CYBER SECURITY RISK ANALYSIS FOR PROCESS CONTROL SYSTEMS USING RINGS OF PROTECTION ANALYSIS (ROPA)

by Paul Baybutt
Primatech Inc.
paulb@primatech.com
614-841-9800
www.primatech.com

A version of this paper appeared in Process Safety Progress, p. 284, December, 2004, Vol. 23, No.4.

Abstract

Process plants may be subject to terrorist and criminal acts that can cause harm such as the release or diversion of hazardous materials and process or product damage. Such risks are evaluated using threat and vulnerability analysis and possible improvements in security measures and safeguards are identified. However, recommendations for improvements are usually based on engineering judgment. Such subjective assessments can lead to disagreements, and possibly inappropriate measures to reduce risk. Rings of Protection Analysis (ROPA), a simplified risk assessment method, can be used to provide more rational, objective and reproducible decisions. ROPA parallels Layers of Protection Analysis (LOPA) that is used to evaluate accident risks.

ROPA assists in identifying and determining the adequacy of existing protection systems. It is used to help determine if there are sufficient rings / layers of protection against a threat scenario and if the risk can be tolerated. A scenario may require multiple protection rings / layers depending on the process and the potential severity of the consequences. ROPA helps provide the basis for clear, functional specifications of required protection layers.

This paper describes and demonstrates how ROPA can be applied to cyber security, although it can also be applied to physical security. It considers the selection of security measures and integrates their consideration with other types of protective measures.

Keywords: Cyber security, risk analysis, rings of protection, layers of protection,

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 (Figure 1). Accidents occur when people make errors or mistakes, or equipment fails. Natural events are phenomena such as lightning strikes and flooding,

sometimes called external events. Deliberate acts, called malevents herein, are performed with the intention of causing harm and include terrorism, sabotage, vandalism and theft.

Process plants contain a variety of computer systems. In particular they are used for process control and safety systems operation. Historically, they have been kept separate from business computer systems but increasingly they are being connected through networks driven by the need to communicate process information to business groups. This exposes the systems to access by more people and, more particularly, access through the Internet. Current control systems often have poor security and are vulnerable to cyber attack. Various other computer systems may be also be subject to attack or manipulation including those used for facility access, information storage, logistics, etc.

Risk analysis of accidents involves evaluating hazard scenarios that originate with an initiating event that is an equipment or human failure, or an external event or a combination thereof. Risk analysis of malevents involves evaluating *threat scenarios* (Figure 2). Threat scenarios originate with hostile action to gain access to processes in order to cause harm. The risk of such threats must be assessed to determine if existing security measures and safeguards are adequate or need improvement.

Both security and safety programs typically use *defense in depth* to protect against threats and accidents. This is called *rings of protection* in security and *layers of protection* in safety. Generally, security protection tries to prevent physical and cyber access to a facility while safety protection tries to prevent misoperation of a process that could cause harm. In process safety, the term *safeguards* is usually intended to convey measures to protect against accidents. In process security, various security measures that do not necessarily assist in protecting against accidents are needed to protect against threats. These can be called *secureguards*. Some safeguards may act as secureguards and vice versa. In process security management, safeguards and secureguards must be combined into a program to provide overall protection[1,2].

Layers of Protection Analysis (LOPA) is a simplified risk assessment method[3]. It provides an objective, rational and reproducible method of evaluating accident risk and comparing it with risk tolerance criteria to decide if existing safeguards are adequate, and if additional safeguards are needed. LOPA is often used as an extension of Process Hazard Analysis (PHA). Typically, it is applied after a PHA has been performed. Scenarios are screened for study by LOPA using PHA. LOPA builds on the information developed in the PHA. One application of LOPA is in the determination of the need for safety instrumented systems to assist in compliance with ANSI/ISA S84.01.

Rings of Protection Analysis (ROPA) parallels LOPA. However, it is used to assess the risk of malevents and is usually performed as a follow-on to a security vulnerability analysis (SVA)[4,5]. ROPA is used to analyze individual threat scenarios. It considers

protective measures that are Independent Protection Layers (IPLs), defined as those whose failure is independent of any other failures involved in the scenario.

Cyber Threats to Process Control Systems

Information technology cyber security is an established discipline for commercial and business computer systems, although it has typically focused on the security of information or data stored in a computer so it cannot be read or compromised. Industrial cyber security for control systems is a new discipline.

