PDHonline Course K106 (2 PDH)

Vulnerability of U.S. Chemical Facilities to Terrorist Attack

Instructor: Robert B. Coulter, PE

2012

PDH Online | PDH Center

5272 Meadow Estates Drive
Fairfax, VA 22030-6658
Phone & Fax: 703-988-0088
www.PDHonline.org
www.PDHcenter.com

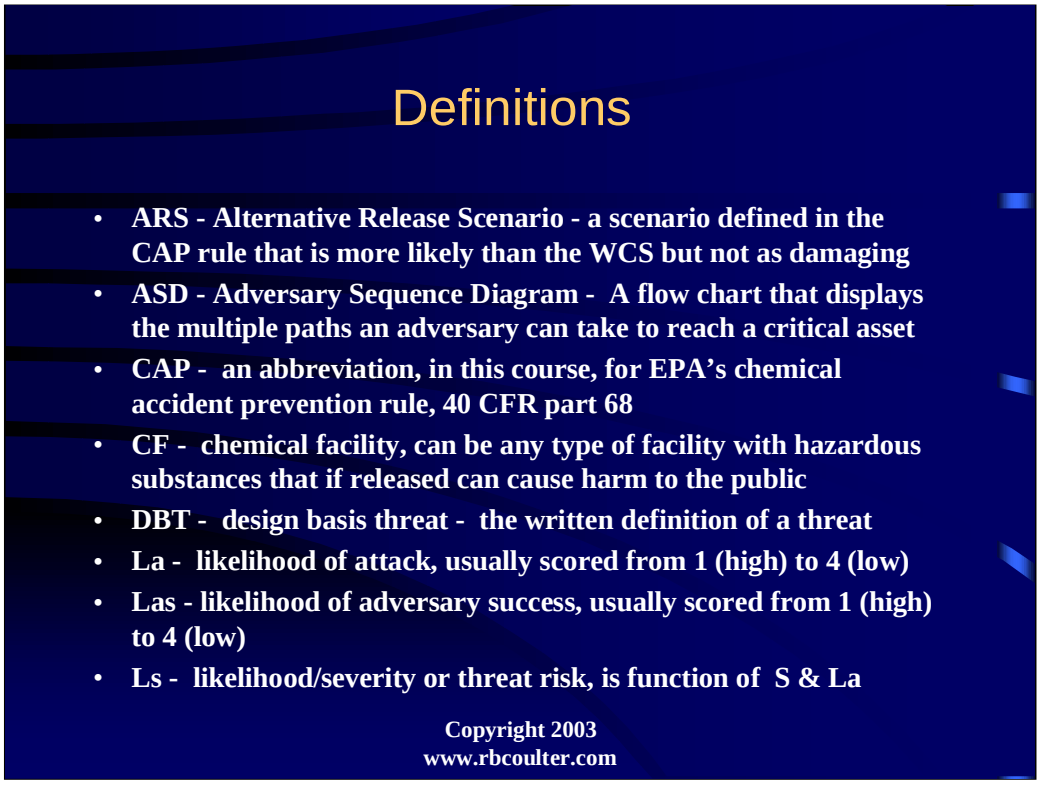
An Approved Continuing Education Provider

This course is based on a prototype methodology to assess the security of U.S. chemical facilities. The goal of the methodology is to assist companies that own or operate chemical facilities (CFs) in reducing the risk of a terrorist attack upon their sites.

This methodology was developed by the National Institute of Justice (research arm of the DOJ) & DOE's Sandia National Laboratories. This joint effort involved research into the threats & risks associated with the chemical industry. Current practices at CFs were surveyed, and comments were solicited from industry, government, academia & private citizens in the development of this methodology.

The guidelines in this methodology are meant to prevent or mitigate terrorist or criminal action at chemical facilities. They are not designed to address transportation or cyber (internet) issues which may also impact CFs. This method does address protection of the process control systems which has some similarity to cyber issues.

The source document was issued in November 2002 and is titled "A Method to Assess the Vulnerability of U.S. Chemical Facilities". It is available for download from the National Institute of Justice's website. (see link below or notebook)



ARS - Alternative Release Scenario - a scenario defined in the CAP rule that is more likely than the WCS but with less negative consequences

ASD - Adversary Sequence Diagram - A flow chart that displays the multiple paths an adversary can take to reach a critical asset. It assists a VA team in analyzing adversarial success & risk.

CAP - an abbreviation, in this course, for EPA's chemical accident prevention rule, 40 CFR part 68 (see the link below). This rule imposes standards on some CFs in order to prevent accidental chemical releases. Many elements of this rule are useful in VA.

CF - chemical facility

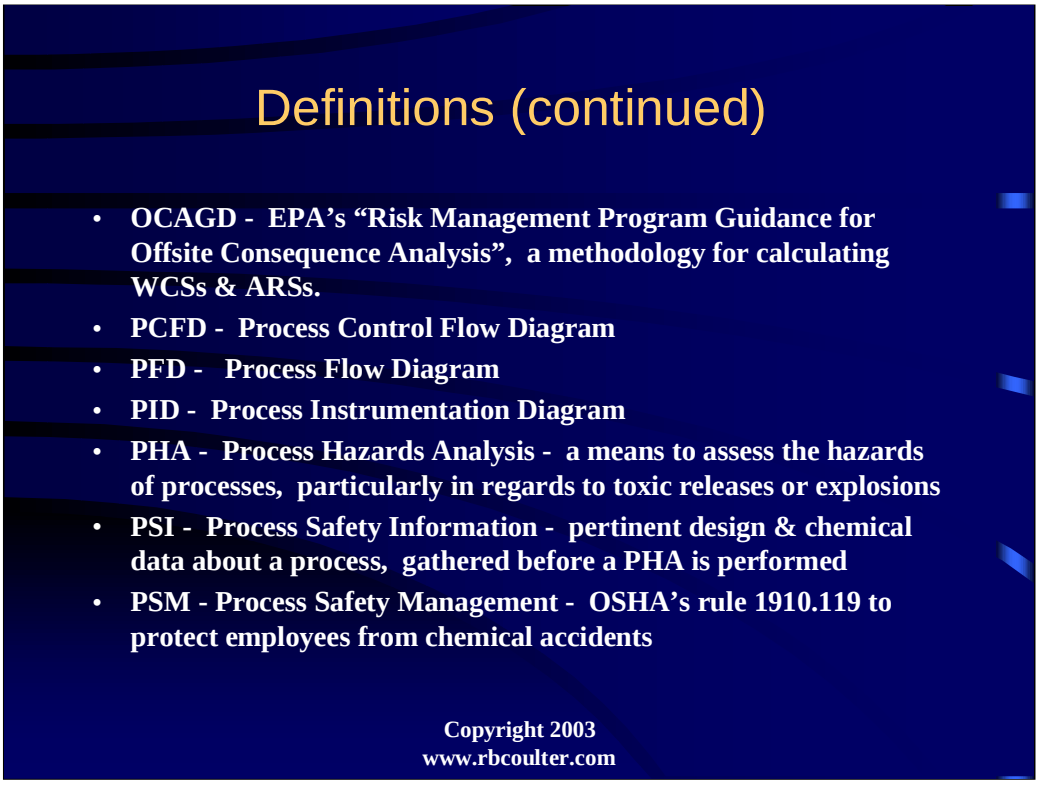
DBT - design basis threat - This is the written definition of a threat and is dependent on the adversary's traits & resources.

