U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

JUNE 02

NIJ

Special REPORT

Initial formatted version. Final version forthcoming.

Chemical Facility Vulnerability Assessment Methodology

U.S. Department of Justice
Office of Justice Programs
810 Seventh Street N.W.
Washington, DC 20531

John Ashcroft
Attorney General

Deborah J. Daniels
Assistant Attorney General

Sarah V. Hart
Director, National Institute of Justice

This and other publications and products of the U.S. Department of Justice, Office of Justice Programs and NIJ can be found on the World Wide Web at the following sites:

Office of Justice Programs
http://www.ojp.usdoj.gov

National Institute of Justice
http://www.ojp.usdoj.gov/nij

Chemical Facility Vulnerability Assessment Methodology

NCJ 195171

NIJ

Sarah V. Hart
Director

This study was conducted by Sandia National Laboratories under Interagency Agreement 1997–LB–R–007.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

Foreword

This special report presents a prototype vulnerability assessment methodology developed for chemical facilities to use to identify and assess potential security threats, risks, and vulnerabilities. The National Institute of Justice developed the vulnerability assessment methodology as a practical method to assess the security of chemical facilities within the United States. The vulnerability assessment methodology is designed to guide the chemical facility industry in making security improvements at chemical facilities.

The National Institute of Justice developed the vulnerability assessment methodology in collaboration with the Department of Energy's Sandia National Laboratories. Sandia National Laboratories employees are recognized experts in the areas of security and counterterrorism and have extensive experience in the protection of nuclear weapons and radiological materials. Sandia National Laboratories also has extensive experience in developing vulnerability assessment methodologies for other components of critical infrastructure, including dams, water treatment and supply facilities, and correctional facilities.

During the development, testing, and validation of the assessment methodology, National Institute of Justice and Sandia National Laboratories staff:

- Collected and reviewed extensive information relevant to the threats, risks, and vulnerabilities associated with chemical facilities, including current security practices in the chemical industry.
- Conducted extensive outreach with the field, including meetings and discussions with a range of industry, government, and citizen representatives, as well as private individuals.
- Created a Web site to describe the development effort and solicit comments.
- Inspected chemical facilities.

This vulnerability assessment methodology is therefore focused primarily on terrorist or criminal actions that could have significant national impact (e.g., through the loss of chemicals vital to the national defense or economy) or cause releases of hazardous chemicals that would compromise the integrity of the facility, cause serious injuries or fatalities among facility employees, contaminate adjoining areas, and cause injuries or fatalities among adjoining populations. Thus the use of this vulnerability assessment methodology should be limited to these areas. It addresses primarily physical security at fixed sites and does not address cyber and transportation security issues. Related information on these issues can be found at the National Institute of Justice Web site, http://www.ojp.usdoj.gov/nij.

The National Institute of Justice appreciates the substantial cooperation of chemical industry representatives who provided invaluable access and assistance in the development of this vulnerability assessment methodology. This project also benefited from the suggestions of other Department of Justice components, the Office of Homeland Security, the Department of Energy, the Environmental Protection Agency, the Department of Transportation, numerous organizations, and private citizens. This cooperative effort has produced a useful and reliable methodology for improving the security of our Nation's chemical facilities.

Sarah V. Hart
Director
National Institute of Justice

Overview of the Prototype VAM

The prototype Vulnerability Assessment Model (VAM) (hereafter just “VAM”) developed for this project is a systematic, risk-based approach where 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, L_A, and $L_{AS,}$ where
S — severity of consequences of an event
L_A — likelihood of adversary attack
L_{AS} — 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 increasing the distance from populated areas. Generally, adversary characteristics are outside the control of chemical facilities (CFs), but CFs could take steps to make themselves a less attractive target and perhaps reduce the likelihood of attack of their facilities. Reducing the quantity of hazardous material present may also make a CF less attractive to attack. The most common approach to reducing the likelihood of adversary success, in causing a catastrophic event, is increasing the protection measures against specific adversary attack scenarios.

Since there may be different undesirable events, each with an associated severity of consequence, different potential adversaries, with differing likelihoods of attack, and different attack scenarios, with differing likelihoods of adversary success, it is necessary to determine the risk for each of the different combinations of the risk factors.

While the focus of the use of the VAM is likely to be on CFs that are required to submit risk management plans (RMPs) or a subset of those facilities, the VAM was developed so it is usable for undesired events of lesser consequence than those found in RMPs.

The VAM has 12 basic steps:

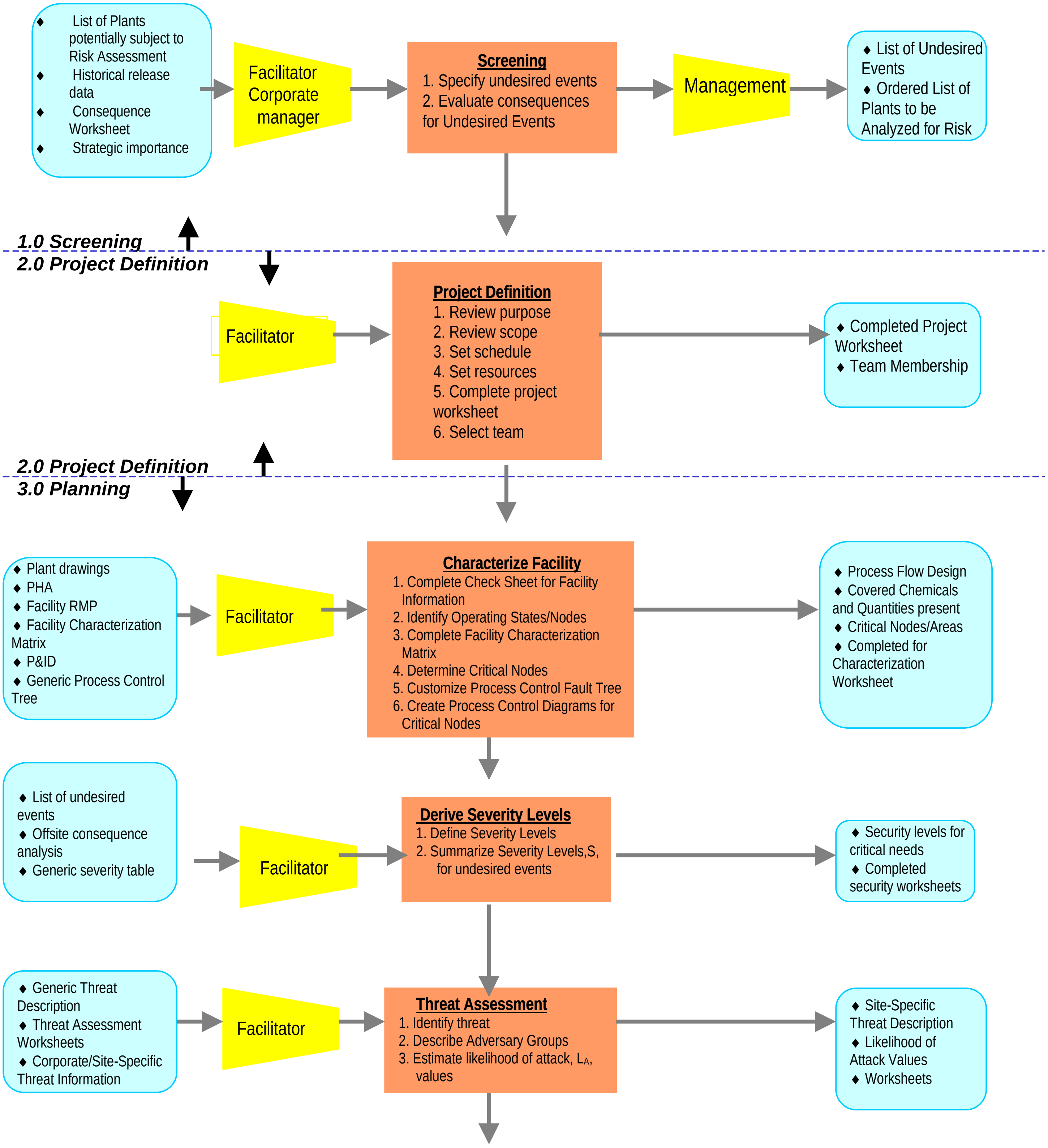
1. screen for need for a vulnerability assessment
2. define the project
3. characterize facility
4. derive severity levels
5. assess threat
6. prioritize cases
7. prepare for analysis
8. survey site
9. analyze system effectiveness
10. analyze risk
11. make recommendations
12. prepare final report

A more detailed discussion of the VAM steps is found in ensuing sections.

VAM Flow Chart

The 12 steps are concisely described in following flow chart (Figure 1), and a detailed explanation of each step follows the chart. The flow chart has been put on three independent pages for ease in copying.