Industrial cyber security can be defined as the protection of manufacturing and process control computer systems from threats of:

- Cyber or physical attack by adversaries who wish to disable or manipulate them.

- Access by adversaries who want to obtain, corrupt, damage, destroy or prohibit access to valuable information. This is an aspect of information security. Electronic data can be obtained by theft of computer storage media or by hacking into the computer system. Note that a cyber attack may be mounted to obtain sensitive information to plan a a future physical or cyber attack.

Computer systems need to be protected from both hacking and physical attacks. Cyber threats can originate externally, for example, from terrorists and saboteurs, as well as internally from employees, contractors and other insiders who desire to cause harm.

Note that not all cyber events are malicious. They can also be caused by accident. People may make mistakes such as incorrectly entering data, using the wrong data, accessing the incorrect system, mis-programming systems, using conflicting software, etc. These accidental risks should be assessed as part of the process hazard analysis conducted for the control system.

ROPA Applied to Cyber Security

The application of ROPA to cyber malevents parallels the application of LOPA to accidents. It involves the following steps:

1) Select cyber threat scenarios

2) Identify initiating events, their frequencies, and enabling events / conditions

3) Identify existing protective measures and their failure probabilities

4) Estimate scenario risk

5) Risk decision making

6) Recommendations for corrective actions.

Typically, a worksheet is used to perform a ROPA (see Figures 3, 4 and 5). One should be completed for each threat scenario considered.

Step 1. Select Cyber Threat Scenarios

High risk accident scenarios are usually selected from a PHA for study using LOPA. Similarly, in ROPA, threat scenarios can be selected from a physical security vulnerability analysis (SVA)[4,5] or a cyber SVA [6,7]. Examples of cyber threat scenarios for a facility identified using SVA are shown in Figure 6.

Three threat scenarios are shown. All involve the misuse of the computer process control system to release hazardous material from a tank. The first scenario involves hacking into the system by an outside attacker such as a terrorist. The second scenario is a physical attack on the computer control system to gain access to it in order to cause a release. In the third scenario an employee uses the computer control system to cause a release.

Step 2. Identify Initiating Events, Their Frequencies, and Enabling Events / Conditions

For a cyber threat scenario, the initiating event is a deliberate hostile action against a facility. Enabling events or conditions do not directly cause the scenario but they must be present or active for the scenario to proceed. They may influence the likelihood of hostile action. Examples for cyber security are:

- Omitting to install a software patch
- Lack of password protection
- Unattended operation

The likelihoods of these factors are used to adjust the frequency of the initiating event in ROPA.

One of the challenges in applying ROPA is developing initiating events frequencies. Data on cyber attacks are sparse. Frequencies are obtained using expert opinion or by combining expert opinion with the sparse data. When the initiating events can be broken down into constituent elements, it is possible to synthesize their frequencies using techniques such as fault tree analysis. There are uncertainties in the analysis but this is true of all risk analyses. However, risk analysis makes the uncertainties explicit so they can be considered in decision making and the robustness of decisions to uncertainties determined.

Initiating events and estimated frequencies for the three scenarios are provided in Table 1.

Step 3. Identify Existing Protective Measures and Their Failure Probabilities

Typically, safeguards against accident scenarios are identified in PHA. In process safety, typical layers of protection considered are:

- Process design
- Basic process control system
- Critical alarms and human intervention
- Safety instrumented systems
- Physical protection such as relief devices
- Post-release physical protection
- Plant emergency response
- Community emergency response

These protection layers may help safeguard against malevents but their adequacy for that purpose must be assessed, and secureguards are also needed.

Typical cyber security measures include:

- Passwords
- User identification and authentication
- Firewalls
- Encryption
- Malware protection
- Separation of functions
- Intrusion detection

Typical physical security measures for computer systems include:

- Access control
- Hardening
- Vehicle barriers
- Buffer zones
- Intrusion detection

Physical protection should be provided for critical computer rooms, server rooms, control rooms, motor control centers, rack rooms, telecommunications rooms, etc.; for example, using fire and blast resistant construction and access controls. Utilities supporting computer systems should also be included.