La - likelihood of attack, usually scored from 1 (high) to 4 (low)

Las - likelihood of adversary success, usually scored from 1 (high) to 4 (low) -

The VA team determine Las values based on a review of protective features & adversary's traits

Ls - likelihood/severity or threat risk, is function of S & La - The VA leader screens scenarios & determines Ls values. Scenarios with higher ranking Ls values are passed on to the VA team for further review.



OCAGD - This EPA's "Risk Management Program Guidance for Offsite Consequence Analysis", This is a methodology for calculating WCSs & ARSs that is freely available from EPA's website (see the link below).

PCFD - Process Control Flow Diagram

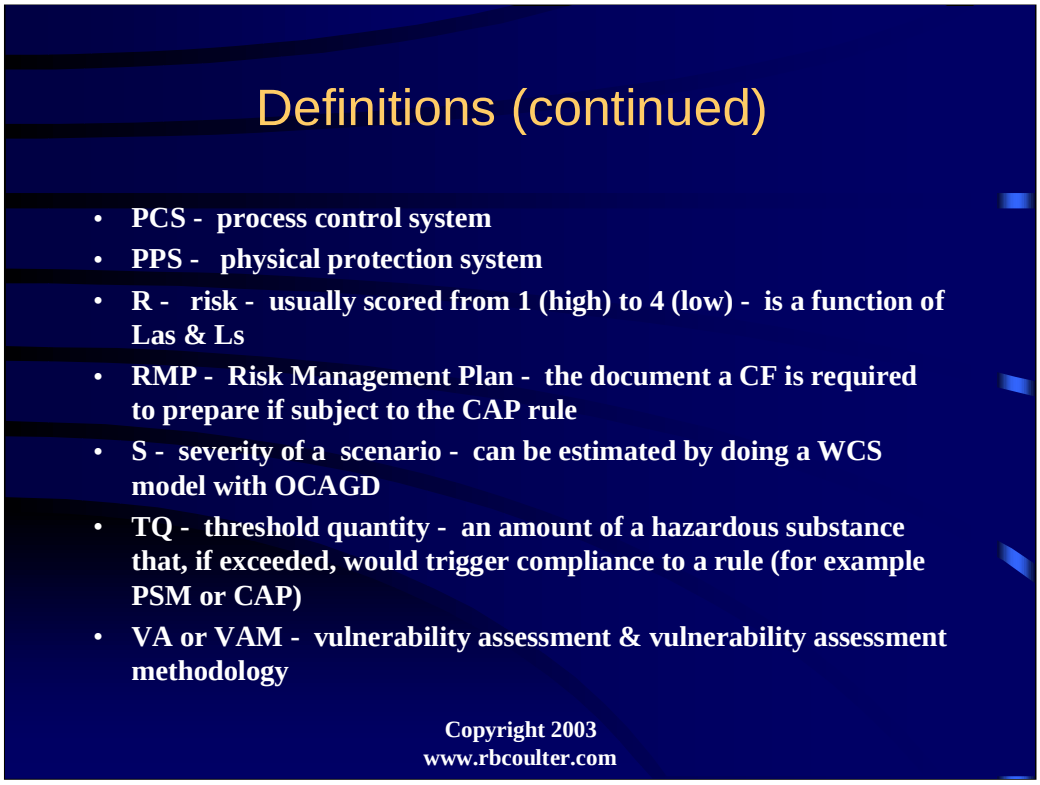
PFD - Process Flow Diagram

PID - Process Instrumentation Diagram

PHA - Process Hazards Analysis - This is a means to assess the hazards of processes, particularly in regards to accidental toxic releases or explosions. Many CFs must already performs PHAs. VA is similar to PHA but considers non-accidental hazards.

PSI - Process Safety Information - This is pertinent design & chemical data about a process. It is gathered before a PHA is performed to assist a PHA team in performing its analysis. The VA team can also draw on this database which would already be in place at many CFs.

PSM - Process Safety Management - This is OSHA's rule 1910.119 to protect employees from chemical accidents