Figure 1: Vulnerability Assessment Methodology for Chemical Facilities Flow Chart



- List of Plants potentially subject to Risk Assessment
- Historical release data
- Consequence Worksheet
- Strategic importance

Screening
1. Specify undesired events
2. Evaluate consequences for Undesired Events

- List of Undesired Events
- Ordered List of Plants to be Analyzed for Risk

1.0 Screening

2.0 Project Definition

Project Definition
1. Review purpose
2. Review scope
3. Set schedule
4. Set resources
5. Complete project worksheet
6. Select team

- Completed Project Worksheet
- Team Membership

2.0 Project Definition

3.0 Planning

- Plant drawings
- PHA
- Facility RMP
- Facility Characterization Matrix
- P&ID
- Generic Process Control Tree

Characterize Facility
1. Complete Check Sheet for Facility Information
2. Identify Operating States/Nodes
3. Complete Facility Characterization Matrix
4. Determine Critical Nodes
5. Customize Process Control Fault Tree
6. Create Process Control Diagrams for Critical Nodes

- Process Flow Design
- Covered Chemicals and Quantities present
- Critical Nodes/Areas
- Completed for Characterization Worksheet

- List of undesired events
- Offsite consequence analysis
- Generic severity table

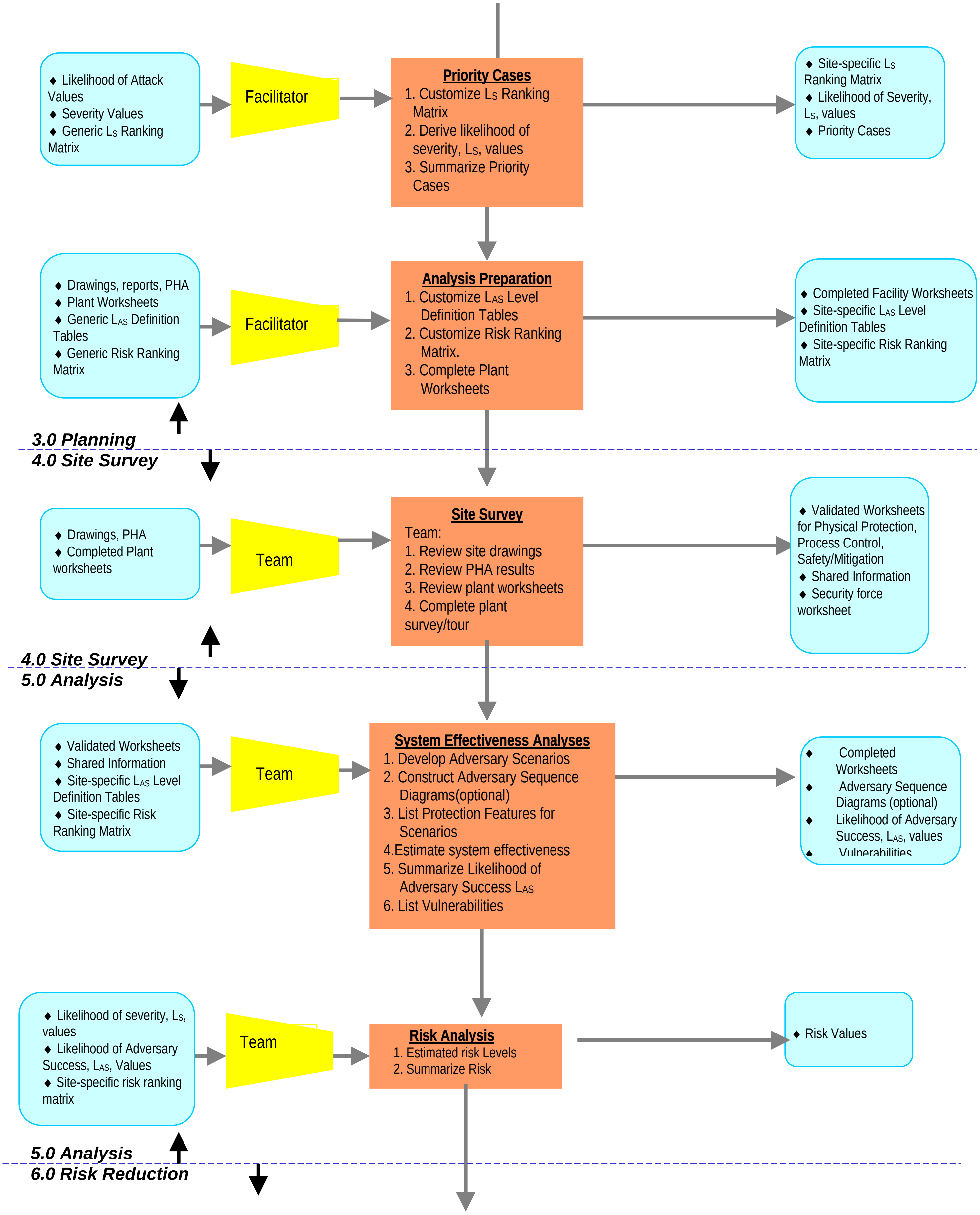
Derive Severity Levels
1. Define Severity Levels
2. Summarize Severity Levels,S, for undesired events

- Security levels for critical needs
- Completed security worksheets

- Generic Threat Description
- Threat Assessment Worksheets
- Corporate/Site-Specific Threat Information

Threat Assessment
1. Identify threat
2. Describe Adversary Groups
3. Estimate likelihood of attack, L_A, values

- Site-Specific Threat Description
- Likelihood of Attack Values
- Worksheets



- Likelihood of Attack Values
- Severity Values
- Generic L_S Ranking Matrix

Facilitator

Priority Cases

1. Customize L_S Ranking Matrix
2. Derive likelihood of severity, L_S, values
3. Summarize Priority Cases

- Site-specific L_S Ranking Matrix
- Likelihood of Severity, L_S, values
- Priority Cases

- Drawings, reports, PHA
- Plant Worksheets
- Generic L_{AS} Definition Tables
- Generic Risk Ranking Matrix

Facilitator

Analysis Preparation

1. Customize L_{AS} Level Definition Tables
2. Customize Risk Ranking Matrix.
3. Complete Plant Worksheets

- Completed Facility Worksheets
- Site-specific L_{AS} Level Definition Tables
- Site-specific Risk Ranking Matrix

3.0 Planning

4.0 Site Survey

- Drawings, PHA
- Completed Plant worksheets

Team

Site Survey

Team:

1. Review site drawings
2. Review PHA results
3. Review plant worksheets
4. Complete plant survey/tour

- Validated Worksheets for Physical Protection, Process Control, Safety/Mitigation
- Shared Information
- Security force worksheet

4.0 Site Survey

5.0 Analysis

- Validated Worksheets
- Shared Information
- Site-specific L_{AS} Level Definition Tables
- Site-specific Risk Ranking Matrix

Team

System Effectiveness Analyses

1. Develop Adversary Scenarios
2. Construct Adversary Sequence Diagrams(optional)
3. List Protection Features for Scenarios
4. Estimate system effectiveness
5. Summarize Likelihood of Adversary Success L_{AS}
6. List Vulnerabilities

- Completed Worksheets
- Adversary Sequence Diagrams (optional)
- Likelihood of Adversary Success, L_{AS}, values
- Vulnerabilities

- Likelihood of severity, L_S, values
- Likelihood of Adversary Success, L_{AS}, Values
- Site-specific risk ranking matrix

Team

Risk Analysis

1. Estimated risk Levels
2. Summarize Risk

- Risk Values

5.0 Analysis

6.0 Risk Reduction

Initial formatted version. Final version forthcoming.