A key aspect of LOPA is establishing the independence, effectiveness and verification of safeguards for consideration as IPLs[3]. Similarly, some secureguards and safeguards

against malevents will qualify as independent protection layers or rings in ROPA. However, the criteria pose some challenges when analyzing threat scenarios since the functioning of some of these protection measures may be deliberately disabled as part of an attack. Consequently, probabilities of failure on demand (PFD's) for secureguards and safeguards that protect against malevents must reflect failure to perform due not only to normal degradation mechanisms but also to disablement by attackers. The likelihood of disablement will depend on how much information attackers have about the protective systems and how obvious they are from inspection. Individual safeguards or secureguards may not be capable of terminating the scenario. Several may be required to operate successfully in combination to stop an attack.

For all three example scenarios, the gas detectors and dike are protective (Figures 3, 4, 5). The plant fence and the presence of operators in the control room act as protective measures for the second and third scenarios, respectively. The gas detectors would probably not be credited as an IPL since it is assumed they would be disabled by the attacker(s). The dike could be claimed as an IPL and is assigned a PFD of 1×10^{-2} taken from the literature. Neither the plant fence nor the presence of another operator would be claimed as IPLs. In the case of a plant fence, it would not stop a determined attacker. For an operator who wishes to sabotage a facility, chances are they would be able to find or arrange an opportunity to misuse the control system without observation by others.

Step 4. Estimate Scenario Risk

ROPA estimates the risk of a scenario by estimating the scenario consequence and the scenario likelihood based on the likelihoods of the constituent elements of the scenario. The following elements of threat scenarios must be considered:

- Hostile action (initiating event)
- Secureguards against cyber attack (intermediate events)
- Safeguards against cyber attack (intermediate events)
- Enabling events or conditions
- Consequence

The consequence is the effect of the scenario on people (on-site or off-site), property (on-site or off-site), the process (downtime, product quality, etc.), the environment, etc.

Data for risk estimates of the three scenarios are shown in Figures 3, 4 and 5. The scenario frequencies are provided numerically and the consequences as categories. A level 4 consequence represents mass fatalities while a level 3 consequence represents serious injuries.

Step 5. Risk Decision Making

Calculated risk is now compared with risk tolerance criteria. If the calculated risk is less than the risk criterion, the scenario is judged to have sufficiently low risk, or sufficient protection, so that no further protection is needed. If the calculated risk exceeds the risk criterion, the scenario is judged to require additional, or stronger, protection, or design changes are needed to make the process more secure. Risk criteria may take various forms[3]. They can be purely qualitative, quantitative or a combination thereof. The form selected must match the form in which the risk estimates are expressed.

Risk tolerance criteria used in the examples are provided in Figures 3, 4 and 5. The frequencies specified are an order of magnitude lower than would typically be used for risk from accidents[3]. This provides a measure of conservatism in the analysis to help account for the uncertainties in the data.

Step 6. Recommendations for Corrective Actions

Strategies for reaching a tolerable risk level can now be devised. Further risk reduction measures are considered based on their ability to reduce risk to the tolerable level (see Table 2). In the case of cyber protection measures, this requires some judgment to decide how much risk reduction is afforded by each measure. However, the risk analysis framework provided by ROPA for making these decisions is as important as the actual data used.

In LOPA, a key part of the analysis involves determining the Safety Integrity Level (SIL) provided by the IPLs involved in the scenario. The SIL is usually defined as a Probability of Failure on Demand (PFD). Security Integrity Levels similar to Safety Integrity Levels can be defined for security measures in ROPA.

In the case of scenario 2, the risk is tolerable. However, the scenario relies only on one IPL, the dike. Additional IPLs should be considered to provide defense in depth, e.g. a hardened control room, or intrusion detection.

The risks for scenarios 1 and 3 are above the tolerable risk level and further risk reduction is required. Options to provide further protection for scenario 1 include a firewall and separation of functions. One option for scenario 3 is to require passwords from two operators for override of set points and safety functions.

Conclusions

ROPA can be applied to all types of cyber security measures. It provides comparable consideration of both safeguards and secureguards and it enables both cyber and physical security to be addressed for cyber threat scenarios. It also allows cyber threat scenarios to be considered together with physical threat scenarios so that resources

can be allocated according to the risk reduction possible considering all types of malevents. ROPA can also be applied to studies of physical security.

References

1. P. Baybutt, *"How Can Process Plants Improve Security?"*, Security Management, Vol. 46, No. 11, p. 152, November, 2002.

