control may be oral instructions to an individual monitoring the process. It may be fully computer controlled and automated, or it may be a hybrid in which only the sensor is automated and the action requires manual intervention. Further, some process control systems may use prior generations of hardware and software, while others are state of the art.[3]

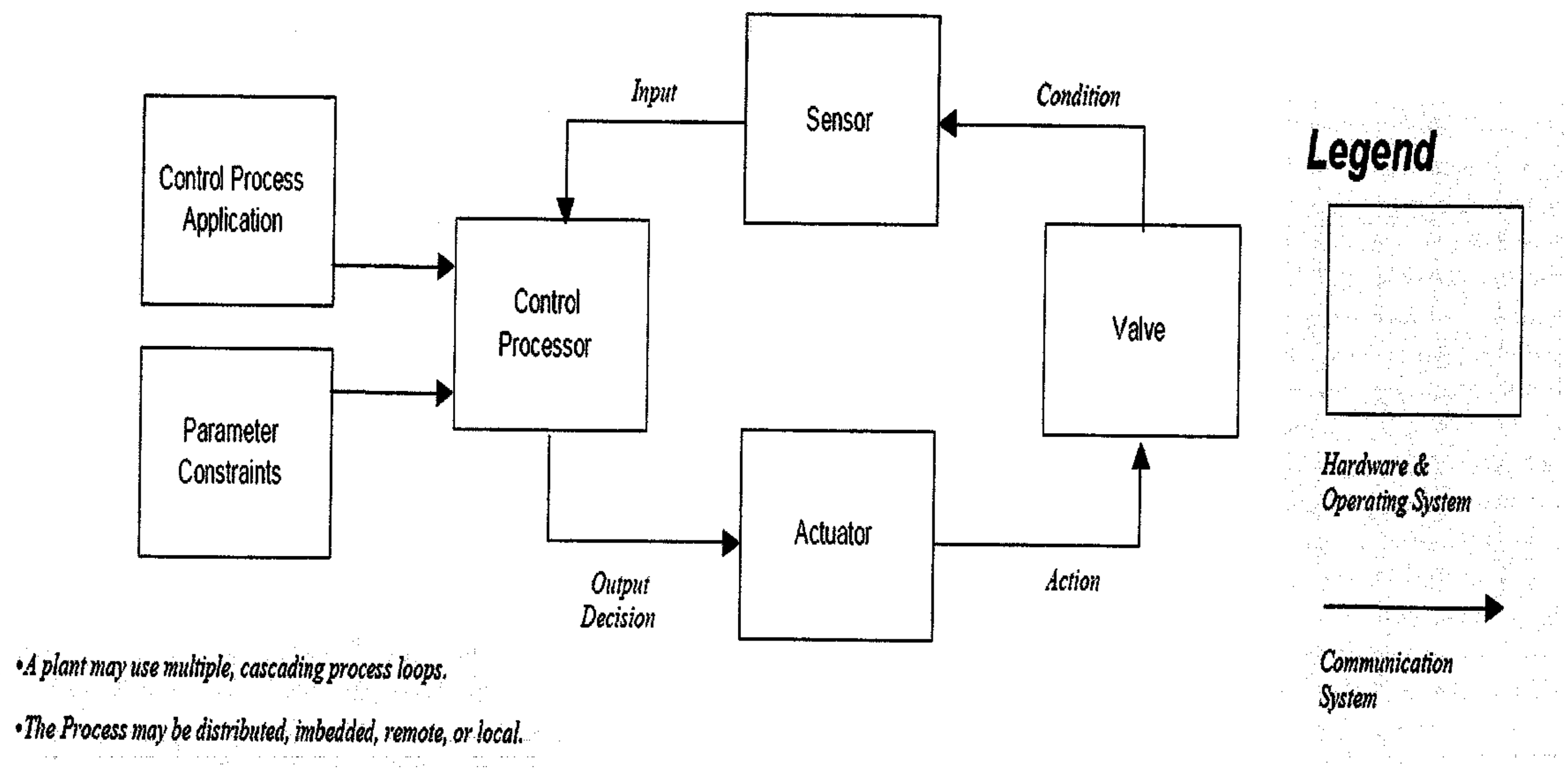


Figure 6: Generic Process Control [3]

3.3 DERIVING SEVERITY LEVELS

The severity of consequences for each undesired event must be derived. For facilities that have conducted PHAs, the severity table created for the PHA should be considered first. This table may need to be modified to account for the consequences of a malevolent (rather than an accidental) event. Another source of data to help determine the severity of consequences is the analysis of the offsite consequences of the worst case and alternative-release scenarios. (The results of these analyses may also need to be modified.) Figure 7 provides sample definitions of severity levels from 1 to 4. CFs that must submit RMPs most likely will be rated at severity level 1. [3]

The sample definitions below are most useful to CFs that do not have to submit RMPs but have decided to perform a VA. This table should be made site specific because various CFs and communities may assign different severity levels to similar consequences. Each undesired event will be assigned a severity level based on the consequences defined by the severity level definition table. This severity value (S) will be used in the risk analysis.[3]

S	Definition
1	Potential for any of the following resulting from a chemical release, detonation, or explosion: worker fatalities, public fatalities, extensive property damage, facility disabled for more than 1 month, major environmental impacts, or evacuation of neighbors.
2	Potential for any of the following resulting from a fire or major chemical release: nonfatal injuries, unit disabled for less than 1 month, or shutdown of road or river traffic.
3	Potential for any of the following resulting from a chemical release: unit evacuation, minor injuries, or minor offsite impact (for example, odor).
4	An operational problem that does not have potential to cause injury or a reportable chemical release with no offsite impact.

Figure 7: Sample Severity Level Definitions [3]

3.4 ASSESSING THREATS

3.4.1 Describing the general threat.

A general description of the threat is required to estimate the likelihood that adversaries might attempt an attack. This description includes the type of adversary and the tactics and capabilities (for example, the number in the group, weapons, equipment, and mode of transportation) associated with each threat. [3]

3.4.2 Defining the site-specific threat.

The threat also must be defined for each specific site. The definition includes the number of adversaries, their modus operandi, the type of tools and weapons they would use, and the type of events or acts they are willing to commit. It is important to update a site's threat analysis regularly, especially when obvious changes in threat occur.[3]

An example of the result of the information collection is shown in Figure 8. This threat information is used to develop adversary scenarios and estimate the effectiveness of the protection system.

Type of Adversary	Number	Equipment	Vehicle	Weapon	Tactic
Terrorist outsider (may include an insider colluding)	2-3	Handtools Power tools Body armor Chemicals Biological agents	4x4 All-terrain vehicles Pickup trucks Aircraft	Handguns Automatics Explosives	Cause catastrophic events Theft
Criminal	2-3	Handtools Body armor	Foot Truck Aircraft	Handguns Explosives	Extortion Theft
Extremist	5-10	Signs Chains Locks Handtools	Cars Buses	No weapons	Protests Civil disobedience Damage Destruction
Insider	1	Onsite equipment	Cars Pickup trucks 4x4	Handguns Automatics Explosives	Destruction Violence Theft
Vandal	1-3	Paint	Cars Pickup trucks	Hunting rifles	Random shootings Tagging

Figure 8: Sample Site-Specific Threat Description[3]

After the threat spectrum has been described, the information can be used together with statistics of past events and site-specific perceptions of threats to categorize threats in terms of likelihood that each would attempt an undesired event [3]. The Department of Defense (DoD) standard definitions1 have been modified for use in categorizing the threats against CFs, as shown in Figure 9

LA	Definition
1	Threat exists, is capable, has intent or history, and has targeted the facility.
2	Threat exists, is capable, has intent or history, but has not targeted the facility.
3	Threat exists and is capable, but has no intent or history and has not targeted the facility.
4	Threat exists, but is not capable of causing undesired event.

Figure 9: Definitions of Level of Likelihood of Attack (LA)[3]

3.5 PRIORITIZING CASES

After the severity (S) of each undesired event and the likelihood of attack (LA) for each adversary group have been determined, these values are ranked in a matrix (Figure 10) to derive the LS values. If, for example, an adversary group has a level 2 likelihood of attack for a specific undesired event and the undesired event has a severity level of 3, the likelihood and severity level (LS) would be 3. Priority cases would be those undesired event/adversary group pairs with a likelihood and severity (LS) value closer to 1 than the value chosen by the CF. These priority cases should be analyzed further for protection system effectiveness.[3]

Ls	Severity of Consequences (S)				
Likelihood of Attack (L_A)		1		3	4
	1	1	1		4
		1		3	4
	3		3	4	4
	4	3	4	4	4

Figure 10: Sample Likelihood and Severity Priority Ranking Matrix [3]

3.6 PREPARING FOR SITE ANALYSIS

To prepare for the analysis to determine the effectiveness of the site protection system, background information should be assembled. This information should include site drawings, the PHA, physical protection system (PPS) features, and process control data. Information worksheets have been developed to collect site information needed for the effectiveness analysis and documentation.[3]

An effective PPS will neutralize the adversary and prevent an undesired event with a high degree of confidence. The more effective the PPS, the less likely the adversary will succeed. Thus LAS is derived directly from estimates of the PPS effectiveness, as shown in the definition table (Figure 11). The facilitator should develop a definition table for the levels of likelihood of adversary success for the physical protection system that is specific to the site.[3]

L_{AS}	Definition
1	Ineffective or no protection measures; catastrophic event is expected.
2	Few protection measures; catastrophic event is probable.
3	Major protection measures; catastrophic event is possible.
4	Complete protection measures; catastrophic event is prevented.