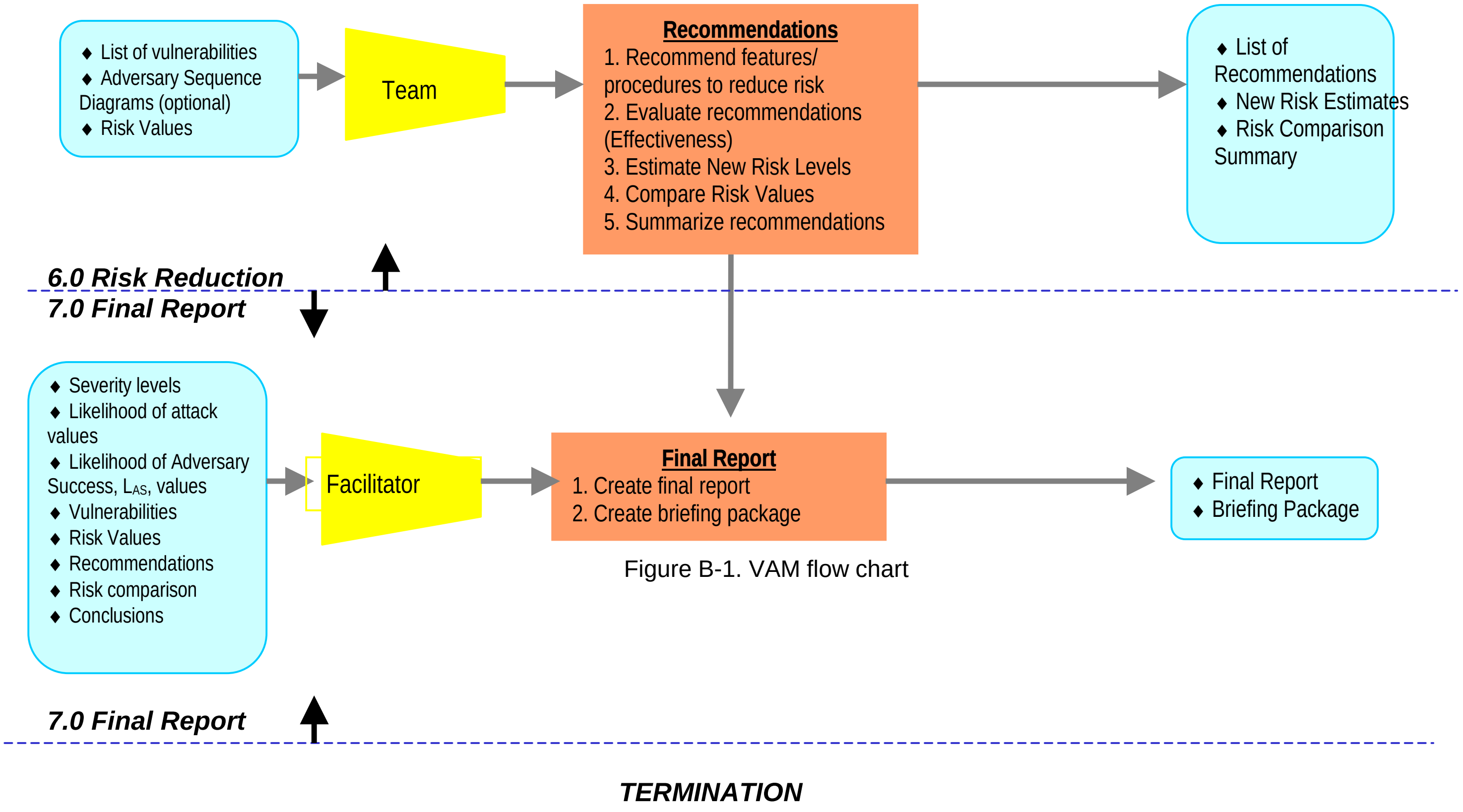

♦ List of vulnerabilities
♦ Adversary Sequence Diagrams (optional)
♦ Risk Values
Team
Recommendations
1. Recommend features/ procedures to reduce risk
2. Evaluate recommendations (Effectiveness)
3. Estimate New Risk Levels
4. Compare Risk Values
5. Summarize recommendations
♦ List of Recommendations
♦ New Risk Estimates
♦ Risk Comparison Summary
6.0 Risk Reduction
7.0 Final Report
♦ Severity levels
♦ Likelihood of attack values
♦ Likelihood of Adversary Success, L_AS, values
♦ Vulnerabilities
♦ Risk Values
♦ Recommendations
♦ Risk comparison
♦ Conclusions
Facilitator
Final Report
1. Create final report
2. Create briefing package
♦ Final Report
♦ Briefing Package
7.0 Final Report
TERMINATION

Figure B-1. VAM flow chart

1. Screening

The purpose of this recommended screening process is twofold:

- for individual CFs, the screening determines if a vulnerability assessment (VA) should be conducted or not.
- for organizations with more than 1 CF, the screening determines which CFs should undergo VAs and then prioritizes among those.

The screening process is based primarily on consequences of potential terrorist incidents at CFs.

The first question in the screening step is what is the desired event? For the information presented below, an off-site release was considered.

The second question, in the screening process step, is whether the loss of a facility would result in a significant national impact (e.g. sole source for a chemical vital to national defense industries). If the answer is YES, then the VA information may need to be classified.

The next question is whether a facility has a total inventory on site of threshold quantities (TQs) or greater of a covered chemical under 40 CFR 69.130. If the answer is NO, then a VA is unlikely to be needed to help protect against unacceptable off-site consequences (CFs may still decide to do a VA for other reasons). For companies with more than one CF, the screening process should proceed to their other CFs. If the answer is YES, further screening is done based on the estimated number of people affected by the worst-case scenario for the RMP as shown below in Figure 2.

What is the estimated number of people affected by the Worst-Case Scenario from the RMP for toxic substances?

Assign Levels:

1	for more than 100,000
2	for 10,000–100,000
3	for 1,000–9,999
4	less than 1,000

Figure 2: Further Screening Based on the Estimated People Affected by Worst-Case Scenario

Other factors considered in the screening step include consideration of accessibility, recognizability, importance, and history/symbolism.

The final screening step is to prioritize the CFs needing VAs beginning with the facilities assigned a level 1 and proceeding to those at levels 2, 3 and 4.

2. Project Definition

For CFs, which have been screened and selected for a VA, the next step is to define the VA as a project specific to each CF. Management needs to assign a facilitator, who is trained in the VAM, to be responsible for the project definition. Defining the project includes reviewing the purpose of the work to be performed, tasks to be accomplished, resources to be allocated, a schedule and a team to accomplish the work. The team may be the same team that prepared the Process Hazards Analysis (PHA) for the facility with the addition of one or more CF employees with security responsibilities. The project definition should be documented in a written statement that may be amended as the VA progresses.

3. Characterize Facility

An early step in security system analysis is to characterize the facility operating states and conditions. This step requires developing a thorough description of the facility itself (location of the site boundary, building locations, floor plans, and access points). Also required are a description of the processes within the facility and the identification of any existing physical protection features. This information can be obtained from several sources, including facility design blueprints, process descriptions, process hazard analysis (PHA) report, facility risk management plan (RMP), piping and instrument drawing (P&ID), and site surveys.

Characterize Facility Infrastructure and Processes

The characterization of a facility includes a description of building structures, traffic areas, infrastructure, terrain, weather conditions, historical data, and operational states. When characterizing the facility, the first step is to gather information that will be helpful in identifying potential security vulnerabilities. The types of documentation include:

Policy and procedure documents:

- unusual occurrence reports
- existing threat assessment information
- results from past security survey/audits
- building blueprints and plans for future structures
- site plans of detection, delay, assessment systems
- operational procedures

Once the documentation has been collected, the following information should be extracted to characterize the facility. Site plans can help identify:

- property borders
- ingress/egress routes to the facility
    - specific vulnerable areas in and around the facility, including routes outside the areas, such as adjacent buildings, that could be used by a sniper to target the building
    - adjacent parking lots and related security countermeasures
    - building locations and characteristics (purpose of the building, who is allowed access, and operational conditions or states)
    - existing physical protection features
- access to process control system
    - list of authorized users
    - access modes
    - protection features of system

Operational conditions are described by:

- length and number of day and night shifts
- activities typical to each shift and the associated security implications
- number of employees/contractors, unions, visitors in the area during each state and the level of access to the facility during weekdays, weekends, and holidays
- availability of security forces, to include local law enforcement
- meteorological conditions for the region and time of the year
- description of adjacent residential or commercial areas
- batch versus continuous chemical processes

Facility structure information that is needed to characterize the facility includes type of materials used in construction and the location and type of doors, gates, entryways, utilities, windows, and emergency exits.

Procedural information that must be obtained includes:

- entry control procedures to the facility for visitors, deliveries, contractors, and vendors
- emergency operations procedures for evacuation
- entry control procedures
- procedures used to evacuate facility personnel in the event an incident occurs
- security procedures
- policies related to alarm assessment and communication to responding security personnel or local law enforcement.
- safety procedures and features
- process control procedures and features

The overall mission and operations conducted at the facility must be clearly understood. In order to determine how the mission can be interrupted, it is necessary to understand what is required for the site to operate effectively. The operation and location of equipment and features that are important to the facility mission must be documented.

Determine List of Reportable Chemicals for Undesired Events

A list of reportable chemicals can be obtained from the PHA report. The processes for the reportable chemicals that pertain to the undesired events will be studied in detail.

Facility Characterization Matrix

A Facility Characterization Matrix was developed to help organize the security factors for each processing node and to provide a framework for determining the critical nodes and prioritizing them. Table 1 is the Facility Characterization Matrix.

No.	**Parameter**	**Node 1**	**Node 2**	**Node 3**	**Node 4**	**Node 5**	**Node 6**	**Node 7**	**Node 8**	**Node 9**	**Node 10**
1	Process Activity										
2	Covered chemicals										
3	Quantity of covered chemicals										
4	Process duration										
75	Criticality rating (sum for node)										

(1) Process Activity. A few words to describe the activity (i.e., from flow diagram, PI&D, reactor, pipe, storage tank, transportation).

(2) Covered chemical. Enter Y and the chemical if it is listed in 40 CFR 68.130 or 29 CFR 1910.119. Enter N and the chemical if not listed. Enter name for all chemicals at this node.

(3) Quantity of covered chemical. Enter 1 if quantity is >25 times the threshold quantity (TQ); 2 if the quantity is between 10 and 25 times TQ; 3 if the quantity is between 1 and 10 times TQ; 4 if the quantity is TQ.

(4) Process duration. Enter 1 if the process duration is 100% continuous; 2 if the process duration is between 50 and 99% continuous; 3 if the duration is between 25 and 49% continuous; 4 if the process is <25% of the time.