2. P. Baybutt, *"Process Security Management Systems: Protecting Plants Against Threats"*, Chemical Engineering, Vol. 110, No. 1, p. 48, January, 2003.

3. *"Layer of Protection Analysis, Simplified Process Risk Assessment"*, AIChE/CCPS, New York, 2001.

4. P. Baybutt, *"Assessing Risks from Threats to Process Plants: Threat and Vulnerability Analysis"*, Process Safety Progress, Vol. 21, No. 4, p. 269, December, 2002.

5. *"Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites"*, AIChE/CCPS, New York, 2002.

6. P. Baybutt, "Cyber Security Vulnerability Analysis: An Asset-Based Approach", Process Safety Progress, Vol. 22. No. 4, p. 220, December 2003.

7. P. Baybutt, "Cyber Security – Are Your Facility Computer Systems Safe From Attack?", Hydrocarbon Processing , Vol. 83, No. 3, p. 49, March 2004.

Figure 1. Extraordinary Events for a Process Plant.

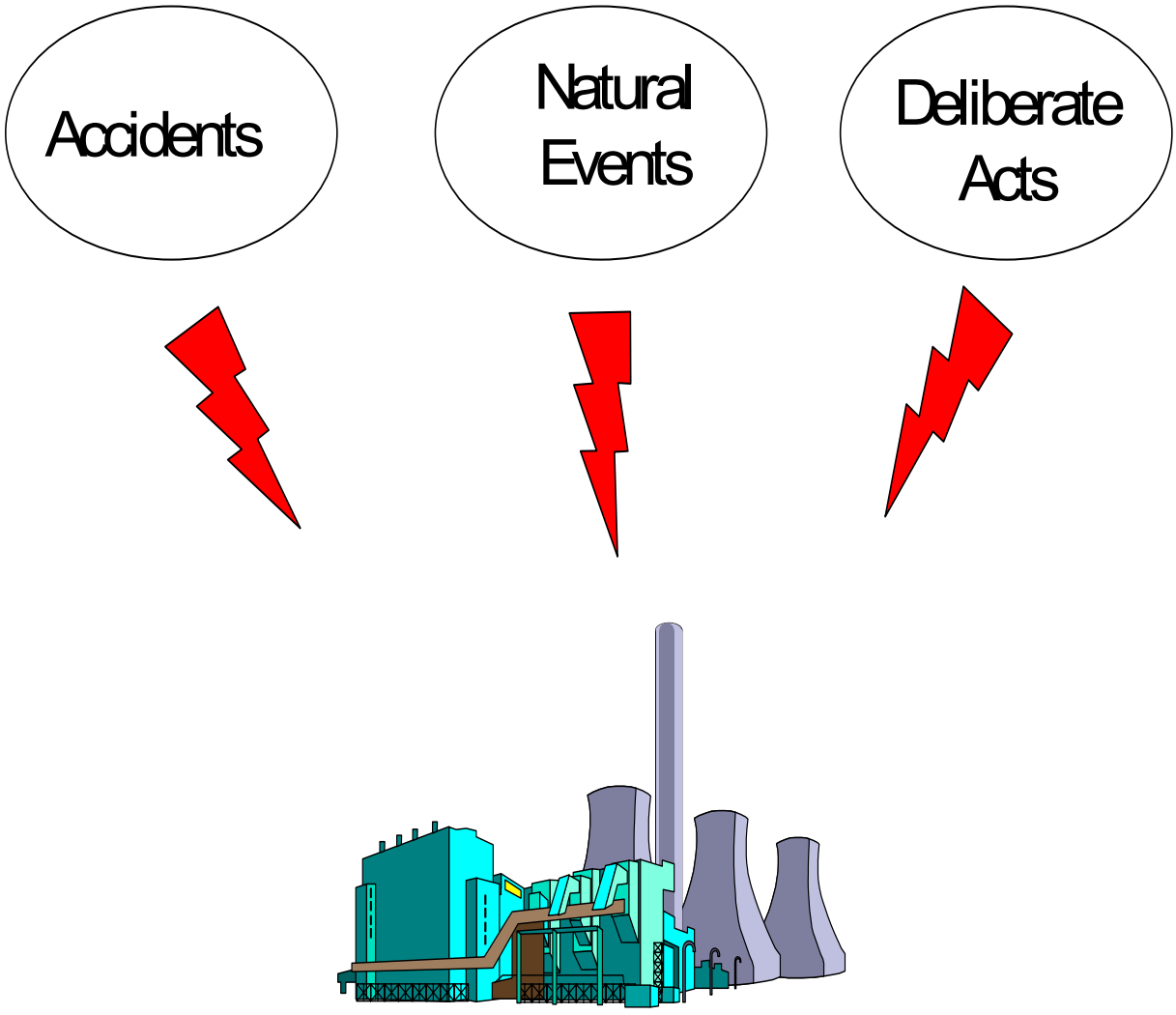

Figure 2. Typical Threat Scenario

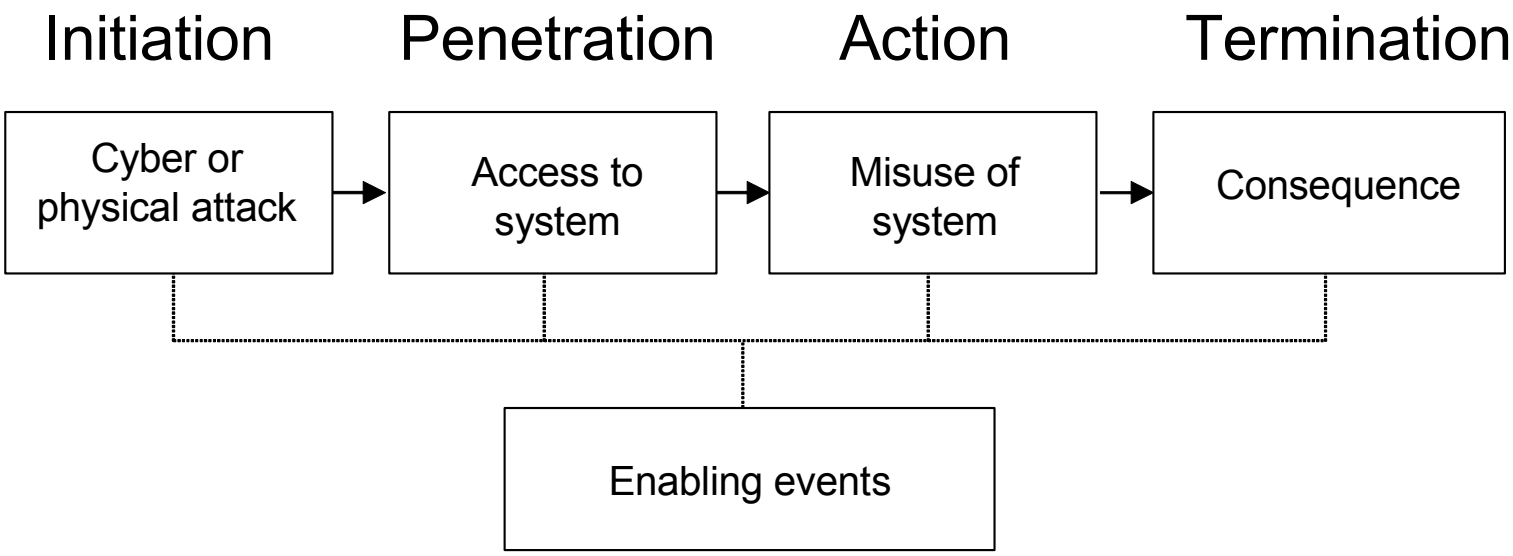

Figure 3. ROPA Worksheet - Example 1

ROPA SUMMARY SHEET

Process: Tank farm		**Date: 1/01/03**	
Scenario Source: Cyber SVA			
Analyst(s): John Major			
Scenario Number: 1	**Scenario Description: Terrorists hack into the computer control system and cause a release from the tank.**	**Equipment ID: TK-101**	
Item	**Description**	**Probability**	**Frequency (per year)**
Consequence	Mass fatalities within the plant and community (level 4)		
Initiating Event	Terrorist hacks into PCN		**1 x 10 (-4)**
Enabling Event or Condition	Unprotected dial-up modem		**1**
Conditional Modifiers (if applicable)			
	Probability of ignition	NA	
	Probability of personnel in affected area	1	
	Probability of injury	1	
	Others	NA	
Frequency of Unmitigated Consequence			**1 x 10 (-4)**
Independent Protection Layers	Dike	**1 x 10 (-2)**	
Safeguards (non-IPLs)	Gas detectors		
Total PFD for all IPLs		**1 x 10 (-2)**	
Frequency of Mitigated Consequece			**1 x 10 (-6)**
Risk Tolerance Criteria:	**1 x 10 (-7) for severity category 4**		
Actions Required: Risk is not tolerable. Reduction of 1 X 10 (-1) is needed.			
Notes:			