Figure 11: Sample Definitions of Likelihood of Adversary Success (L_{AS})[3]

The final step of preparing for the system effectiveness analysis is to create a priority ranking matrix that combines likelihood and severity of attack (LS) (the matrix for which is presented in Figure 10) and likelihood of adversary success (LAS) (see Figure 12). The completed matrix will be used to estimate risk levels.[3]

Risk	Likelihood of Adversary Success (L_{AS})				
Likelihood and Severity of of Attack (L_S)		1		3	4
	1	1	1		4
		1		3	4
	3		3	4	4
	4	3	4	4	4

Figure 12: Sample Risk Priority Ranking Matrix [3]

3.7 SURVEYING THE SITE

The information, drawings, and worksheets that were assembled and completed by the facilitator should be reviewed by the entire team for accuracy and validation in preparation for the system effectiveness analysis that follows. A walk-through survey of the site should be done with special emphasis on verifying critical activities and target information.[3]

3.8 ANALYZING THE SYSTEM'S EFFECTIVENESS

Estimating system effectiveness means judging whether the protection features of the facility are adequate to prevent the undesired event from occurring. For each critical activity, two or more estimates of protection system effectiveness will be made: One or more for the physical protection system and one or more for the protection system for process control. For the physical protection system, the first estimate measures the system's effectiveness in preventing the undesired event. If the undesired event cannot be prevented, another estimate measures the system's effectiveness in detecting the event and mitigating its consequences so that the event is not catastrophic.[3]

After the most vulnerable adversary strategies for each undesired event have been established, adversary paths to the critical assets to cause that event are considered. Site layout drawings may help summarize all possible physical paths from outside the facility into areas that house critical assets[3]. Figure 13 illustrates a layout drawing with possible adversary paths.

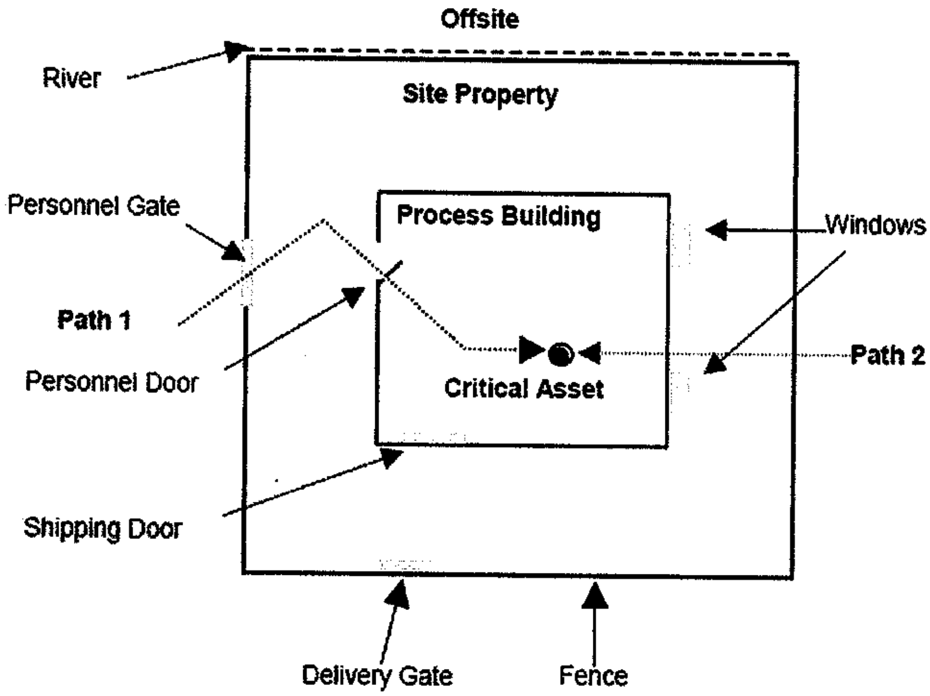


Figure 13: Possible Adversary Paths[3]

The adversary sequence diagram (ASD), which models the facility's physical protection system, identifies paths that adversaries can follow to commit sabotage or theft. ASDs help prevent overlooking possible adversary paths and help identify protection system upgrades that affect the paths most vulnerable to adversaries. Exhibit 14 presents an ASD for the facility shown in Figure 13. The most vulnerable adversary path is used to measure the effectiveness of the physical protection system.[3]

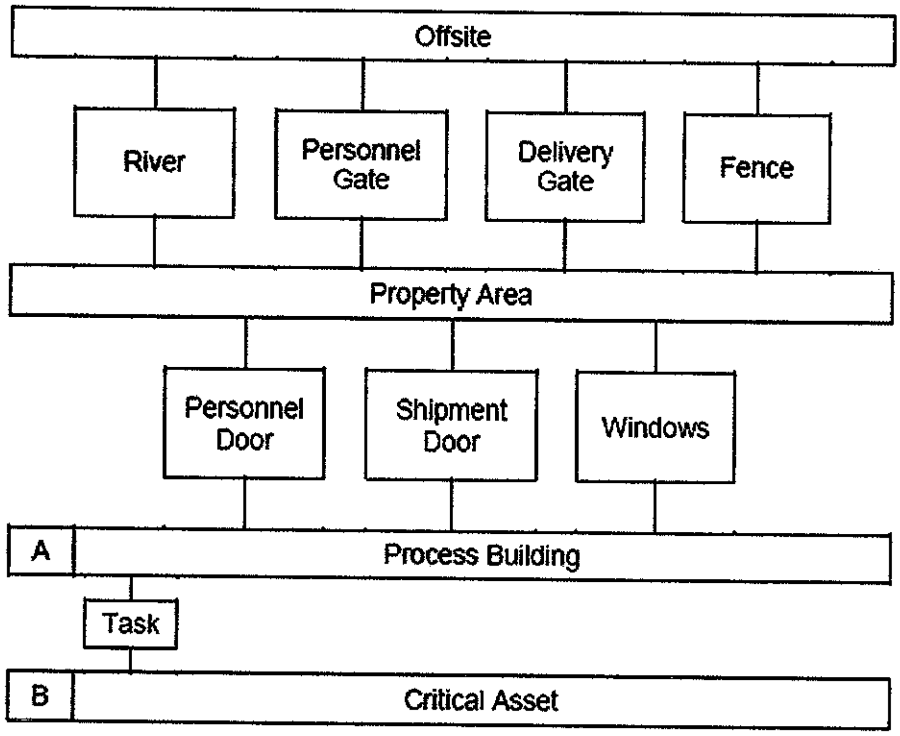


Figure 14: Sample Facility Adversary Sequence Diagram[3]

3.7.1 Physical Protection Features for Scenario

The features of the facility that support the functions of detection, delay, response, and mitigation and any safety features that could affect the outcome of the adversary scenario should be noted. These features can be identified from the facility worksheets used to determine the system's effectiveness, the characterization matrix, and facility personnel's knowledge of such features. [3] Figure15 presents a sample adversary scenario and lists site features for each system function.