PCS - process control system

PPS - physical protection system

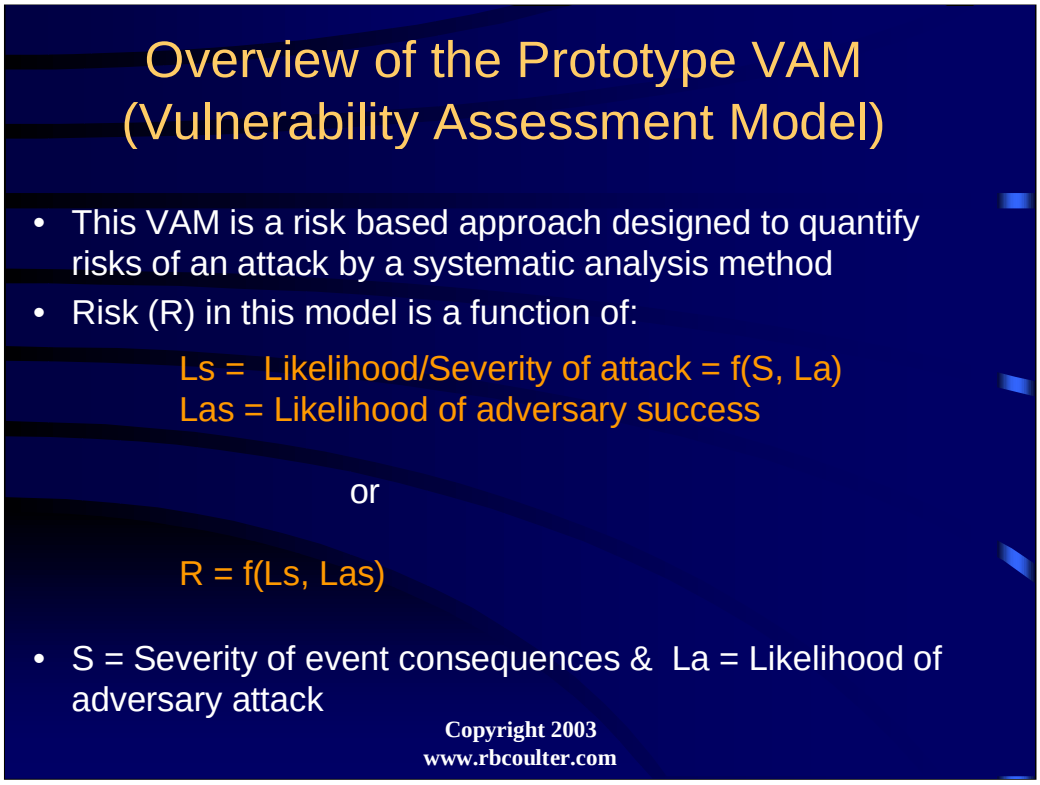
R - risk - It is usually scored from 1 (high) to 4 (low) and is a function of Las & Ls. It is the final value in judging a scenario and indicates which areas require risk reduction.

RMP - Risk Management Plan - This is the document a CF is required to prepare if subject to the CAP rule. Much of the information in an RMP can be used in a VA, particularly the severity of a scenario.

S - severity of a scenario - It can be estimated by doing a WCS model with OCAGD.

TQ - threshold quantity - an amount of a hazardous substance that, if exceeded, would trigger compliance to a rule (for example PSM or CAP)

VA or VAM - vulnerability assessment & vulnerability assessment methodology



This VAM or vulnerability assessment model is a risk based approach designed to quantify risks of an attack by a systematic analysis method.

Risk, for those familiar with PHA or process hazards analysis, is a ranking of a hazard and is usually defined as a function of Severity & Likelihood. The VAM risk model is similar but also considers adversary parameters (likelihood of attack, for example) in the determination of risk.

Specifically , Risk (R) in the VAM is a function of:

Ls = Likelihood/Severity of attack = f(S, La)

Ls can be thought of as the risk of an attack. It does not indicate or quantify the success of the attack.

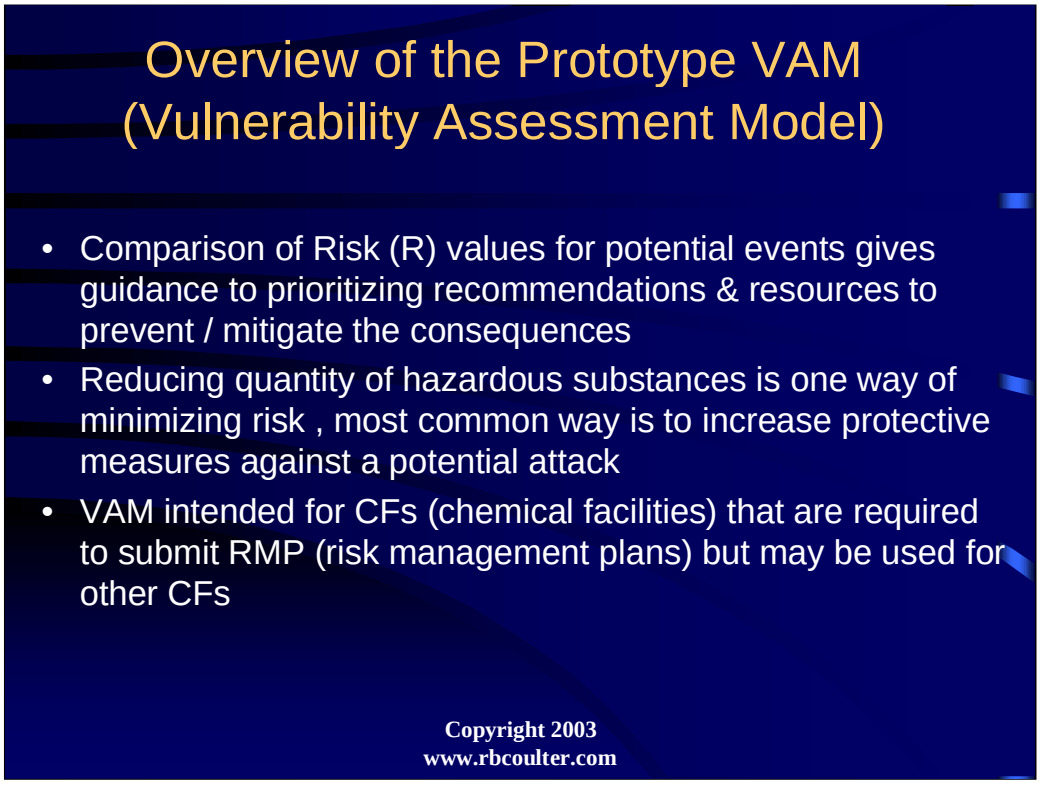
Las = Likelihood of adversary success

This term is a measure of an adversary's ability to be successful in an attack and is a strong function of a CF's protective features to prevent the attack.