(5) Recognizability. Enter 1 if target and importance are clearly recognizable and little or no prior knowledge is required; 2 if target and importance are easily recognizable and requires small amount of prior knowledge; 3 if target and importance are fairly difficult to recognize and some prior knowledge is required; 4 if target and importance are very difficult to recognize and require extensive knowledge for recognition.

(6) Accessibility. Enter 1 for easily accessible; 2 for fairly accessible, target located outside or in unsecured area; 3 if moderately accessible, target located inside a building or enclosure, 4 if not accessible or only accessible with extreme difficulty.

Determine Critical Node(s): _______________________

The critical node is node or nodes with the lowest score for (57)

Table 1. Facility Characterization Matrix

Process Flow Diagram

A process flow diagram must be created for each reportable chemical that can be exploited to cause an undesired event. This type of diagram might already exist, however, as it might have been used in the Process Hazards Analysis (PHA) analysis to determine the critical nodes of operation. If so, it can be used for the vulnerability assessment (VA) as well.

Figure 3 provides an example Process Flow Diagram. The operational steps are divided into operation nodes; the operation nodes for each chemical must be reviewed against a set of security-related factors. These factors must be considered during all of the following states of operations: when the chemical is incoming, temporarily staged or stored; while in process, temporarily staged or stored awaiting shipment; and, when the chemical is being shipped out. A security hazard possibility may not exist during all operating nodes. As an example, a hazardous chemical that has already been converted to a nonhazardous material would not be a security hazard during an operating node. One way to determine which nodes provide a potential for the undesired event to occur (i.e., critical nodes) is to assess the attributes of each operational node. The factors that determine which nodes are critical are: what process activity is underway, the specific chemical, the quantity/form/concentration of the chemical, the potential for offsite release, and the accessibility and recognizability of the chemical. Figure 4 generically describes the operating nodes to be analyzed.

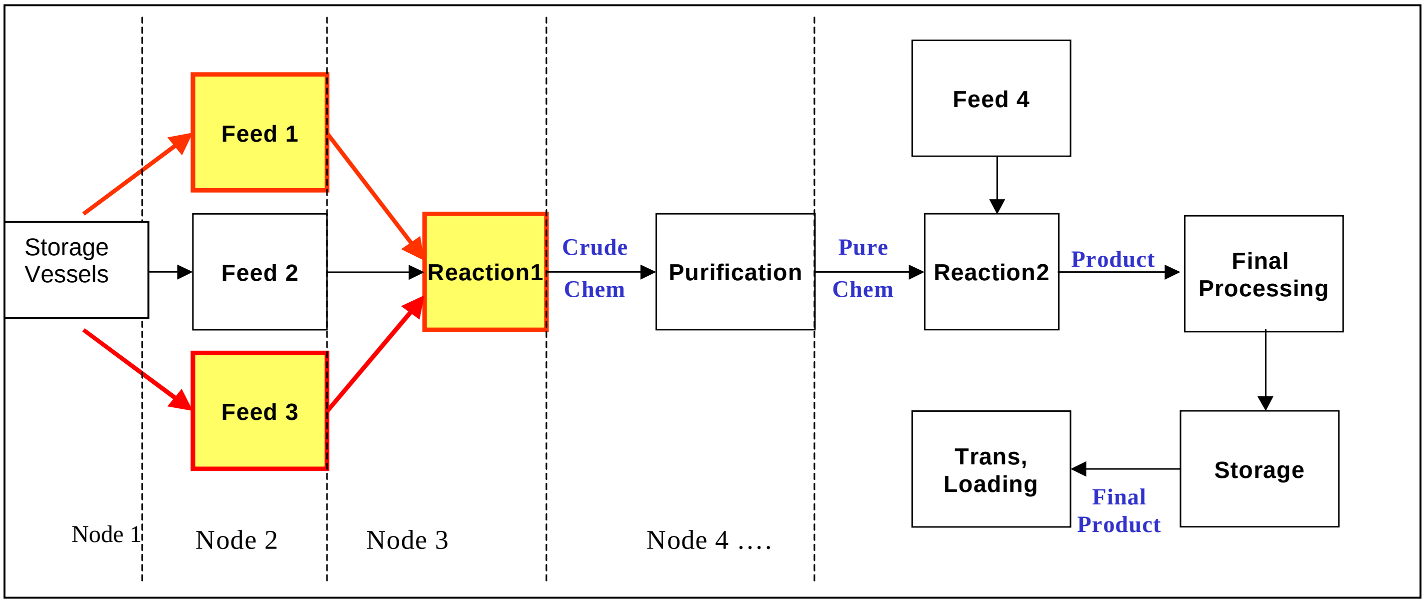


Figure 3. Example Process Flow Diagram

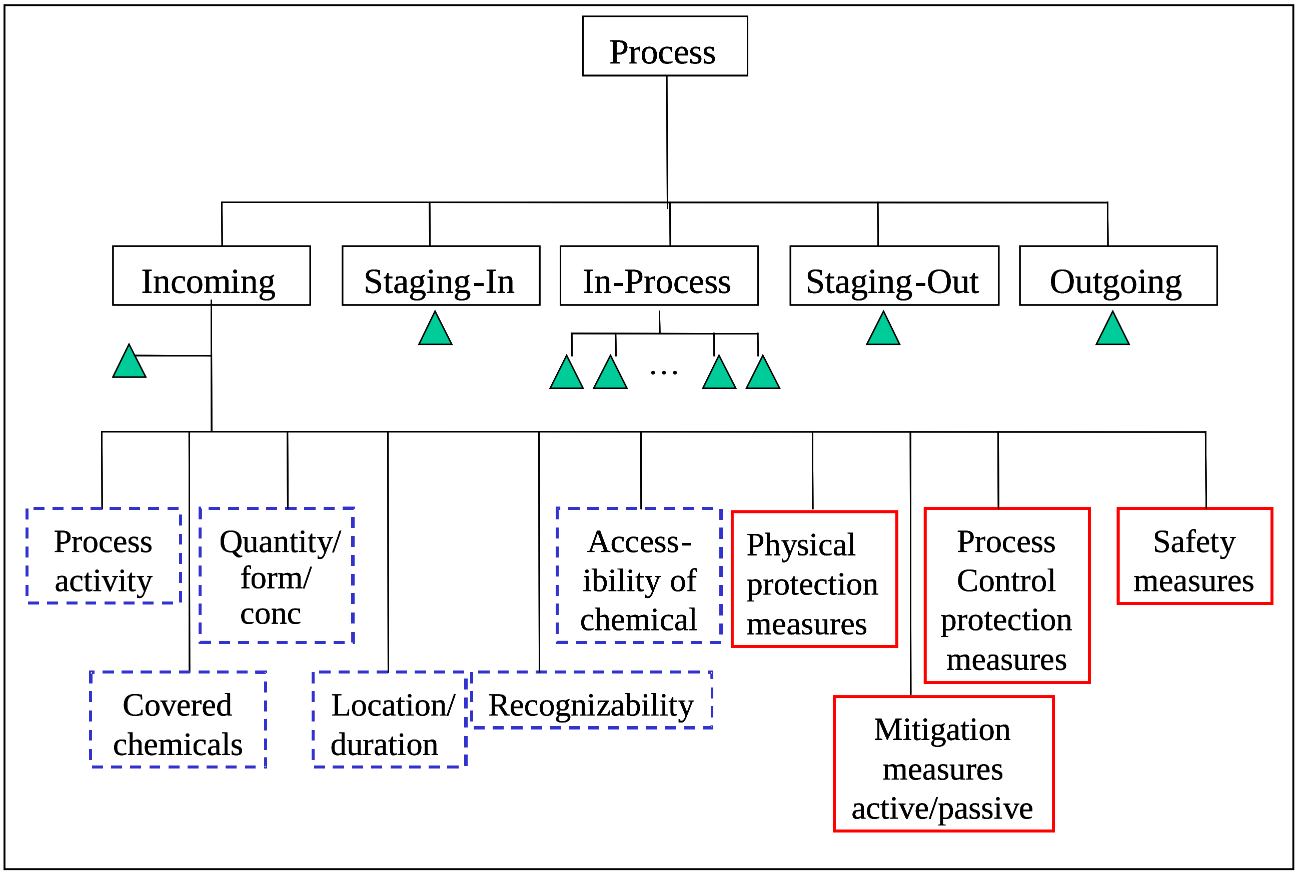


Figure 4. Operating Step Characterization

Process Control Flow Diagram

An additional flow diagram may be developed for the process control system for each critical node. A generic control process flow diagram is provided in Figure 5. A generic process control is normally a closed cycle in which a sensor provides information to a process control software application through a communications system. Simplistically, the application determines if the sensor information is within the predetermined (or calculated) data parameters/constraints. The results of this comparison are fed to an actuator, which controls the critical component. This feedback may electronically control the component or may provide an indication for a manual action. This closed-cycle process has many checks and balances to ensure that it maintains a safe process. The investigation of how the process control can be subverted is very likely to be extensive because it is possible that part or all of the process control could be verbal instructions to an individual monitoring the process. It may also be fully computer controlled and automated, or may be a hybrid where only the sensor is automated and the action is a manual intervention. Further, some legacy control process systems may use prior generations of hardware and software while other process control systems are state-of-the-art.