Detection Features	Delay Features	Response Features	Mitigation/ Safety Features
• Security officer personnel entrance • Camera surveillance of building perimeter • Personnel during working hours • Process sensors	• Property fence—6-foot chain link • Standard doors and locks	• Local law enforcement can respond in 30 minutes • Personnel during working hours	• Process safety controls

Figure 15: Sample Scenario and Protection System Features[3]

3.7.2 Protection for Process Control Scenario

The features of the process control protection system that could affect the outcome of the adversary scenario should be noted. As with the physical protection system, these features can be identified from facility worksheets used to evaluate the system's effectiveness, the characterization matrix, and facility personnel's knowledge of the features. The system must protect the process control features mentioned in the section on preparing the site analysis: communications, commercial hardware and software, application software, and parameter data or support infrastructure (for example, power and HVAC)[3]. Figure 16 proposes a process control adversary scenario and lists process control features that can protect against that scenario

Communications	Commercial Hardware and Software	Application Software	Parameter Data	Support Infrastructure
• Encryption • Lock and sensor communications rooms • Supervised lines • Authentication • Redundant systems	• Current security patches • Strong passwords • Audits • Monitoring unusual use	• Configuration control • Trusted source • Documentation • Thorough testing	• Validate value and effect • Configuration control • Read only • Authenticate written privilege	• Uninterruptable power supply • Automatic switch to backup • Environmental controls

Figure 16: Sample Process Control Protection Features[3]

3.9 ANALYZING RISKS

A brief review of the methodology is presented below in preparation for risk analysis. For the purposes of this methodology,

Risk is a function of S, LA, and LAS.
S= severity of consequences of an event
LA= likelihood of adversary attack
LS= likelihood of adversary attack and severity of consequences of an event
LAS= likelihood of adversary success in causing a catastrophic event

Priority cases for an undesired event or adversary group were determined by estimating the likelihood and severity level (LS) using the priority ranking matrix for likelihood of attack (LA) and severity (S) (see Figure 10). LS levels are combined with LAS levels to estimate the level of risk for each undesired event/adversary group (see Figure 12). Figure 17 is a flowchart for the process, and Figure 18 summarizes the results of the risk analysis.[3]

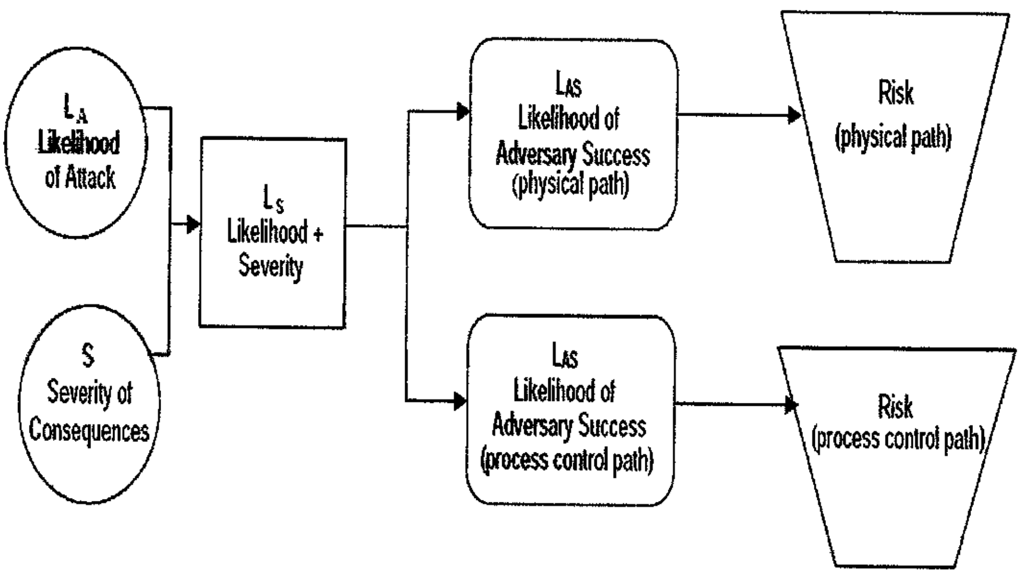


Figure 17: Risk Analysis Flowchart[3]

Risk Level Summary	Undesired Event = ______ Severity (S) = ______					
	Adversary Group	Ls	Las (physical)	Risk (physical)	Las (process control)	Risk (process control)
Activity 1						
Activity 2						
Activity 3						

Figure 18: Risk Level Summary[3]

3.10 MAKING RECOMMENDATIONS FOR RISK REDUCTION

If the risk level is 1, 2, or 3, detection, delay, response, and mitigation/safety features that eliminate or mitigate the specific identified vulnerabilities should be suggested. The goal is low-cost, high-return upgrades. [3]

3.11 PREPARING THE FINAL REPORT

The final report and package for briefing management can be prepared from the worksheets when completing the analysis. [3]

CHAPTER 4

RESULTS (CASE STUDY) AND DISCUSSION

Vinyl Chloride (Malaysia) SDN BHD

PETRONAS VINYL CHLORIDE	**Vulnerability Assessment Method (VAM)**	**Facilitator: Mohd Hafez Bin Mamujalean** **Assistant : Esa Bin Diman**

4.0 SCREENING FOR THE NEED OF VULNERABILITY ASSESSMENT (VA)

The screening process is based primarily on the possible consequences of potential terrorist incidents at chemical facilities. In order to fulfill the screening processes, several information are needed such as the desired event, the impact on the nation, and the facility tools. For the desired event, an offsite release was considered. If the lose of the facility have a significant impact on the nation, the VA information need to be classified. If the facility has a tool onsite inventory of threshold quantities (TQ) or greater of chemical covered under Federal regulation 40 CFR 68.130, further screening is needed to estimate the number of people that would be affected under the worst-case-scenario.[3] For the case study, the Vinyl Chloride Malaysia Sdn Bhd (VCMSB) was selected to be undergoing the vulnerability assessment due to the feasibility on collecting data.

4.1 DEFINING THE VCMSB PROJECT

Table 4.0 (a): VA Screening Summary

Company	Vinyl Chloride Malaysia Sdn Bhd (VCMSB)
Assistant	Technical and Services Departmen Executive Engineer, Esa Bin Diman
Impact on the nation	Terrorist attack has a significant impact on the nation especially in the tourism industries. According to Department of Foreign Affairs and Trade (Australia), Several cautions have been issued for tourist who chose Malaysia as their holiday location due to the high risk of terrorist attack. The law fall under Safety and Security: Local Travel (piracy update) [8]
Threshold Quantities (TQ)	Greater [7]

4.1.1 Threshold Quantities (TQ) for VCMSB

VCMSB Raw Materials:

1. Ethylene
2. Hydrochloric Acid
3. Oxygen

Oxychlorination Process

$C_2H_4 + 2HCl + 1/2O_2 \rightarrow C_2H_4Cl_2 \text{ (EDC)} + H_2O$

EDC Cracker Process

$C_2H_4Cl_2 \rightarrow C_2H_3Cl \text{ (VCM)} + HCl$

1mol basis of oxygen = 7135 kg/hr

C_2H_4 (Ethylene)	= 7135 kg/hr
2HCl(Hydrochloric Acid)	= 7135 x 2 = 14270 kg/hr
$C_2H_4Cl_2$(EDC)	= 7135 kg/hr
C_2H_3Cl(VCM)	= 7135 kg/hr

7135 kg/hr	= 15729.98 lbs/hr
14270 kg/hr	= 31459.93 lbs/hr

4.1.2 Threshold Quantities (TQ) in Federal Regulation 40 CFR 68.130

Ethylene	= 10000 lbs
Hydrochloric Acid	= 15000 lbs
EDC	= 10000 lbs
VCM	= 10000 lbs

*Oxygen is not stated in the Federal Regulation

All chemicals that are using in the VCMSB plant to produce Vinyl Chloride Monomer has a greater TQ in Federal Regulation 40 CFR 68.130

4.2 CHARACTERIZING THE VCMSB

An early step in a security system analysis is to describe thoroughly the facility, including the site boundary, building location, floor plans, access points, physical protection features and process involve. [3]

4.2.1 VCMSB Process Flow Diagram

A process flow diagram must be created to show the use of each reportable chemical that can be exploited to create an undesired event. The diagram prepared for the PHA to determine the critical processing activities can be used for the VA as well [3]. Figure 4.2 (a) presents the VCMSB process flow diagram.

Vinyl Chloride (Malaysia) SDN BHD

PETRONAS VINYL CHLORIDE	Plant-area Process Training VCM Plant Overview	Document Number	: VCM-PPT-001
		Revision	: 0
		Date	: 31/01/2007
		Page 15 of 44	

5. ISBL PROCESS FLOW AND DESCRIPTION

5.1. ISBL PROCESS FLOW

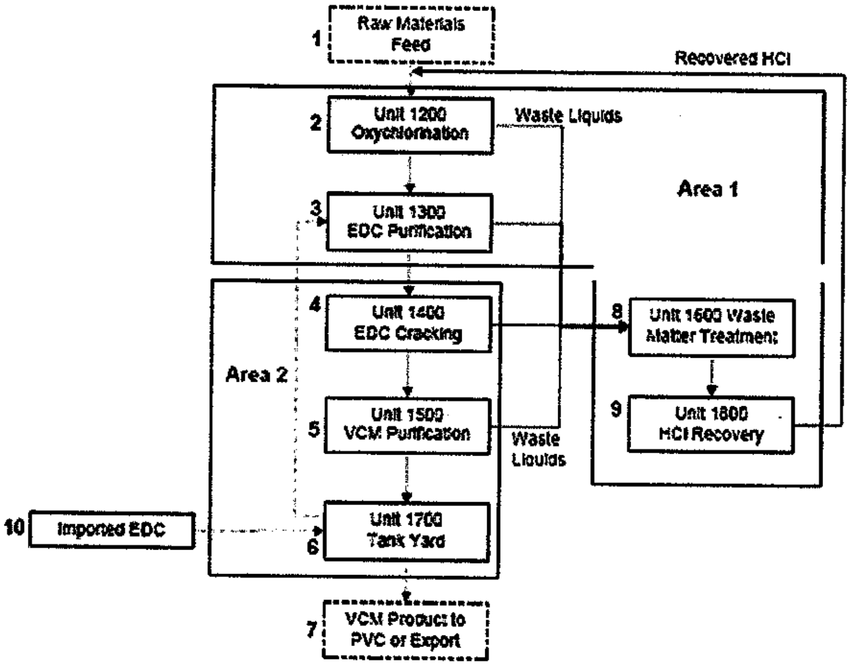


Figure 4.2 (a) : VCMSB Process Flow Diagram [6]