Risk is is then defined as follows:

R = f(Ls, Las)

S = Is the severity of the event consequences and can be thought of as being equivalent to the consequences associated with a worse case scenarios (WCSs) or alternative release scenarios (ARSs). Many CFs may have already determined WCSs & ARSs for some processes under the CAP rule (40 CFR part 68). La is the likelihood of an adversary attack and is a function of known threats to the CF.



A comparison of Risk (R) values for potential events or scenarios gives guidance to prioritizing recommendations & resources to prevent an attack or mitigate the consequences of an attack.

Reducing the quantity of hazardous substances at a CF is one way of minimizing risk. This often not feasible at a CF. The most common way to reduce risk is to increase the protective measures against a potential attack. (For example, installing barricades around toxic chemical storage tanks)

The VAM is intended for CFs (chemical facilities) that are required to submit RMP (risk management plans). This is the CAP rule (40 CFR part 68). This methodology; however, can be applied to any CF that wishes to reduce their risk of a terrorist attack.

The VAM steps to be discussed are as follows:

Screening for the need for a VAM - Corporate level

Defining the VA project - facilitator

Planning - Characterizing the facility - facilitator

Planning - Deriving severity levels - facilitator

Planning - Assessing threats - facilitator

Planning - Prioritizing scenarios / threats - facilitator

Planning - Preparing for the site analysis - facilitator

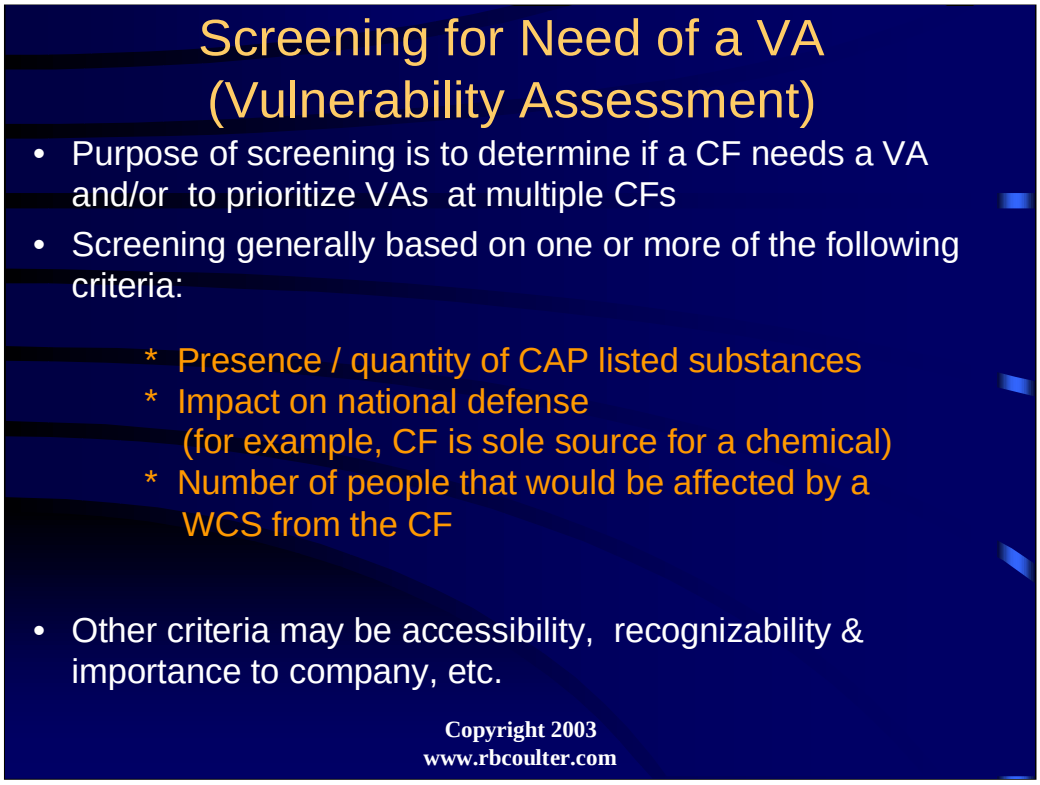
Site Survey - Surveying the site - team

Analysis - Analyzing the system's effectiveness - team

Analysis - Analyzing risks - team

Risk Reduction - Making recommendations - team

Preparing the final report - facilitator



The first step is suggested to be done at the corporate level of a company that operates CFs. The purpose of the screening is to determine if one or more CFs within the company need a VA. If so, then the VAs should be prioritized as part of the screening process. Naturally, the company should consider doing the high priority VA s first and/or commit more resources to them.

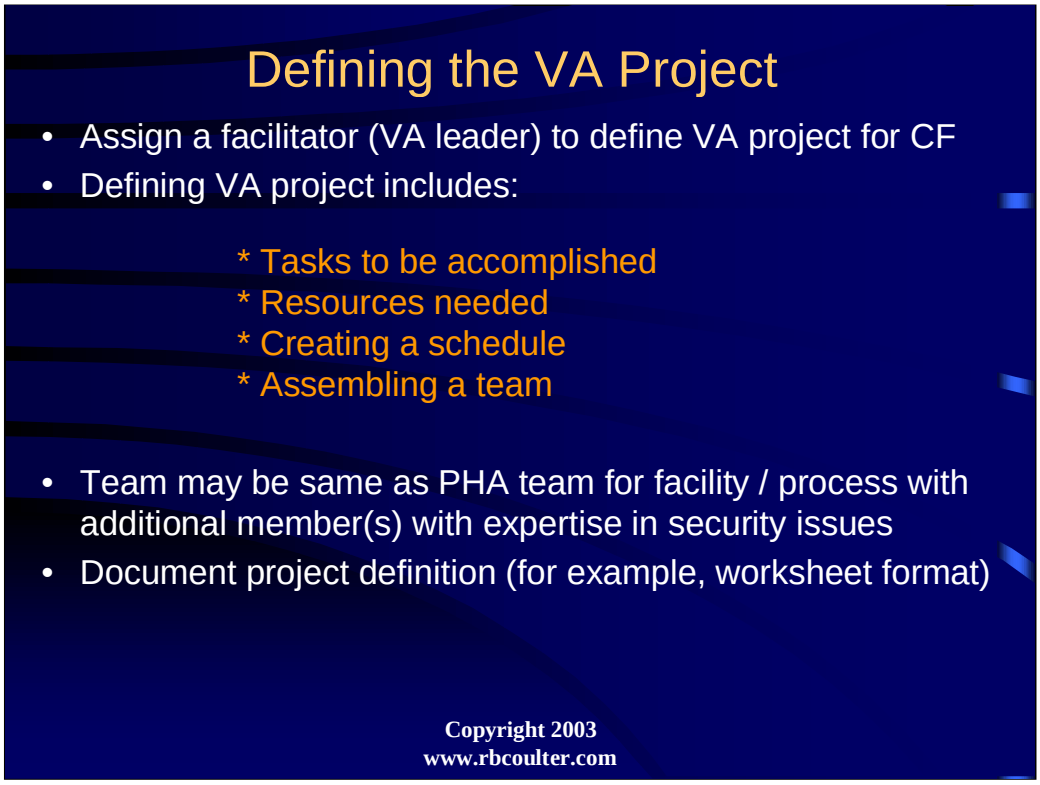
The screening will generally based on one or more of the following criteria:

* **The presence & quantity of CAP listed substances.** CFs subject to the CAP rule should receive higher priority over those facilities that are not required to comply with CAP. Facilities with the larger amounts of CAP listed substances should have even higher priority.

* **The impact on national defense** (for example, a CF may be the sole source for a chemical)

* **The number of people that would be affected by a WCS from the CF**. This should be easily obtained for CFs subject to the CAP rule.

Other criteria may be accessibility, recognizability & importance to company, etc



Next, a facilitator (or VA leader) should be chosen to define VA project for a CF.

The process of defining a VA project includes:

* Tasks to be accomplished

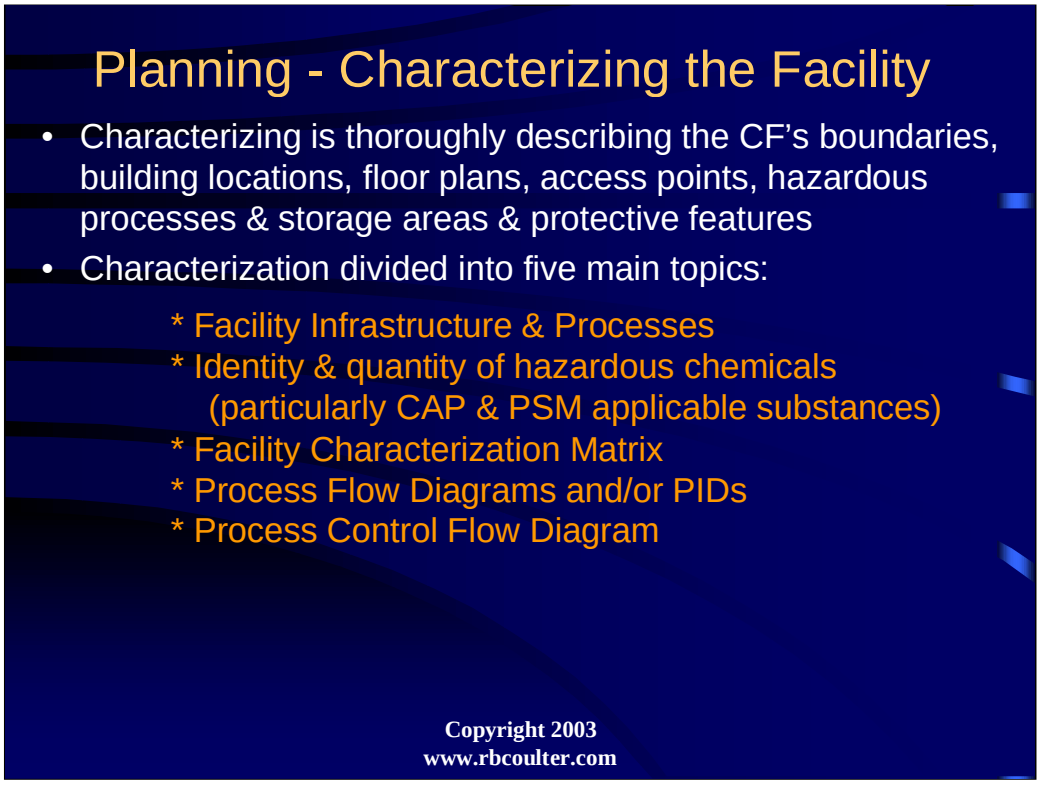
* Resources needed

* Creating a schedule

* Assembling a team

The team may be the same as the PHA team for the facility. If multiple PHA teams were involved at a facility then the VA leader may want to draw from this pool of personnel for the VA team.

The VA leader will need to document the VA project scope or definition prior to the team meeting. This can be done as a worksheet or other format. This documentation is similar to process safety information (PSI) generated prior to a process hazards analysis (PHA).



The VA leader should characterize or thoroughly describe the CF's boundaries, building locations, floor plans, access points, hazardous processes & storage areas & protective features.

Characterization is divided into five main topics:

* Facility Infrastructure & Processes -

* Indicating the identity & quantity of hazardous chemicals. (particularly CAP & PSM applicable substances).

* Facility Characterization Matrix

* Process Flow Diagrams and/or PIDs

* Process Control Flow Diagram - Characterize the pertinent process control systems (computers etc.) if they can be exploited in an attack.