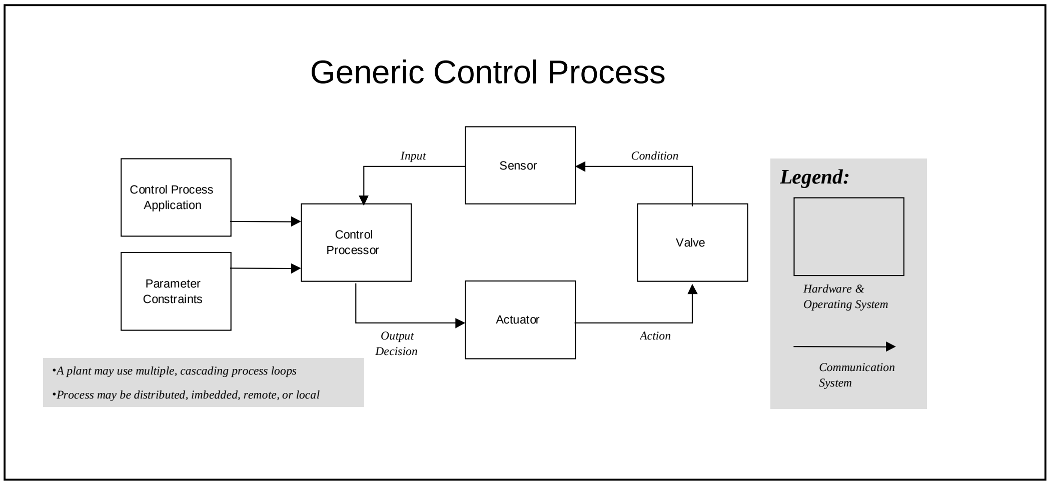

Generic Control Process
Input
Sensor
Condition
Control Process Application
Control Processor
Valve
Parameter Constraints
Actuator
Output Decision
Action
•A plant may use multiple, cascading process loops
•Process may be distributed, imbedded, remote, or local
Legend:
Hardware & Operating System
Communication System

Figure 5. Generic control process

Customize Process Control Fault Tree

The creation of a process control fault tree is highly recommended because it will help the team understand the process control system of the plant and will help the team develop scenarios in the system effectiveness analysis section of the methodology.

The facilitator and/or the process control manager should be responsible for creating the tree.

4. Derive Severity Levels

The severity of consequences for each undesired event must be derived. The severity table created for the PHA should be considered first. The severity of consequences from the PHA may need to be modified in light of a malevolent (rather than an accidental) event causing the consequences. Another source of severity of consequences is the results from the worst-case scenario and alternative-release scenario offsite-consequences analysis results. (Those results may also need to be modified.)

Table 2 provides example definitions of severity levels. For CFs which have to submit RMPs, they most likely will have a severity level 1. The example definitions below are likely most useful to CFs, which do not have to submit RMPs, which have decided to perform a VA. This table should be made site-specific because different 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.

	Severity Level
1	Potential for any of the following resulting from a chemical release, a detonation, or an explosion: worker fatality(ies) public fatality(ies) extensive property damage, disable facility for more than a month, major environmental impacts, or evacuation of neighbors
2	Potential for any of the following resulting from a fire or major release: nonfatal injuries, disabled unit for less than one month, shut down of road or river traffic
3	Potential for any of the following resulting from a release event: unit evacuation, minor injuries, or minor off-site impact (i.e., odor)
4	An operational problem that does not have potential to cause injury or a reportable release with no off-site impact

Table 2. Severity Level Definition Table

5. Threat Assessment

Threat —Before a vulnerability assessment can be completed, a description of the threat is required. This description includes the type of adversary, tactics, and capabilities (number in the group, weapons, equipment, and transportation mode) associated with each threat. Also, information about the threat is needed to estimate the4 likelihood that the adversaries might attempt an attack.

Defining the Threat— A threat description specific for a site must be defined. 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 regularly update a site's threat analysis, including when obvious changes in threat occur.

Information Needed to Define Threat

Although having accurate knowledge about the threat(s) is the goal of defining the threat, realistically that goal is very unlikely to be met. Therefore, judgments will have to be made in defining the threat, and the more complete the collection of available threat information is, the better the judgments are likely to be. The written definition of the threat(s) is called the design basis threat (DBT).

The type of information that is needed to describe a threat includes:

- type of adversary
- potential actions of the adversary
- motivations of the adversary
- capabilities of the adversary

Adversaries are generally divided into three types: outsiders, insiders, and outsiders in collusion with insiders. Outsiders might include terrorists, criminals, extremists, gangs, or vandals. Insiders might include hostile employees; employees forced into cooperating with a criminal by blackmail or threats of violence to them or their families; a psychotic; or possibly an employee who is a criminal.

A discussion of the potential actions of the adversary includes what sorts of crimes these various adversaries are interested in and capable of carrying out and which of these crimes are of concern to the specific site. Examples would be theft, destruction, violence, or bombing.

Knowing the possible motivation of the adversary can provide valuable information. Motivations that might prompt potential adversaries to undertake criminal actions can be grouped into three broad categories: ideological, economic, and personal. Ideological motivations are those linked to a political or philosophical system. They would include those of political terrorists, extremists, and radical environmentalists. Economic motivations obviously would involve a desire for financial gain. Criminals generally view theft for ransom, sale, or extortion purposes. Personal motivations pertain to the special situations of specific individuals. Personal reasons for committing a crime could range from those of the hostile employee with a grievance against an employer or coworker to those of the psychotic individual.

The capability of the potential adversary is an important concern to the designer of a physical protection system. The number of attackers to be defended against has always been a question of important concern, but it is also valuable to know how the adversary might be armed. The adversary may have weapons and explosives of different kinds. Other factors that describe adversary capabilities include a description of the adversary’s tools and equipment, their means of transportation (truck, helicopter, ultralight, radio-controlled vehicle), extent of technical skills and experience, how much information gathering they do, and whether they might have insider assistance.

Information Collection

The types of organizations that may be contacted during the development of a DBT include local, state, and federal law enforcement (to include searching source material), and related intelligence agencies. Local authorities should be able to provide reports on the type of criminal activities that are occurring and analytical projections of future activities. As an example, a special interest group may have previously only demonstrated at a facility, but recently may have announced plans to commit acts of sabotage that would disrupt normal operations.

A review should be conducted for past incident reports associated with the site, from local periodicals, professional journals, the Internet, and from other related material.

Employee data should also be reviewed because employees may present an insider threat. The review should include the following:

- the number of personnel at the facility and types of positions
- employee numbers versus the number of contractors, visitors, and vendors
- any problems that may have occurred with either direct or contract employees (e.g., domestic violence problems, union disputes, downsizing)

An example of the result of the information collection is shown in Table 3. This threat information is used later to develop adversary scenarios and to estimate protection system effectiveness.

Type of Adversary	Number	Equipment	Vehicles	Weapons	Tactics
Terrorist Outsider (May include an insider colluding)	2–3	Hand and power tools, body armor, chem/bio	4x4, ATV, pickup, aircraft	Handguns, automatics, explosives	Cause catastrophic event, theft
Criminal	2–3	Hand tools, body armor	Foot, truck, aircraft	Handgun, explosives	Extortion, theft
Extremists	5–10	Signs, chains, locks, hand tools	Car, bus	No weapons	Protest, civil disobedience, damage/ destruction
Insider	Single	Onsite equipment	Car, pickup, 4x4	Handguns, automatics, explosives	Destruction, violence, theft
Vandal	1–3	Paint	Car, pickup	Hunting rifle	Random shooting, tagging

Table 3. Example Site-specific Threat Description

Likelihood of Attack, L_A —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. The Department of Defense (DoD) standard definitions [Henry Shelton 1998] were modified for use in categorizing the threats against CFs. The modified standard definitions are shown in Table 4.

	Likelihood of Attack
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, history or targeting of the facility.
4	Threat exists, but not capable of causing undesired event.

Table 4. Example Level of Likelihood of Attack, L_A, Definition Table

6. Priority Cases

After severity levels have been determined for each undesired event and likelihood of attack levels have been determined for each adversary group for each undesired event, the values are used to derive the L_S values. These values are obtained from a ranking matrix of likelihood of attack, L_A, versus severity, S, for each undesired event/adversary group. The facilitator should develop the likelihood and severity, L_S, ranking matrix. An example of a matrix is provided in Table 5. Using this table, for example, if an adversary group has a level 2 likelihood of attack for a specific undesired event, and that undesired event has a severity level of 3, the likelihood and severity level, L_S, would be given a value of level 3. Priority cases would be those undesired event/adversary group pairs with a likelihood and severity, L_S, value less than 4 or some other value chosen by a CF. These cases are the priority cases which should be analyzed further for protection system effectiveness.