4.2.2 Process Control Flow Diagram

A process flow diagram can be developed for the process control system for each critical activity. Process control is normally a closed cycle in which a sensor provides information to a process control software application through a communications system. The application determines if the sensor information is within the predetermined (or calculated) data parameters and constraints. The results of this comparison are fed to an actuator, which controls the critical component. Figure 4.2 (b) represent a VCMSB flow diagram

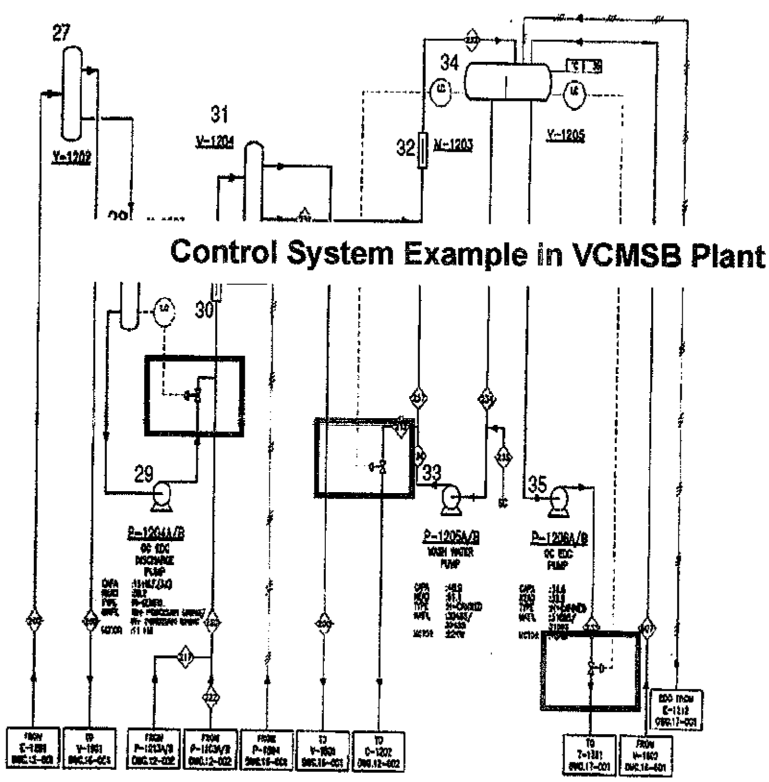


Figure 4.2 (b) : Example of Process Control in VCMSB P&ID [6]

This feedback may control the component electronically or may indicate the need for a manual action. This closed-cycle process has many checks and balances to ensure that it stays safe. The investigation of how the process control can be subverted is likely to be extensive because all or part of the process control may be oral instructions to an individual monitoring the process. It may be fully computer controlled and automated, or it may be a hybrid in which only the sensor is automated and the action requires manual intervention. Further, some process control systems may use prior generations of hardware and software, while others are state of the art. [3]

Table 4.2 (a) presents a form for recording the use and handling of chemicals and the hazard reduction measures available at each stage in the manufacturing process. The information recorded can then be used to analyze the manufacturing process to determine the critical activities

Table 4.2 (a) : Use of Handling of Chemicals and Hazard Reduction

	Manufacturing Steps				
	Incoming	Staging In	In Process	Staging Out	Outgoing
Use of Handling Chemicals					
Manufacturing Activities	Raw Materials from Storage Tank	Raw Materials into Reactor	Oxychlorination Process	Final Product Purification	Chemical Loading
Regulated Chemicals Used	Ethylene, Hydrochloric Acid, Oxygen	Ethylene, Hydrochloric Acid, Oxygen	Ethylene, Hydrochloric Acid, Oxygen	Ethylene Dichloride (EDC) and Vinyl Chloride Monomer (VCM)	Vinyl Chloride Monomer (VCM)
Quantity/Concentration	Higher then TQ	Higher then TQ	Higher then TQ	Higher then TQ	Higher then TQ
Location	Storage Tank	Mixer	Reactor	Distillation Column	Storage Tank
Accessibility	Easy	Hard	Medium	Medium	Easy
Recognizability	Easy	Hard	Hard	Hard	Easy
Hazard Reduction Measure					
Physical Protection	Full PPE	Full PPE	Full PPE	Full PPE	Full PPE
Process Control Protection	Feed Forward Control (Level Control)	-	Cascade Control (Temperature and Pressure)	Cascade Control (Pressure, Temperature, Flow, and Level)	Feed Forward Control (Level Control)
Active Mitigation	-	-	-	-	-
Passive Mitigation	-	-	-	-	-
Safety Procedures	Level Alarm Low (LAL) Level Alarm High (LAH)	-	-	-	Level Alarm Low (LAL) Level Alarm High (LAH)

4.2.3 The Facility Characterization Matrix

The facility characterization matrix organizes the security factors for each processing activity and provides a framework for determining and prioritizing the critical activities. Table 4.2 (b) present a VCM facility characterization matrix

Table 4.2 (b) : The Facility Characterization Matrix

No	Parameter	Activity 1	Activity 2	Activity 3	Activity 4	Activity 5	Activity 6	Activity 7	Activity 8	Activity 9	Activity 10
1	Process Activity	Chemical Storage	Feed inlet to the process	Oxychlorination Process	EDC Purification	EDC Cracker	VCM Purification	Final Product Storage	Final Product Loading	None	None
2	Covered Chemicals	Y	Y	Y	Y	Y	Y	Y	Y	None	None
3	Quantity of Chemicals Covered	1	1	1	1	1	1	1	1		
4	Process Duration	2	1	1	1	1	1	2	2		
5	Recognizability	1	4	4	3	3	3	1	1		
6	Accessibility	1	3	3	3	3	3	1	1		
7	Criticality Rating (Sum of Activity)	5	9	9	8	8	8	5	5		

1	**Process Activity**	Describe the activity (Example: Flow Diagram, P&ID, Reactor, Pipe, Storage, Tank and Etc)
2	**Covered Chemicals**	Enter the name of all the chemicals used in the activity. Enter Y if the chemical is listed in 40 CFR 68.130 or 29 CFR 1910.119. Enter N if not listed
3	**Quantity of Chemicals Covered**	Enter 1 if the quantity is more than 25 times threshold quantity (TQ), 2 if 10-25 times TQ, 3 if 1-10 times TQ and 4 if the quantity is TQ or less
4	**Process Duration**	Enter 1 if the process is 100% continuous, 2 if 50%-99% continuous, 3 if 25%-49% continuous and 4 if less than 25% continuous
5	**Recognizability**	Enter 1 if the target and importance are clearly recognizable with little or no prior knowledge, 2 if the target and importance are easily recognizable with a small amount of prior knowledge, 3 if the target and importance are difficult to recognize without some prior knowledge, and 4 if the target and importance requires extensive knowledge for recognition
6	**Accessibility**	Enter 1 if easily accessible, 2 if fairly accessible (target is located outside or in unsecured area), 3 if moderately accessible (target is located inside building or enclosure, and 4 if not accessible or only accessible with extreme difficulty
	Critical Activities	Activity 2, 3, 4, 5, and 6 — *The critical activity is the activity or activities with the lowest score under number 7 and above

4.3 DERIVING SEVERITY LEVELS

The severity of consequences for each undesired event must be derived. Each undesired event will be assigned a severity level based on the consequences defined by the severity level definition table as in Table 4.3 (a).

Table 4.3 (a): Activity 2 (Feed Inlet to Process) Severity Level

Severity (S)	Definition
1	Potential for any of the following resulting from a chemical release, detonation or explosion, worker fatalities, public fatalities, extensive property damage facilities disable for more than 1 month, major environment impacts or evacuation of neighbors
2	Potential for any of the following resulting from a fire or major chemical release, non fatal injuries, unit disable for less than 1 month, or shutdown of road or river traffic
3	Potential for any of the following resulting from a chemical release, unit evacuation, minor injuries, or minor offsite impact (Odor)
4	An operational problem that does not have potential to cause injury or a reportable chemical release with no offsite impact

Severity (S) = 1

Table 4.3 (b): Severity level for all activities

Activity	(S)	Information
Feed inlet to the process (Unit 1200)	1	Feed inlet to the reactor R-1201 do involve mixer M-1201 with high pressure 3.5b. The oxygen is mix with ethylene and hydrochloric acid before entered the reactor. The mixer do have potential risks involving chemical release, detonation, and etc.
Oxychlorination process (Unit 1200)	1	The reactor used for oxychlorination is fluidized bed reactor R-1201. Oxychlorination process is very exothermic. Major chemical released will occur when undesired event occur.
EDC purification (Unit 1300)	2	EDC will be purified in the column C-1401A/B/C/D.EDC is very dangerous and carcinogen. EDC release will not do a fatal injury to the worker
EDC cracking (Unit 1400)	2	EDC will be cracked in the furnace E-1405A/B/C/D in 450C. The furnace cracker failure will involve a major fire released.
VCM purification (Unit 1500)	2	VCM will be purified in the column C-1501A/B/C/D. VCM is very hazardous and carcinogen. VCM release will not do a fatal injury to the worker

4.4 ASSESSING THREATS

The threat also must be defined for each specific site. The definition includes the number of adversaries, their modus operandi, the type of tools and weapons they would use, and the type of events or acts they are willing to commit. It is important to update a site's threat analysis regularly, especially when obvious changes in threat occur. This threat information is used to develop adversary scenarios and estimate the effectiveness of the protection system.