The VA leader should focus on gathering the following information concerning the CF:

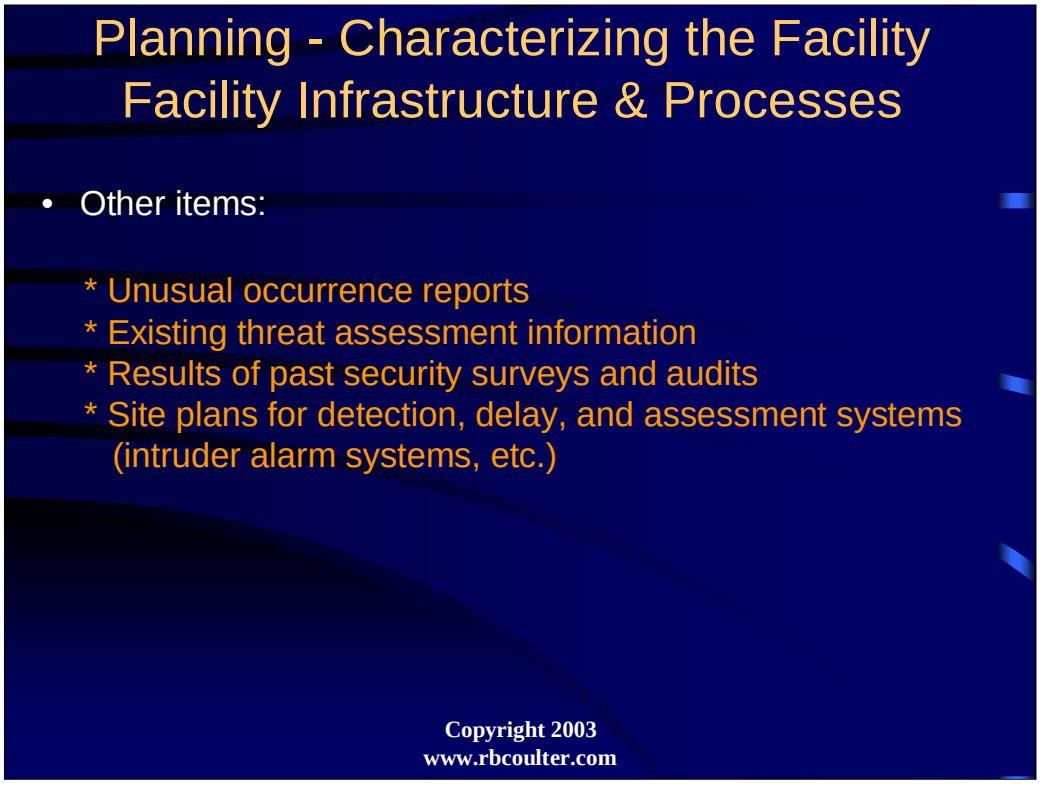
* Building design(s), traffic areas, terrain, weather purpose of building(s)
* Property borders, entrance/exit routes, adjacent parking lots & buildings (commercial / residential)
* Existing protective features, access/permissions, number of employees/contractors/visitors, operating schedules, other security procedures
* Emergency procedures / evacuation procedures
* Emergency notifications procedures
* Availability of onsite & local security personnel

The following information related to processes and control systems should be obtained:

* Access to process control system (authorized users, means of access, protective features)

* Safety procedures & features - The VAM does not seem to clarify this very well. This appears to be safety procedures & features associated with multiple processes at a CF.

* Process control procedures & features - This appears to be related to features common to all processes.



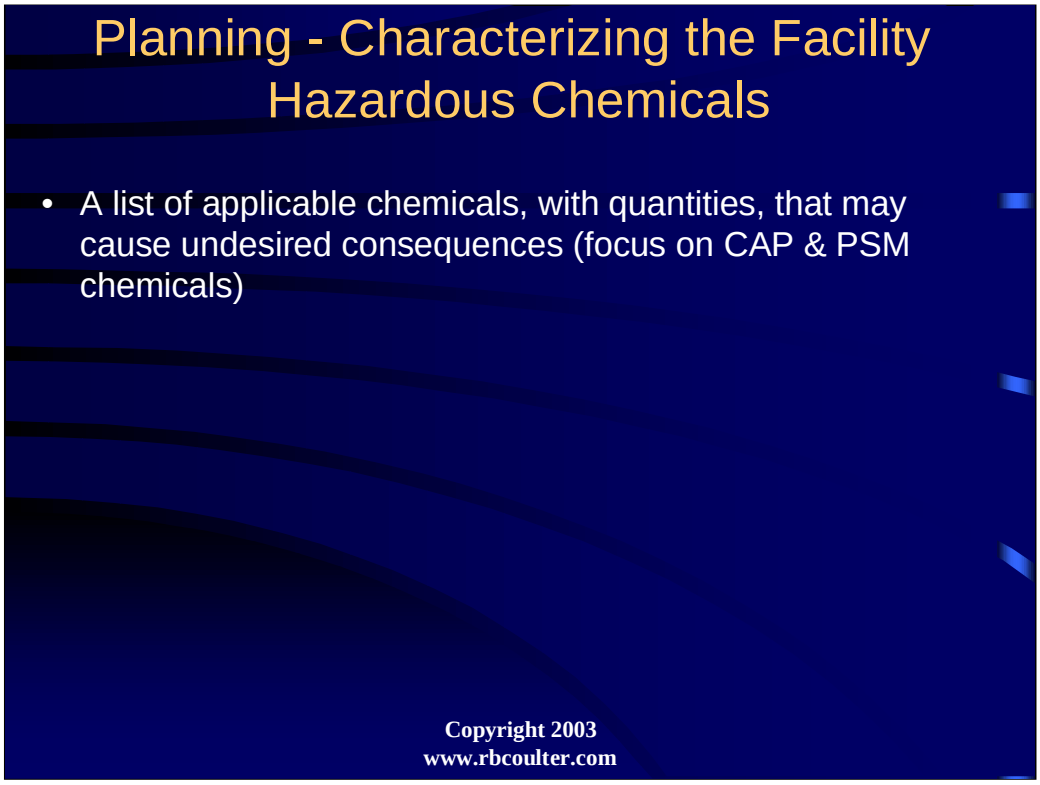
Other important items needed are:

* Unusual occurrence reports (chemical releases, process upsets, etc.)

* Existing threat assessment information (consider consulting law enforcement agencies)

* Results of past security surveys and audits

* Site plans for detection, delay, and assessment systems
(intruder alarm systems, etc.)



Indicate the identity & quantity of hazardous chemicals. Focus on those chemicals that could have a significant offsite impact (particularly CAP & PSM applicable substances). Consult the RMP for CFs that must comply with the CAP rule. The 312 (hazardous chemical inventory forms) reports are also another good source of information.