L_S	**S**				
L_A		1	2	3	4
	1	1	1	2	4
	2	1	2	3	4
	3	2	3	4	4
	4	3	4	4	4

Table 5. Example Likelihood and Severity Priority Ranking Matrix

7. Analysis Preparation

To prepare for the site protection system effectiveness analysis, background information should be assembled. This information should include site drawings, the PHA, physical protection system (PPS) features, and process control information. Information worksheets have been developed to provide a systematic means to collect site information needed for the effectiveness analysis and for later use in documentation.

Physical Protection System

An effective security system must be able to detect the adversary and delay the adversary long enough for a response force to arrive and neutralize the adversary before the mission is accomplished. In particular, an effective protection system provides effective:

- detection
- delay
- response

These security system functions (detection, delay, and response) must be integrated to ensure that the adversary threat is neutralized before the mission is accomplished.

DETECTION, the first required function of a protection system, is the discovery of adversary action and includes sensing covert or overt actions. In order to discover an adversary action, the following events must occur:

- sensor (equipment or personnel) reacts to an abnormal occurrence and initiates an alarm
- information from the sensor and assessment subsystems is reported and displayed
- someone assesses information and determines the alarm to be valid or invalid

Methods of detection include a wide range of technologies and personnel. Entry control—a means of allowing entry of authorized personnel and detecting the attempted entry of unauthorized personnel and contraband—part of the detection function of physical protection. Entry control works best when entry control through several layers of protection, which surround targets of malevolent attacks, is required. Entry control to various layers of the system should be designed to filter and reduce the population that has access as they approach targets. Only those individuals who need direct access to the target should be allowed through the final entry control point. Searching for metal (possible weapons or tools) and explosives (possible bombs or breaching charges) is required for high-security areas. This may be accomplished using metal detectors, x-ray (for packages), and explosive detectors. Security personnel also can accomplish detection. Security personnel at fixed posts or on patrol may serve a vital role in detecting an intrusion. Other personnel can contribute to detection if they are trained in security concerns and have a means to alert the security force in the event of a problem.

An effective detection alarm assessment system provides two types of information associated with detection: 1) information about whether the alarm is a valid alarm or a nuisance alarm, and 2) details about the cause of the alarm. The effectiveness of the detection function is measured both by the probability of sensing adversary action and the time required for reporting and assessing the alarm.

DELAY, the second required function of a protection system, impedes adversary progress. Delay can be accomplished by fixed or active barriers, (e.g., doors, vaults, locks) or by sensor-activated barriers (e.g., dispensed liquids, foams). Entry control, to the extent it includes locks, may also be considered a delay factor in some cases. The security force can be considered an element of delay if they are in fixed and well-protected positions.

The measure of delay effectiveness is the time required by the adversary (after detection) to bypass each delay element.

RESPONSE, the third requirement of protection systems, comprises actions taken by the security response force (usually on-site security personnel or local law enforcement officers) to prevent adversarial success. Response consists of interruption and neutralization. Interruption is defined as the response force arriving at the appropriate location to stop the adversary's progress. It includes the communication to the response force of accurate information about adversarial actions and the deployment of the response force. The effectiveness measures for response communication are the probability of accurate communication and the time required to communicate with the response force. Neutralization is the act of stopping the adversary before the goal is accomplished. The effectiveness measures for neutralization are security police force equipment, training, tactics, cover capabilities, and engagement effectiveness.

The measure of response effectiveness is the time between receipt of a communication of adversarial actions and the interruption and neutralization of the action.
In addition to the PPS elements described above, an effective PPS has several specific characteristics.

A well designed PPS will include the following:

- protection-in-depth
- minimum consequence of component failure
- balanced protection

Protection-in-Depth

Protection-in-depth means that an adversary should be required to avoid or defeat several protective devices in sequence to accomplish the goal. For example, an adversary might have to penetrate three separate barriers before gaining entry to a process control room. The times required to penetrate each of these barriers may not necessarily be equal, and the effectiveness of each may be quite different, but each will require a separate and distinct act as the adversary moves along the planned path.

Minimum Consequence of Component Failure

It is unlikely that a complex system will ever be developed and operated that does not experience some component failure during its lifetime. Causes of component failure in a PPS are numerous and can range from environmental factors (which may be expected) to adversary actions beyond the scope of the threat used in the system design. Although it is important to know the cause of component failure to restore the system to normal operation, it is more important that contingency plans are provided so the system can continue to operate.

Balanced Protection

Balanced protection implies that no matter how adversaries attempt to accomplish their goals, they will encounter effective elements of the PPS. For a completely balanced system, the minimum time to penetrate each of these barriers would be equal, and the minimum probability of detecting penetration of each of these barriers should be equal. However, complete balance is probably not possible or desirable. There is no advantage to over-designing a PPS.

Additionally, all of the hardware elements of the system must be installed, maintained, and operated properly. Further, the procedures of the PPS must be compatible with the facility procedures. Security, safety, and operational objectives must be accomplished at all times.

Determination of L_{AS}

As discussed above, an effective PPS should be able to prevent an undesired event from occurring (by neutralizing the adversary) with a high degree of confidence. The likelihood of adversary success is the complement of PPS effectiveness. If protection system effectiveness is high, the likelihood of adversary success is low. Conversely, if the PPS effectiveness is low, then the likelihood of adversary success is high. Thus, L_{AS} is derived directly from estimations of the PPS effectiveness. Table 6 provides an example of a definition table for the levels of likelihood of adversary success, L_{AS} based on estimations of PPS effectiveness.

The facilitator should develop a definition table for the levels of likelihood of adversary success for the physical protection system that is specific for the site.

	Likelihood of Adversary Success, L_{AS}
1	Protection system features are nonexistent (catastrophic event expected to occur)
2	Protection system features are judged to provide low level of protection
3	Protection system features are judged to provide medium level of protection
4	Protection system features are judged to provide high level of protection (catastrophic event prevented)

Table 6. Example Definition Table for Likelihood of Adversary Success With Respect to Physical Protection Effectiveness

Protection System for Process Control

Only an overview of the process control systems at CFs was completed in conjunction with the project that developed the prototype CF VAM. Consequently, the protection system analysis for process control systems is quite abbreviated and should not be considered a complete analysis procedure.

An effective protection system for process control protects all of the critical functions of the system and their respective interfaces. These critical functions may include:

- communications
- commercial hardware and software
- application software
- parameter data
- support infrastructure, e.g., power, HVAC

If any one of these functions is not adequately protected, the adversary could exploit that function to use the process control system to cause the undesired event. In the worst-case scenario, the adversary would not even have to come onsite to cause the undesired event to occur. Table 7 provides an example definition table for likelihood of adversary success, LAS, with respect to process control protection. Again, protection system effectiveness is the complement of likelihood of adversary success.

	Likelihood of Adversary Success, L_{AS}
1	Ineffective or no protection features for communications, commercial hardware and software, application software, parameter data, and support infrastructure for the process control system.
2	Some protective measures exist for communications, commercial hardware and software, application software, parameter data, and support infrastructure for the process control system.
3	Major protective measures exist for communications, commercial hardware and software, application software, parameter data, and support infrastructure for the process control system.
4	Significant and complete protective measures exist for communications, commercial hardware and software, application software, parameter data, and support infrastructure for the process control system.

Table 7. Example Definition Table for Likelihood of Adversary Success with Respect to Protection for Process Control

The final step of preparing for the system effectiveness analysis is the establishment of the priority-ranking matrix for likelihood of attack and severity, L_S, and likelihood of adversary success, L_{AS}. The completed matrix will later be used to estimate risk levels. Table 8 provides an example of the priority-ranking matrix, which combines likelihood of attack and severity with likelihood of adversary success.

Risk	$\mathbf{L}_{AS}$				
		1	2	3	4
$\mathbf{L}_S$	1	1	1	2	4
	2	1	2	3	4
	3	2	3	4	4
	4	3	4	4	4

Table 8. Example Risk Priority Ranking Matrix

Mitigation

In the case that the undesired event cannot be prevented by the protection system and system effectiveness is still low, risk might be reduced by mitigation features that reduce consequences, and thus reduce risk. Mitigation features could range from sensors that cause systems to shut down and assume a fail-safe condition if a problem is detected to early warning systems to alert first responders**.** Mitigation measures may be disabled by adversaries.

8. 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 step that follows. A walk-through survey of the site should be completed with special emphasis on verifying critical process node and target information.

9. System Effectiveness Analyses

Estimating system effectiveness means judging whether the protection features of the facility are adequate to prevent the undesired event from occurring. For each critical node, two or more estimates of protection system effectiveness will be made: one or more for the physical protection system, and one for the protection system for process control. For the physical protection system, the first estimate will be estimating the effectiveness of the system to prevent the undesired event. If the undesired event cannot be prevented, another estimate will be made for the effectiveness of the system to detect and reduce or mitigate the consequences of the undesired event so that the event is not catastrophic.