Table 4.4 (a): Threat Description

Type of Adversary	Number	Equipment	Vehicle	Weapon	Tactic
Vandal	1-3	Paint	Cars, Motorcycle	Hunting rifles	Random shootings, Tagging
Insider	1	Onsite equipment	Cars, Pickup trucks	Handguns, Explosives	Destruction, Violence, Theft
Extremist	5-10	Signs, Chains, Locks, Hand tools	Cars, Buses, Van	None	Protest, Damage, Destruction
Criminal	2-3	Hand tools, Body armor	Foot, Truck, Aircraft	Handguns, Explosive	Extortion, Theft
Outsider Terrorist	2-3	Hand tools, Power tools, Body armor, Chemicals,	All terrain vehicles, Pickup trucks, Aircraft	Handguns, Explosive	Catastrophic events, Theft

After the threat spectrum has been described, the information is used together with statistics of past events and site-specific perceptions of threats to categorize threats in terms of likelihood that each would attempt an undesired event.

Table 4.4 (b) : Likelihood of Attack for Activity 2 (Feed inlet to process)

L (A)	Definition
1	Threat exist,is capable,has intent or history,and has targeted the facility
2	Threat exist,is capable,has intent or history,and but not targeted the facility
3	Threat exist and capable, but has no intent or history and not targeted the facility
4	Threat exist but not capable of causing undesired event

L (A) = 3

Table 4.4(c): Likelihood of Attack for all activities

Activity	L(A)	Information
Feed inlet to the process (Unit 1200)	3	Threats exist in Unit 1200 and capable of being attack. There are no history recorded in VCMSB and the unit is not yet targeted
Oxychlorination process (Unit 1200)	3	Threats exist in Unit 1200 and capable of being attack. There are no history recorded in VCMSB and the unit is not yet targeted
EDC purification (Unit 1300)	3	Threats exist in Unit 1300 and capable of being attack. There are no history recorded in VCMSB and the unit is not yet targeted
EDC cracking (Unit 1400)	3	Threats exist in Unit 1400 and capable of being attack. There are no history recorded in VCMSB and the unit is not yet targeted
VCM purification (Unit 1500)	3	Threats exist in Unit 1500 and capable of being attack. There are no history recorded in VCMSB and the unit is not yet targeted

4.5 PRIORITIZING CASES

After the severity (S) of each undesired event and the likelihood of attack (LA) for each adversary group have been determined, these values are ranked in a matrix (Table 4.5 a) to derive the LS values. If, for example, an adversary group has a level 2 likelihood of attack for a specific undesired event and the undesired event has a severity level of 3, the likelihood and severity level (LS) would be 3. Priority cases would be those undesired event/adversary group pairs with a likelihood and severity (LS) value closer to 1 than the value chosen by the CF. These priority cases should be analyzed further for protection system effectiveness

Table 4.5 (a) : Matrix of Severity (S) and Likelihood of Attack, L(A) for Activity 2

L (S)		Severity of Consequence (S)			
Likelihood of Attack L (A)		[redacted]	2	3	4
	1	1	1	2	4
	2	1	2	3	4
	3	[redacted]	3	4	4
	4	3	4	4	4

L (S) = 2

Table 4.5 (b): The likelihood and severity level for all activities

Activity	L(S)
Feed inlet to the process (Unit 1200)	2
Oxychlorination process (Unit 1200)	2
EDC purification (Unit 1300)	3
EDC cracking (Unit 1400)	3
VCM purification (Unit 1500)	3

4.6 VCMSB SITE ANALYSIS

To prepare for the analysis to determine the effectiveness of the site protection system, background information should be assembled. This information should include site drawings, the PHA, physical protection system (PPS) features, and process control data. Information worksheets have been developed to collect site information needed for the effectiveness analysis and documentation. An effective PPS will neutralize the adversary and prevent an undesired event with a high degree of confidence. The more effective the PPS, the less likely the adversary will succeed. Thus LAS is derived directly from estimates of the PPS effectiveness, as shown in the definition table (Table 4.6a). The facilitator should develop a definition table for the levels of likelihood of adversary success for the physical protection system that is specific to the site

Table 4.6 (a) : Likelihood of Adversary Success, L (AS) for Activity 2

L (AS)	Definition
1	Ineffective and no protection measures, catastrophic event is expected
2	Few protection measures, catastrophic event is probable
3	Major protection measures, catastrophic event is possible
4	Complete protection measures, catastrophic event is prevented

L (AS) = 4

Table 4.6 (b) : Likelihood of Adversary Success, L (AS) for all activities

Activity	L(AS)	Information
Feed inlet to the process (Unit 1200)	4	The mixer M-1201 is covered with thick concrete
Oxychlorination process (Unit 1200)	2	Reactor R-1201 is widely open to the atmosphere. There are possibility of causing the catastrophic events
EDC purification (Unit 1300)	2	Column C-1301A/B/C/D are widely open to the atmosphere. There are probability of causing the catastrophic events
EDC cracking (Unit 1400)	3	Furnace cracker E-1405A/B/C/D are build with a high temperature resistant steel. There are possibility of causing the catastrophic events
VCM purification (Unit 1500)	2	Column C-1501A/B/C/D are widely open to the atmosphere. There are probability of causing the catastrophic events

The final step of preparing for the system effectiveness analysis is to create a priority ranking matrix that combines likelihood and severity of attack (LS) and likelihood of adversary success (LAS) The completed matrix will be used to estimate risk levels.

Table 4.6.1 (a) : Matrix of Likelihood and Severity of Attack L (S)and Likelihood of Adversary Success L (AS) for Activity 2

Risk	Likelihood of Adversary Success L (AS)				
		1	2	3	4
Likelihood and Severity of Attack L (S)	1	1	1	2	4
	2	1	2	3	4
	3	2	3	4	[redacted]
	4	3	4	4	4

Risk = 4

Table 4.6.1 (b) : Risk for all activities

Activity	Risk
Feed inlet to the process (Unit 1200)	4
Oxychlorination process (Unit 1200)	3
EDC purification (Unit 1300)	3
EDC cracking (Unit 1400)	4
VCM purification (Unit 1500)	3

4.7 VCMSB SITE SURVEY

The information, drawings, and worksheets that were assembled and completed by the facilitator should be reviewed by the entire team for accuracy and validation in preparation for the system effectiveness analysis that follows. A walk-through survey of the site should be done with special emphasis on verifying critical activities and target information

4.8 ANALYZING THE SYSTEM'S EFFECTIVENESS

Estimating system effectiveness means judging whether the protection features of the facility are adequate to prevent the undesired event from occurring. For each critical activity, two or more estimates of protection system effectiveness will be made: One or more for the physical protection system and one or more for the protection system for process control. For the physical protection system, the first estimate measures the system's effectiveness in preventing the undesired event. If the undesired event cannot be prevented, another estimate measures the system's effectiveness in detecting the event and mitigating its consequences so that the event is not catastrophic.

After the most vulnerable adversary strategies for each undesired event have been established, adversary paths to the critical assets to cause that event are considered. Site layout drawings may help summarize all possible physical paths from outside the facility into areas that house critical assets. Figure 4.8 (a) illustrates a layout drawing with possible adversary paths.