Planning - Characterizing the Facility/ Facility Characterization Matrix

Exhibit 3. 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										
2	Covered chemicals										
3	Quantity of covered chemicals										
4	Process duration										
5	Recognizability										
6	Accessibility										
7	Criticality rating (sum for activity)										

1. **Process activity.** Describe the activity (for example, from flow diagram, P&ID, reactor, pipe, storage tank, transportation).
2. **Covered chemicals.** Enter the names of all chemicals used in this activity. Enter *Y* if the chemical is listed in 40 CFR 68.130 or 29 CFR 1910.119. Enter *N* if the chemical is not listed.
3. **Quantity of covered chemicals.** Enter *1* if the quantity is more than 25 times the threshold quantity (TQ); *2* if the quantity is 10–25 times TQ; *3* if the quantity is 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 the process is 50–99% continuous; *3* if the process is 25–49% continuous; and *4* if the process is 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 require extensive knowledge for recognition.
6. **Accessibility.** Enter *1* if easily accessible; *2* if fairly accessible (target is located outside or in an unsecured area); *3* if moderately accessible (target is located inside a building or enclosure); and *4* if not accessible or only accessible with extreme difficulty.

Determine critical activities: _____

The critical activity is the activity or activities with the lowest score under number 7 above.

This is basically a pre-assessment of the CFs process hazards and vulnerabilities and is generally shown in tabular form. It may be more useful to complete PFDs and Process Control characterizations (in the next sections) for each process/activity before doing the facility characterization matrix.

Each column in this table represents a process or process activity. This can be a reactor, storage tank or pipe system, etc. Its description is entered into row #1.

Row #2 is to list the identity of the hazardous chemical associated with the particular activity. Also, enter Y or N to indicate if the chemical is subject to the CAP, PSM or other applicable guidelines that is consistent with this characterization matrix. The CF may want to specify it's own guidelines and TQs covering a broader list of chemicals than specified in the CAP and PSM lists. It is recommended; however, that the VA leader not specify TQs for CAP and PSM listed substances that are greater than indicated in the regulations.

Row #3 is for entering a rank for the quantity of hazardous chemical present in the activity. Enter "1" if the amount present > than 25 times the TQ under the applicable rule. "2" if it is 10-25 times the TQ. "3" for 1-10 times the TQ, and "4" for if the quantity is less than the TQ.

Enter the rank indicating the duration of the activity or process in row #4. "1" for 100% of the time, "2" for 50% to 99%, "3" for 25%-49%, "4" for less than 25%. Processes or activities that are ongoing (for example, many storage tanks) would be considered operating 100% of the time and would have process duration rank of "1".

Planning - Characterizing the Facility/ Facility Characterization Matrix

Exhibit 3. 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										
2	Covered chemicals										
3	Quantity of covered chemicals										
4	Process duration										
5	Recognizability										
6	Accessibility										
7	Criticality rating (sum for activity)										

1. **Process activity.** Describe the activity (for example, from flow diagram, P&ID, reactor, pipe, storage tank, transportation).
2. **Covered chemicals.** Enter the names of all chemicals used in this activity. Enter *Y* if the chemical is listed in 40 CFR 68.130 or 29 CFR 1910.119. Enter *N* if the chemical is not listed.
3. **Quantity of covered chemicals.** Enter *1* if the quantity is more than 25 times the threshold quantity (TQ); *2* if the quantity is 10–25 times TQ; *3* if the quantity is 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 the process is 50–99% continuous; *3* if the process is 25–49% continuous; and *4* if the process is 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 require extensive knowledge for recognition.
6. **Accessibility.** Enter *1* if easily accessible; *2* if fairly accessible (target is located outside or in an unsecured area); *3* if moderately accessible (target is located inside a building or enclosure); and *4* if not accessible or only accessible with extreme difficulty.

Determine critical activities: _____

The critical activity is the activity or activities with the lowest score under number 7 above.

Row #5 is the rank of recognizability for the activity. "1" being the most important & easily recognizability with little or no prior knowledge. "4" is for an activity that requires extensive knowledge for recognition.

Row #6 ranks the accessibility of the activity/process to a potential attacker. "1" is most accessible. "4" is the least accessible.

The final row is the rank of the criticality rating. It may be computed as an average of the rank values in that column for a particular process/activity. Low criticality ranks / scores indicate processes that are at higher risk.

Planning - Characterizing the Facility
Facility Characterization Matrix

Exhibit 3. 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	Reactor	AT tank								
2	Covered chemicals	ATy , BNy	ATy								
3	Quantity of covered chemicals	3	2								
4	Process duration	2	1								
5	Recognizability	2	1								
6	Accessibility	3	2								
7	Criticality rating (sum for activity)	2.5	1.5								

1. **Process activity.** Describe the activity (for example, from flow diagram, P&ID, reactor, pipe, storage tank, transportation).
2. **Covered chemicals.** Enter the names of all chemicals used in this activity. Enter *Y* if the chemical is listed in 40 CFR 68.130 or 29 CFR 1910.119. Enter *N* if the chemical is not listed.
3. **Quantity of covered chemicals.** Enter *1* if the quantity is more than 25 times the threshold quantity (TQ); *2* if the quantity is 10–25 times TQ; *3* if the quantity is 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 the process is 50–99% continuous; *3* if the process is 25–49% continuous; and *4* if the process is 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 require extensive knowledge for recognition.
6. **Accessibility.** Enter *1* if easily accessible; *2* if fairly accessible (target is located outside or in an unsecured area); *3* if moderately accessible (target is located inside a building or enclosure); and *4* if not accessible or only accessible with extreme difficulty.