For each undesired event/adversary group, the steps for estimating physical protection system effectiveness are:

1. specifying the most vulnerable adversary scenario—a physical path
2. listing the protection features of the facility to protect against the scenario
3. determining a likelihood of adversary success level for the scenario from the definition table for physical protection (Table 6)

For each undesired event/adversary group, the steps for estimating process control protection system are:

1. specifying the most vulnerable adversary scenario—process control path
2. listing the protection features for the process control system against the scenario
3. determining a likelihood of adversary success level for the scenario from the definition table for process control protection (Table 7)

Most Vulnerable Adversary Scenario – Physical Path

Team members will use on-site data and their own knowledge and experience to determine the most vulnerable adversary scenarios. The first step in determining scenarios is to consider adversary strategies. The most vulnerable strategy from the protection system perspective is the adversary strategy of choice to accomplish the undesired event. Team members' opinions—based on knowledge of the site, operations, and the existing protection system features—will determine the selection of the most vulnerable strategy.

Several factors must be considered in determining the most vulnerable strategy:

- protection system weaknesses noted on data collection worksheets and the site survey
    - least-protected system features (detection, delay, response/mitigation)
    - easiest system features to defeat
    - worst consequence results
- facility operating states that the adversary could use to an advantage
    - emergency conditions
    - no personnel on-site
    - inclement weather

After the most vulnerable adversary strategies for each undesired event have been established, adversary paths to the critical assets to cause the undesired event are considered. For the physical paths, site layout drawings may help summarize all of the possible adversary paths from offsite the facility into the critical assets. Figure 6 illustrates an example layout drawing showing possible adversary paths.

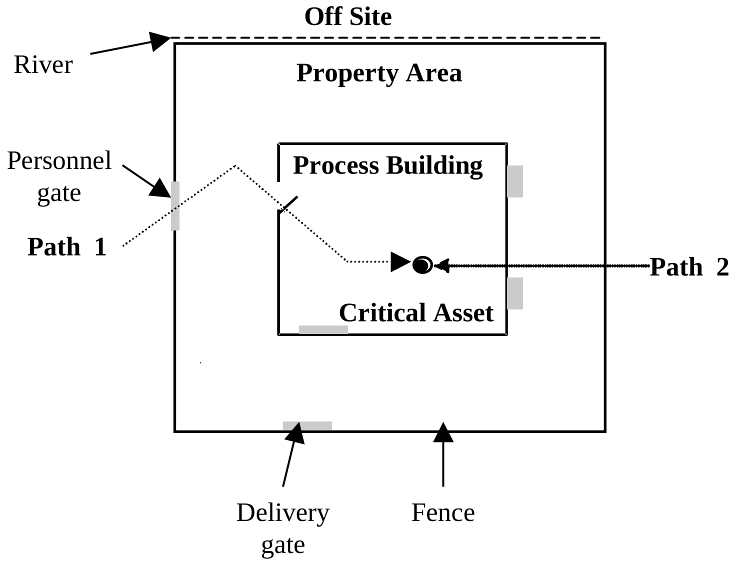


Figure 6. Example adversary paths

The adversary sequence diagram (ASD), which models the physical protection system at a facility, is another way to consider all of the physical adversary paths into a facility. It identifies paths that adversaries can follow to accomplish sabotage or theft. ASDs help prevent overlooking possible adversary paths and, when considering protection system upgrades, ASDs help select upgrades that affect the most adversary paths. Figure 7 provides an ASD for the example facility of Figure 6. The most vulnerable adversary path is used to measure the effectiveness of the physical protection system.

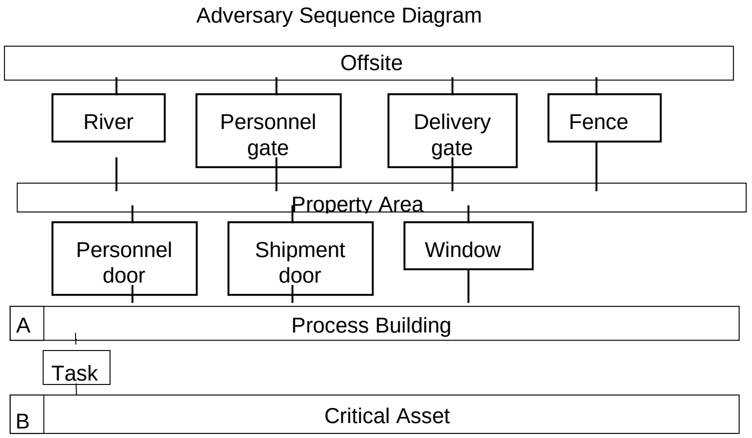


Figure 7. ASD for example facility

From the postulated most vulnerable strategies and physical paths noted, the team should specify a most-vulnerable adversary scenario. If necessary, more than one scenario can be analyzed. The scenario(s) will be used to determine protection system effectiveness.

Physical Protection Features for Scenario

The features of the facility that support the functions of detection, delay, response, and mitigation that could affect the outcome of the adversary scenario should be noted. Any safety features that could affect the outcome should also be noted. The information about features can be taken from the facility worksheets, the characterization matrix, and facility knowledge. Table 9 describes an example adversary scenario and lists site features for each system function.

Most Vulnerable Scenario: Adversary climbs over property fence, enters process building via rollup doors (open), traverses to critical asset and destroys equipment

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

Table 9. Example Scenario and Protection System Feature List

Likelihood of Adversary Success for Scenario – Physical

Using the list of features for each PPS element (i.e., detection, delay, and response) together with the definition table for likelihood of adversary success, L_{AS}, (Table 5), the assessment team then determines a likelihood of adversary success level for each specific scenario. The team should first consider if the PPS features would be expected to prevent the undesired event. If the judgment is a low expectation, the team should next consider if the detection element combined with mitigation measures would reduce the consequences of undesired events to acceptable levels. Mitigation measures may be disabled by adversaries.

As an example, assume a team decides that, for the scenario in Figure 9, the levels of detection, delay, and response are judged to be low. Since all functions are judged to be low, the protection system is judged to not be able to prevent the undesired event. Further assume that the team judges the mitigation/safety function to be at the medium level. Since the detection function was judged to be low, the estimated ability of the site features to reduce the consequences of the scenario, to not have a catastrophic event, is judged to be low. System effectiveness for this scenario would be at the low level. Using Figure 7—the likelihood of adversary success definition table—the likelihood of adversary success level, L_{AS}, for this scenario would be given a level of 2. This level will be used to estimate the risk level for physical protection for the node.

Whenever protection system effectiveness is judged to be low, vulnerabilities are implied. Specific system vulnerabilities may be identified by reviewing why any specific system function (detection, delay, response, or mitigation) is not at the high level. Any specific vulnerabilities identified should be addressed when making recommendations.

Most Vulnerable Adversary Scenario – Process Control Path

The possible process control adversary paths can be reviewed on the process flow diagram for the facility and the process control diagram described earlier in Figures 2 and 4, respectively. Just as in the case for the physical paths, the assessment team should specify what they believe to be the most vulnerable adversary scenario to cause the undesired event using the process control system.

In addition to the analysis for prevention of an undesired event, the analysis should also consider the effects of the control process (or lack of control process) to either eliminate or slow the mitigation process.

Protection for Process Control Scenario

The features of the protection system for process control that could affect the outcome of the adversary scenario should be noted. The information about features can be taken from the facility worksheets, the characterization matrix, and facility knowledge. The protection system must protect the communications, commercial hardware and software, application software, parameter data, or support infrastructure, e.g., power, HVAC. Table 10 describes an example process control adversary scenario and provides a table to list features of the protection system.

Most Vulnerable Process Control Scenario:
Adversary accesses process control system via the Internet

Communications	Commercial Hardware & Software	Application Software	Parameter Data	Support Infrastructure
▪ Encryption ▪ Lock & sensor comm. rooms ▪ Supervised lines ▪ Authentication ▪ Redundant systems	▪ Current security patches ▪ Strong passwords ▪ Audits ▪ Monitor unusual use	▪ Config. control ▪ Trusted source ▪ Documen-tation ▪ Thorough testing	▪ Validate value & effect ▪ Config. control ▪ Read only ▪ Auth. write privilege	▪ UPS ▪ Automatic switch to backup ▪ Environ. controls

Table 10. Example Process Control Protection

Likelihood of Adversary Success for Process Control Scenario

The assessment team must judge the protection system effectiveness for the process control system to prevent the adversary from using the process control system to cause the undesired event. If any one of the categories of communications, commercial hardware and software, application software, parameter data, or support infrastructure can be exploited, the system effectiveness is judged to be low. The definition table for likelihood of adversary success for process control paths, Table 7, should be used to determine the likelihood of adversary success level, L_{AS}, for this scenario. The level will be used to estimate the risk level.

Whenever protection system effectiveness is judged to be low, vulnerabilities are implied. Specific system vulnerabilities may be identified by reviewing any process control protection categories (communications, commercial hardware and software, application software, parameter data, or support infrastructure) that were judged to be lacking features. Any specific vulnerabilities identified should be addressed when making recommendations.

10. Risk Analysis (Review of Methodology to This Point)

A brief review of the methodology to this point is presented below in preparation for risk analysis.

For the purposes of this methodology,

Risk is a function of S, L_A, and $L_{AS,}$ where
S —severity of consequences of an event (Section 4
L_A — likelihood of adversary attack(Section 5)
L_{AS} —likelihood of adversary success in causing a catastrophic event (Section 9)

Priority cases for undesired event/adversary group were determined by estimating the likelihood and severity level, L_S, using the priority ranking matrix for likelihood of attack, L_A, and severity, S. L_S levels are combined with L_{AS} levels to estimate the level of risk for each undesired event/adversary group. Figure 8 is a flow chart for the process.