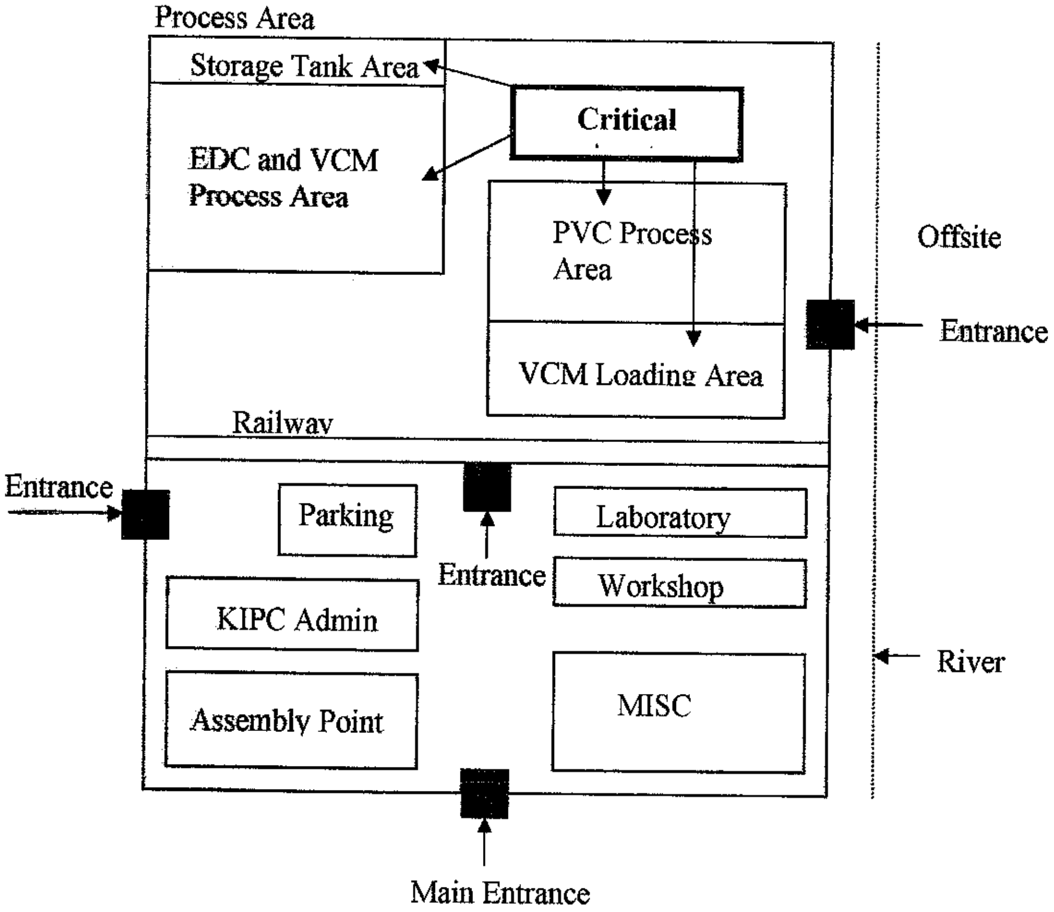


Figure 4.8 (a): Possible Adversary Paths [6[

The adversary sequence diagram (ASD), which models the facility's physical protection system, identifies paths that adversaries can follow to commit sabotage or theft. ASDs help prevent overlooking possible adversary paths and help identify protection system upgrades that affect the paths most vulnerable to adversaries. Figure 4.8 (a) and (b) present ASD for the facility. The most vulnerable adversary path is used to measure the effectiveness of the physical protection system.

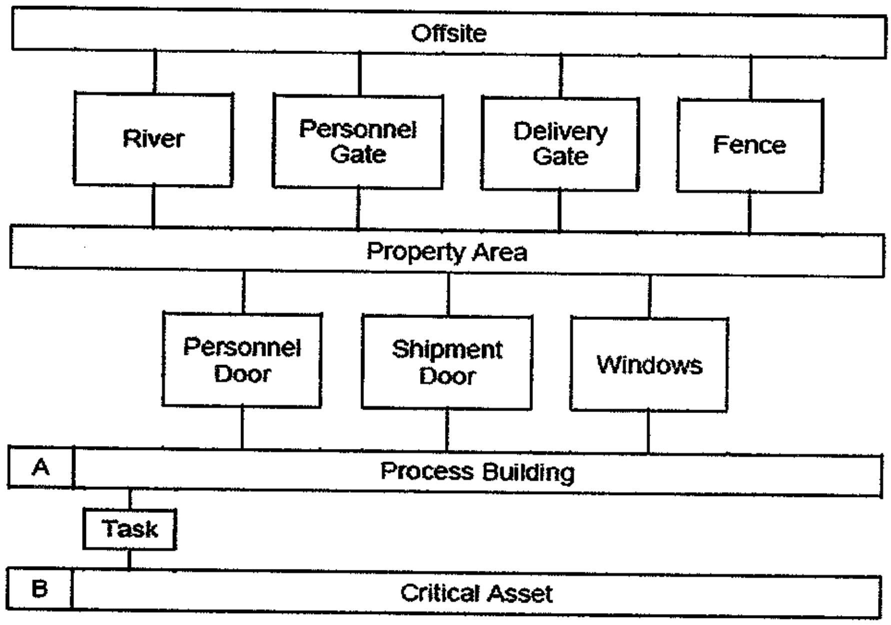


Figure 4.8 (b): Facility Adversary Sequence Diagram

4.8.1 Physical Protection Features for Scenario

The features of the facility that support the functions of detection, delay, response, and mitigation and any safety features that could affect the outcome of the adversary scenario should be noted. These features can be identified from the facility worksheets used to determine the system's effectiveness, the characterization matrix, and facility personnel's knowledge of such features. Figure 4.8 (c) presents the adversary scenario and lists site features for each system function.

Detection Features	Delay Features	Response Features	Mitigation/ Safety Features
• Security officer personnel entrance • Camera surveillance of building perimeter • Personnel during working hours • Process sensors	• Property fence—6-foot chain link • Standard doors and locks	• Local law enforcement can respond in 30 minutes • Personnel during working hours	• Process safety controls

Figure 4.8 (c): Scenario and Protection System Features[3]

4.8.2 Protection for Process Control Scenario

The features of the process control protection system that could affect the outcome of the adversary scenario should be noted. As with the physical protection system, these features can be identified from facility worksheets used to evaluate the system's effectiveness, the characterization matrix, and facility personnel's knowledge of the features. The system must protect the process control features mentioned in the section on preparing the site analysis: communications, commercial hardware and software, application software, and parameter data or support infrastructure. Figure 4.8 (d) proposes a process control adversary scenario and lists process control features that can protect against that scenario

Communications	Commercial Hardware and Software	Application Software	Parameter Data	Support Infrastructure
• Encryption • Lock and sensor communications rooms • Supervised lines • Authentication • Redundant systems	• Current security patches • Strong passwords • Audits • Monitoring unusual use	• Configuration control • Trusted source • Documentation • Thorough testing	• Validate value and effect • Configuration control • Read only • Authenticate written privilege	• Uninterruptable power supply • Automatic switch to backup • Environmental controls

Figure 4.8 (d): Process Control Protection Features[3]

The information above will be used to determine the Severity (S), Likelihood of Adversary Attack L (A), Likelihood of Adversary Attack and Severity L (S), Likelihood of Adversary Success L (AS) and the risk.

Table 4.8 (e): Summary of the Process Control VA

	(S)	L (A)	L (S)	L (AS)	Risk
Activity 2	2	1	1	2	1
Activity 3	3	1	2	2	2
Activity 4	1	4	3	3	4
Activity 5	2	3	3	4	4
Activity 6	2	2	2	1	1

4.9 ANALYZING RISKS

A brief review of the methodology is presented below in preparation for risk analysis. Priority cases for an undesired event or adversary group were determined by estimating the likelihood and severity level (LS) using the priority ranking matrix for likelihood of attack (LA) and severity (S) LS levels are combined with LAS levels to estimate the level of risk for each undesired event/adversary group

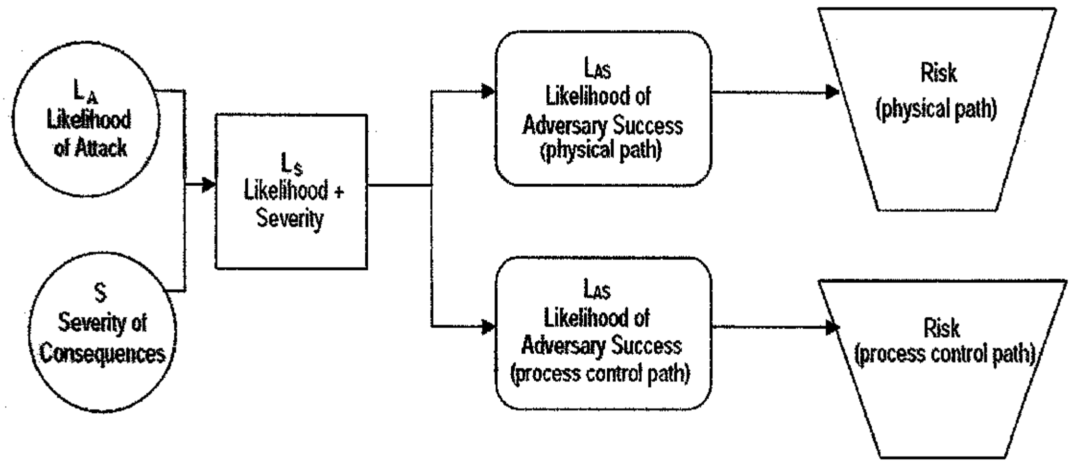


Figure 4.9 (a): Risk Analysis Flowchart[3]