Figure 4. ROPA Worksheet - Example 2

ROPA SUMMARY SHEET

Process: Tank farm		**Date: 1/01/03**	
Scenario Source: Cyber SVA			
Analyst(s): John Major			
Scenario Number: 2	**Scenario Description: Terrorists physically attack an unprotected control room and open valves to cause a release.**	**Equipment ID: TK-101**	
Item	**Description**	**Probability**	**Frequency (per year)**
Consequence	Mass fatalities within the plant and community (level 4)		
Initiating Event	Terrorists attack control room		**1 x 10 (-5)**
Enabling Event or Condition	Control room is not secured		**1**
Conditional Modifiers (if applicable)			
	Probability of ignition	NA	
	Probability of personnel in affected area	1	
	Probability of injury	1	
	Others	NA	
Frequency of Unmitigated Consequence			**1 x 10 (-5)**
Independent Protection Layers	Dike	**1 x 10 (-2)**	
Safeguards (non-IPLs)	Plant fence		
	Gas detectors		
Total PFD for all IPLs		**1 x 10 (-2)**	
Frequency of Mitigated Consequece			**1 x 10 (-7)**
Risk Tolerance Criteria:	**1 x 10 (-7) for severity category 4**		
Actions Required: None. Risk is tolerable.			
Notes:			

Figure 5. ROPA Worksheet - Example 3

ROPA SUMMARY SHEET

Process: Tank farm		**Date: 1/01/03**	
Scenario Source: Cyber SVA			
Analyst(s): John Major			
Scenario Number: 3	**Scenario Description: A disgruntled employee uses the control system to cause an overflow of the storage tank.**	**Equipment ID: TK-101**	
Item	**Description**	**Probability**	**Frequency (per year)**
Consequence	Injuries on-site requiring hospitalization (level 3)		
Initiating Event	Emloyee misuses the control system		**1 x 10 (-3)**
Enabling Event or Condition	Free access to control consoles		**1**
Conditional Modifiers (if applicable)			
	Probability of ignition	NA	
	Probability of personnel in affected area	1	
	Probability of injury	1	
	Others	NA	
Frequency of Unmitigated Consequence			**1 x 10 (-3)**
Independent Protection Layers	Dike	**1 x 10 (-2)**	
Safeguards (non-IPLs)	Gas detectors		
	Other operators present in control room		
Total PFD for all IPLs		**1 x 10 (-2)**	
Frequency of Mitigated Consequece			**1 x 10 (-5)**
Risk Tolerance Criteria:	**1 x 10 (-6) for severity category 3**		
Actions Required: Risk is not tolerable. Reduction of 1 X 10 (-1) is needed.			
Notes:			

Figure 6. SVA Worksheet Showing Cyber Threat Scenarios

SECTOR: (1) TANK

THREATS	VULNERABILITIES	CONSEQUENCES	SAFEGUARDS	S	L	R	RECOMMENDATIONS
Hazardous material release by a terrorist	Computer control system can be hacked into to cause a release	Mass fatalities within the plant and the community	Gas detectors Dike	4	1	M	
	Physical attack on computer control center to cause a release	Mass fatalities within the plant and the community	Plant fence Gas detectors Dike	4	2	D	
Hazardous material release by a disgruntled employee	Computer control system can be used to transfer material to a full tank with over-ride of high level trip	Injuries on-site requiring hospitalization	Other operators present in control room Gas detectors Dike	3	2	M	

Table 1. Threat Scenarios and Initiating Event Frequencies.

Scenario	Event	Frequency (per year)
1	A terrorist hacks into the process control system	1×10^{-4}
2	An assailant physically attacks the building containing the process control system to gain access	1×10^{-5}
3	A disgruntled employee uses the computer control system to cause a release	1×10^{-3}

Table 2. Risk Decision Making

Scenario	Risk	Risk Reduction Needed
1	Not tolerable	1×10^{-1}
2	Tolerable	None
3	Not tolerable	1×10^{-1}