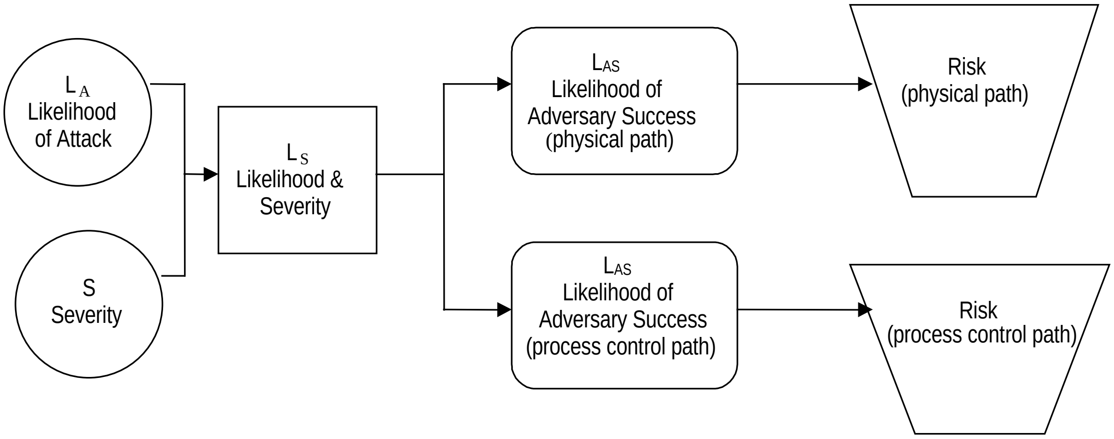


Figure 8. Risk analysis flow chart

Risk levels for each undesired event/adversary group can be estimated using the levels estimated for likelihood and severity, L_S, and the likelihood of adversary success, L_{AS}, levels used as input to the risk priority-ranking matrix (Table 9) developed in Section 7, *Prepare for Site Analysis*. Table 11 summarizes the results of the risk analysis.

Risk Level Summary	Undesired Event =_______________ Severity, S, = ___________________					
	Adversary group	L_S	L_{AS} (physical)	Risk (physical)	L_{AS} (process control)	Risk (process control)
Node 1						
Node 2						
Node 3						

Table 11. Risk Level Summary

If the risk level is less than a value of four (or other value as chosen by a CF) for any adversary group, the risk level should be decreased. Recommendations to reduce the risk level should address the specific vulnerabilities identified as part of estimating the protection system effectiveness in Section 9.

11. Recommendations for Risk Reduction

When the risk level is less than a value of four, recommendations should be made and include suggested detection, delay, response, and mitigation/safety features that answer or mitigate the specific identified vulnerabilities. The goal is low-cost, high-return upgrades. Guidance for selecting upgrade features include providing:

- protection for common vulnerabilities
- protection-in-depth
- balanced protection

Vulnerabilities that are common to all undesired events should be addressed first. A system feature common to many scenarios is a good candidate for upgrade because upgrading this single feature can usually result in a higher level of protection for many scenarios. Guidance considerations for where to place specific features would be: 1) Where would it be most desirable to have the first detection point? and 2) Where would added delay affect the most scenarios? In general, the first detection point must be as early as possible. However, placing the delay and response/mitigation features closer to a target could provide the most benefit if all paths are affected. The site layout plan or an ASD, if developed, can help make decisions about where features should be placed.

Protection-in-depth means that an adversary should be required to avoid or defeat several protective devices in sequence to accomplish the goal. Layers of features cause difficulty for an adversary including increased uncertainty about the system, more extensive preparations prior to the attack, and additional steps where failure could occur.

Balanced protection ensures that an adversary will encounter effective elements of the physical protection system no matter how the critical asset is approached. For a completely balanced layer of system features, the detection performances and delay times would be equal along all ASD paths. Complete balance is probably not possible. Some features may have inherent protection. Walls, for example, may be resistant to penetration, not because of physical protection requirements, but because of structural or safety requirements. Thus, door, hatch, and grill delays may be less than wall delays and still be adequate. There is no advantage to over-designing specific features that result in unbalanced protection. As an example, it is pointless to install a costly vault door on a flimsy wall. Reviewing the site layout plan or the ASD will help ensure all adversary paths are protected.

Recommendations might include:

- Physical protection improvements (detection, delay, response improvements). Examples:
  - Sensors on gates, doors
  - Assessment system (cameras)
  - Security alarm control center
  - Hardened doors and locks
  - Access control (cards + PIN) on doors and gates
  - Compartmentalized facility
- Consequence reduction improvements (detection, mitigation improvements). Examples:
  - Reduce quantity of controlled chemicals, i.e., to <TQ
  - Disperse chemicals, i.e., in storage
  - **Add additional mitigation measures**
- Process Control protection improvements. Examples:
  - Chemical/process sensors routed to alarm control center
  - Protected/strong passwords (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
  - Isolate process control from external information systems

After recommendations are made, the new system effectiveness level and risk level should be estimated. The process can continue until acceptable risk levels (probably 3 or 4) are achieved. Other impacts of the recommendations—cost, impact on operations or schedules, and employee acceptance—should also be considered.

12. Final Report

The final report and/or package for briefing management can be prepared from the worksheets when completing the analysis. Item suggested for inclusion in the final report are:

1. screening process results
2. facility characterization matrix and critical nodes analyzed
3. severity level definition table and severity level for each undesired event
4. threat definition table
5. likelihood of attack level definition table and L_A levels for each undesired event/adversary group
6. L_S (likelihood and severity) priority ranking matrix and L_S levels for each undesired event/adversary group
7. priority undesired event/adversary groups analyzed
8. most vulnerable adversary scenarios for physical path for each priority undesired event/adversary group
9. most vulnerable adversary scenarios for process control path for each priority undesired event/adversary group
10. likelihood of adversary success level definition table for physical paths and L_{AS} levels for each priority undesired event/adversary group
11. likelihood of adversary success level definition table for process control paths and L_{AS} levels for each priority undesired event/adversary group

12. risk priority ranking matrix and risk levels for both physical paths and process control paths for each priority undesired event/adversary group (risk level summary table)
13. summary of recommendations to reduce risk levels

About the National Institute of Justice

NIJ is the research, development, and evaluation agency of the U.S. Department of Justice and is solely dedicated to researching crime control and justice issues. NIJ provides objective, independent, nonpartisan, evidence-based knowledge and tools to meet the challenges of crime and justice, particularly at the State and local levels. NIJ's principal authorities are derived from the Omnibus Crime Control and Safe Streets Act of 1968, as amended (42 U.S.C. §§ 3721–3722).

NIJ's Mission

In partnership with others, NIJ's mission is to prevent and reduce crime, improve law enforcement and the administration of justice, and promote public safety. By applying the disciplines of the social and physical sciences, NIJ—

- Researches the nature and impact of crime and delinquency.
- Develops applied technologies, standards, and tools for criminal justice practitioners.
- Evaluates existing programs and responses to crime.
- Tests innovative concepts and program models in the field.
- Assists policymakers, program partners, and justice agencies.
- Disseminates knowledge to many audiences.

NIJ's Strategic Direction and Program Areas

NIJ is committed to five challenges as part of its strategic plan: 1) *rethinking* justice and the processes that create just communities; 2) *understanding* the nexus between social conditions and crime; 3) *breaking* the cycle of crime by testing research-based interventions; 4) *creating* the tools and technologies that meet the needs of practitioners; and 5) *expanding* horizons through interdisciplinary and international perspectives. In addressing these strategic challenges, the Institute is involved in the following program areas: crime control and prevention, drugs and crime, justice systems and offender behavior, violence and victimization, communications and information technologies, critical incident response, investigative and forensic sciences (including DNA), less-than-lethal technologies, officer protection, education and training technologies, testing and standards, technology assistance to law enforcement and corrections agencies, field testing of promising programs, and international crime control. NIJ communicates its findings through conferences and print and electronic media.

NIJ's Structure

The NIJ Director is appointed by the President and confirmed by the Senate. The NIJ Director establishes the Institute's objectives, guided by the priorities of the Office of Justice Programs, the U.S. Department of Justice, and the needs of the field. NIJ actively solicits the views of criminal justice and other professionals and researchers to inform its search for the knowledge and tools to guide policy and practice.

NIJ has three operating units. The Office of Research and Evaluation manages social science research and evaluation and crime mapping research. The Office of Science and Technology manages technology research and development, standards development, and technology assistance to State and local law enforcement and corrections agencies. The Office of Development and Communications manages field tests of model programs, international research, and knowledge dissemination programs.

To find out more about the National Institute of Justice, please contact:

National Criminal Justice
  Reference Service
P.O. Box 6000
Rockville, MD 20849–6000
800–851–3420
e-mail: *askncjrs@ncjrs.org*

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

Washington, DC 20531

JUNE 02

NCJ 195171