Table 4.9 (a): Risk Level Summary

Risk Level Summary	Undesired Event = Severity (S) =	Activity 2, 3, and 6 1, 1, and 2				
	Adversary Group	L (S)	L (AS) (physical)	Risk (physical)	L (AS) (process control)	Risk (process control)
Activity 2	Terrorist Attack	2	4	4	2	1
Activity 3	Terrorist Attack	2	2	3	2	2
Activity 4	Terrorist Attack	3	2	3	3	4
Activity 5	Terrorist Attack	3	3	4	4	4
Activity 6	Terrorist Attack	3	2	3	1	1

From table 4.9 (a), activity 3, 4 and 6 have a physical risk level of 3 while for the process control risk, activity 2, 3 and 6 do have a risk level lower than 4. If the risk level is 1, 2, or 3, a few recommendations will be suggested. After recommendations are made, the new system effectiveness level and risk level should be estimated. The process continues until acceptable risk levels 4 are achieved

4.10 RECOMMENDATIONS FOR RISK REDUCTION [3]

1. Physical protection improvements (detection, delay, and response improvements); for example:

- Sensors on gates and doors.
- An assessment system (cameras).
- A security alarm control center.
- Hardened doors and locks.
- Access control (cards + PIN) on doors and gates.
- A compartmentalized facility.

2. Consequence reduction improvements (detection, mitigation improvements); for example:

- Reduction of quantity of controlled chemicals (to less than TQ).
- Dispersion of chemicals (in storage).
- Addition of mitigation measures conceived or known by facility personnel.

3. Process control protection improvements; for example:

- Chemical/process sensors routed to alarm control center.
- Protected and strong passwords that are changed regularly.
- Firewalls.
- Configuration control (of security patches/routing table/control parameters).
- Virus protection.
- Computer audits of activity on network.
- Encryption and authentication.
- Emergency backups/backup power.
- Redundant communication.
- Process control isolated from external information systems.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

5.0 CONCLUSION

Basically, all the VA methods (Vulnerability Assessment Methodology (VAM), American Chemical Council (ACC) and Chemical Engineers Center for Chemical Process Safety (CCPS)) can be applied within the PETRONAS. Due to the procedure completeness, the VAM is chose to be used in the case study in Vinyl Chloride Malaysia Sdn Bhd (VCMSB). There are twelve basic steps in the VAM, starting from the screening for the purpose of the VA until the final report. In order to fulfill the VAM, real databases from VCMSB are needed. However, due to copyright issue, certain data are unable to collect, hence affecting the result. Some dummy value was used to continue the case study. From the results, we can see that there are three activities in VCMSB plant that are need to be focus on due to its high risk. The three activities are feed inlet to the process, oxychlorination process and VCM purification. The risk is reducing by introducing the recommendation.

5.1 RECOMMENDATION

Due to time constraint and copyright issues, the VAM are not fully success. Actual data from plant and further research on the VAM need to be done in order to enhance the framework. Further studies on VAM need to be done in grouping since the VAM covered wide area

REFERENCES

1. Vulnerability Assessment Methodology for Electric Power Infrastructure by U.S Department of Energy Office of Energy Assurance (http://www.esisac.com/publicdocs/assessment_methods/VA.pdf)

2. National Oceanic and Atmospheric Administration (http://www.csc.noaa.gov/vata/glossary.html)

3. A method to Assess the Vulnerability of U.S Chemical Facilities by U.S Department of Justice; (http://www.ncjrs.gov/pdffiles1/nij/195171.pdf)

4. Anio Mosaic Corporation Whitepaper By : R. Peter Stickles, Henry Ozog and Sanjeev Mohindra (http://archives1.iomosaic.com/whitepapers/SVA.pdf)

5. National Institute for Occupational Safety and Health (http://www.cdc.gov/niosh/npg/npgsyn-a.html)

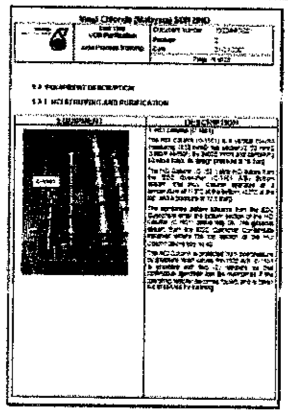
6. Vinyl Chloride Malaysia Sdn Bhd (VCMSB) Operation Manual and Data Sheets

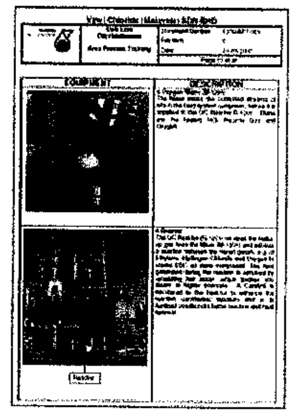
7. 40 CFR 68.130 - List of substances.(http://cfr.vlex.com/vid/68-130-list-substances-19801315)

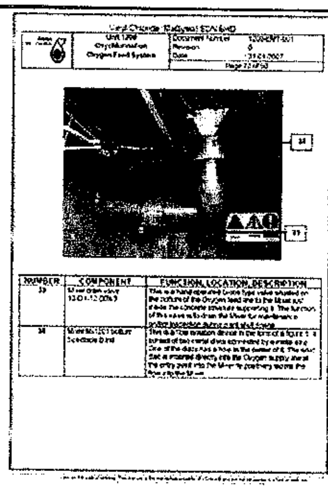
8. Smart Traveler, Australian Government Department of Foreign Affairs and Trade (http://www.smartraveller.gov.au/zw-cgi/view/Advice/Malaysia)

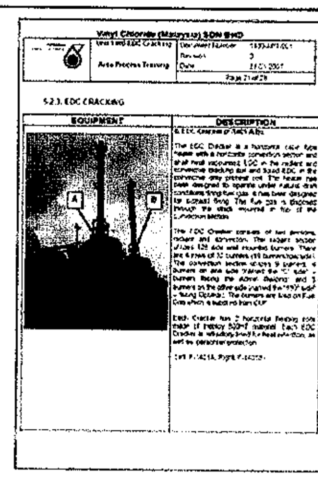
9. Climate *Vulnerability* Impact *Assessment* of. Malaysian Oil and Gas Industry. Dr. Foo Say Moo, *PETRONAS* (*www.ptm.org.my/PARM/pdf_files/Presentation%202-VA%20Progress.pdf*)

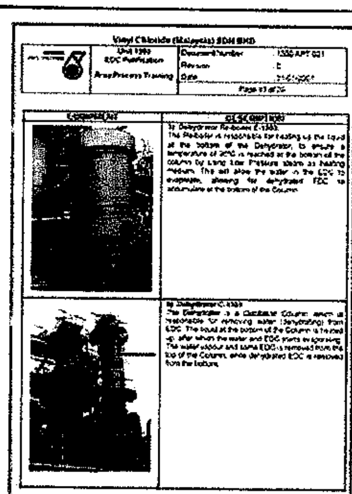
APPENDIX

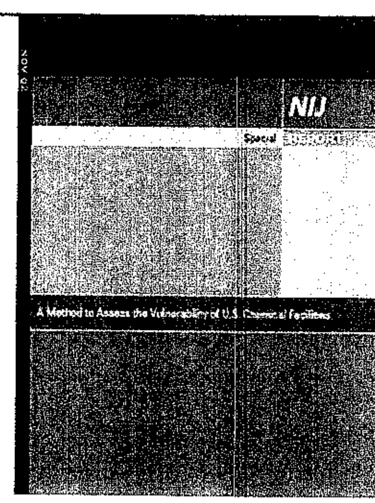


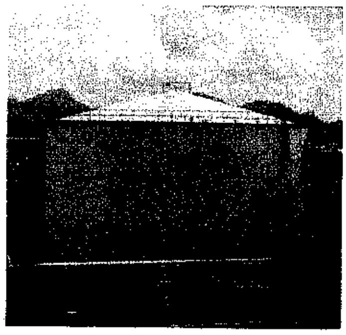




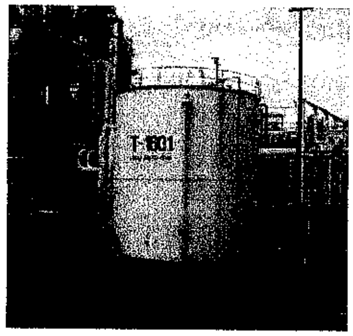





NIJ
Special Report
A Method to Assess the Vulnerability of U.S. Chemical Facilities

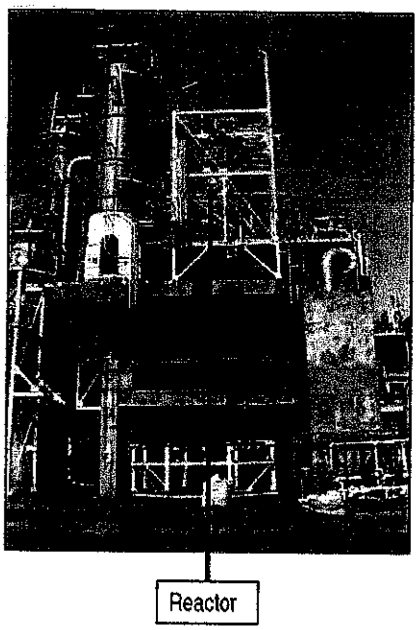


CONE ROOF TANK

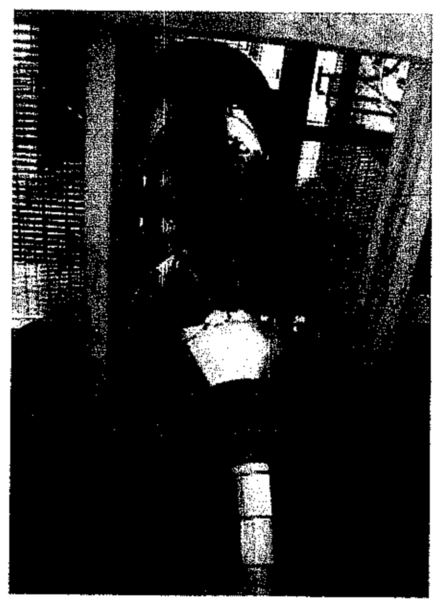


STORAGE TANK

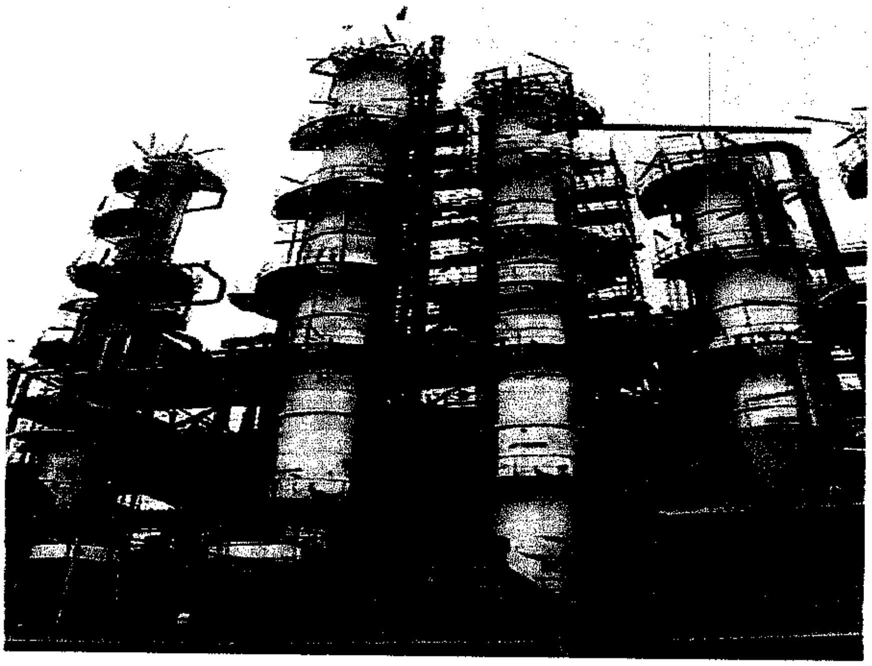
SPHERE VESSEL



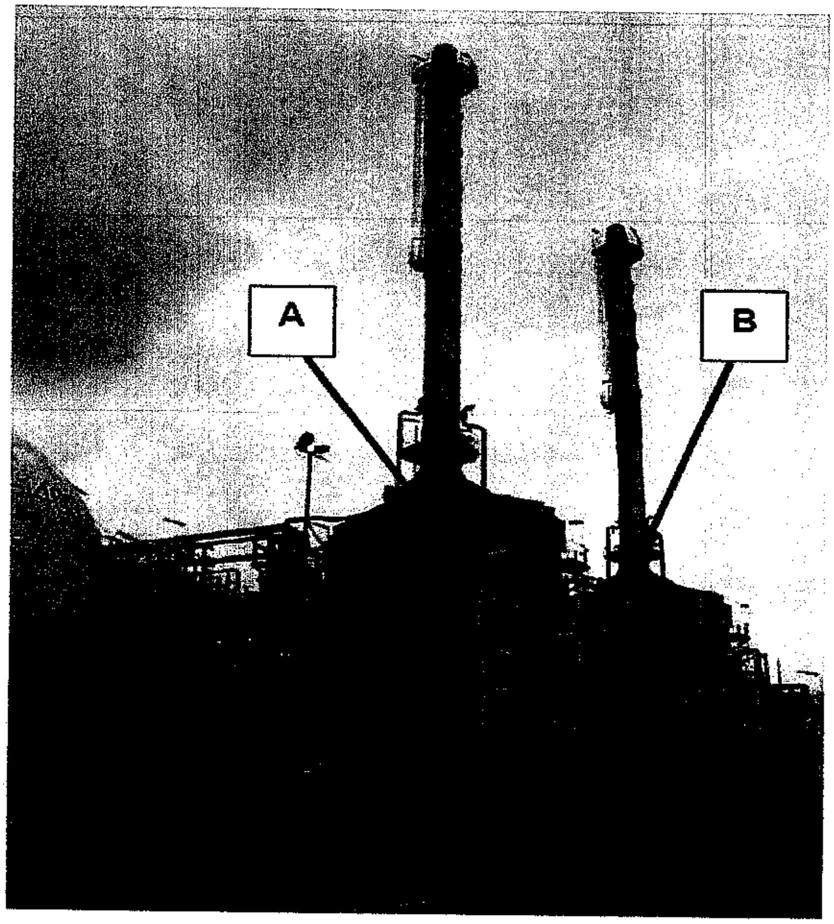
Oxychlorination Reactor



Mixer



EDC and VCM Purification Unit



EDC Cracker

TABLE 3 TO §68.130—LIST OF REGULATED FLAMMABLE SUBSTANCES [1] AND THRESHOLD QUANTITIES FOR ACCIDENTAL RELEASE PREVENTION—Continued

[Alphabetical Order—63 Substances]

Chemical name	CAS No.	Threshold quantity (lbs)	Basis for listing
Butane	106-97-8	10,000	f
1-Butene	106-98-9	10,000	f
2-Butene	107-01-7	10,000	f
Butene	25167-67-3	10,000	f
2-Butene-cis	590-18-1	10,000	f
2-Butene-trans [2-Butene, (E)]	624-64-6	10,000	f
Carbon oxysulfide [Carbon oxide sulfide (COS)]	463-58-1	10,000	f
Chlorine monoxide [Chlorine oxide]	7791-21-1	10,000	f
2-Chloropropylene [1-Propene, 2-chloro-]	557-98-2	10,000	g
1-Chloropropylene [1-Propene, 1-chloro-]	590-21-6	10,000	g
Cyanogen [Ethanedinitrile]	460-19-5	10,000	f
Cyclopropane	75-19-4	10,000	f
Dichlorosilane [Silane, dichloro-]	4109-96-0	10,000	f
Difluoroethane [Ethane, 1,1-difluoro-]	75-37-6	10,000	f
Dimethylamine [Methanamine, N-methyl-]	124-40-3	10,000	f
2,2-Dimethylpropane [Propane, 2,2-dimethyl-]	463-82-1	10,000	f
Ethane	74-84-0	10,000	f
Ethyl acetylene [1-Butyne]	107-00-6	10,000	f
Ethylamine [Ethanamine]	75-04-7	10,000	f
Ethyl chloride [Ethane, chloro-]	75-00-3	10,000	f
Ethylene [Ethene]	74-85-1	10,000	f
Ethyl ether [Ethane, 1,1'-oxybis-]	60-29-7	10,000	g
Ethyl mercaptan [Ethanethiol]	75-08-1	10,000	g
Ethyl nitrite [Nitrous acid, ethyl ester]	109-95-5	10,000	f
Hydrogen	1333-74-0	10,000	f
Isobutane [Propane, 2-methyl]	75-28-5	10,000	f
Isopentane [Butane, 2-methyl-]	78-78-4	10,000	g
Isoprene [1,3-Butadinene, 2-methyl-]	78-79-5	10,000	g
Isopropylamine [2-Propanamine]	75-31-0	10,000	g
Isopropyl chloride [Propane, 2-chloro-]	75-29-6	10,000	g
Methane	74-82-8	10,000	f
Methylamine [Methanamine]	74-89-5	10,000	f
3-Methyl-1-butene	563-45-1	10,000	f
2-Methyl-1-butene	563-46-2	10,000	g
Methyl ether [Methane, oxybis-]	115-10-6	10,000	f
Methyl formate [Formic acid, methyl ester]	107-31-3	10,000	g
2-Methylpropene [1-Propene, 2-methyl-]	115-11-7	10,000	f

Federal Regulation 40 CFR 68.130