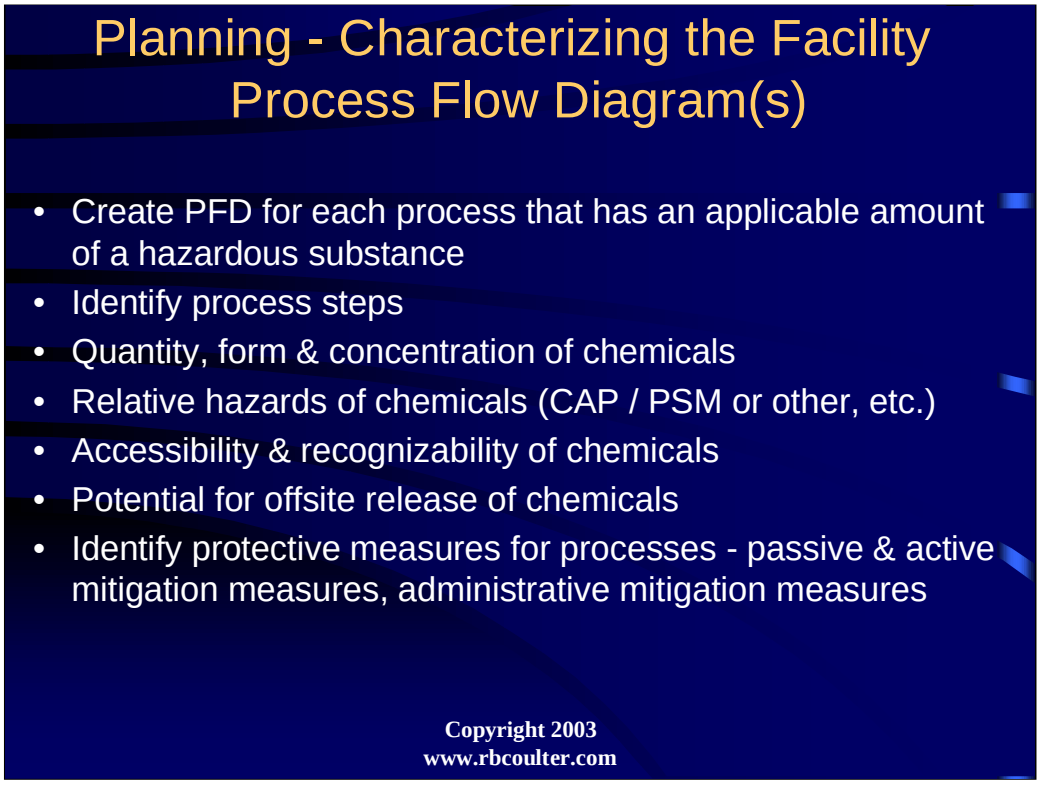
Determine critical activities: Reactor & AT tank

The critical activity is the activity or activities with the lowest score under number 7 above.

This is how data can be entered into the facility characterization form. For this example, AT and BN, are the chemicals of interest. The “y” entered next to their names indicate that they are subject to the CAP rule. The reactor activity has a smaller amount of the listed chemicals, operates at about 75% duration and is somewhat recognizable & accessible. Its criticality rating is 2.5.

The AT storage process has a greater quantity of chemical, has chemical present all the time (100%), and is more recognizable & accessible.

Both processes are critical activities, but the AT storage is more critical because it has a criticality rating of 1.5 compared to 2.5 for the reactor.



This is generally a block flow diagram to indicate a process's hazards and protective features. This is similar to characterization for "Facility Infrastructure & Processes" but is the specific information for a process.

Create a PFD for each process that has an applicable amount (for example, above a pre-defined TQ) of a hazardous substance. (See the next slide for a sample PFD)

Also tabulate the following data:

Identify the applicable process steps

Quantity, form & concentration of chemicals

Relative hazards of chemicals (For example, are they subject to the CAP / PSM/ other rules or some pre-defined guidelines, etc.)

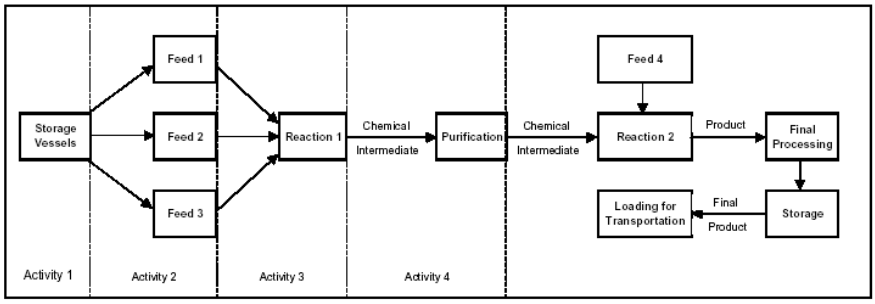
Accessibility & recognizability of chemicals

Potential for offsite release of chemicals

Identify protective measures for processes - passive, active & administrative mitigation measures (passive measures include dikes, active measures include emergency shutdown systems, administrative mitigation measures include inventory control procedures, etc.)

Planning - Characterizing the Facility
PFD Sample

Exhibit 4. Sample Process Flow Diagram



This is a sample process flow diagram(PFD). Note that the process is broken down into five parts - incoming, staging or storing, chemical in process, staging or storing while waiting shipment of products/chemicals.

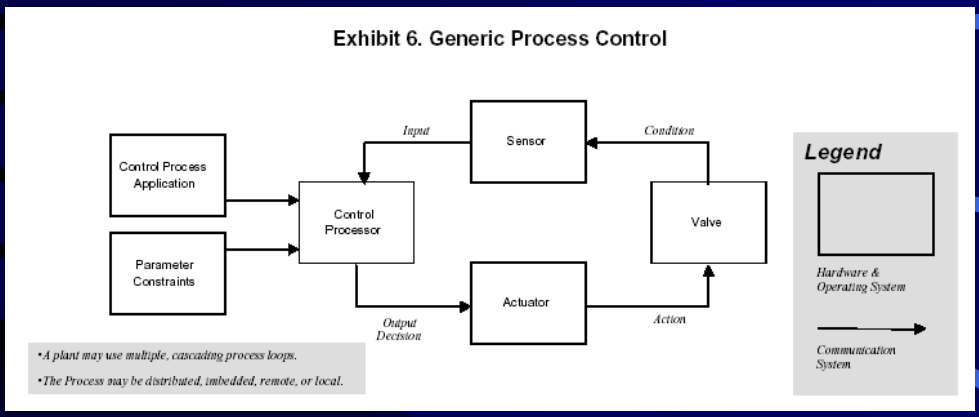
Planning - Characterizing the Facility
PFD Sample

Exhibit 5. Form for Analysis of Operating 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.					

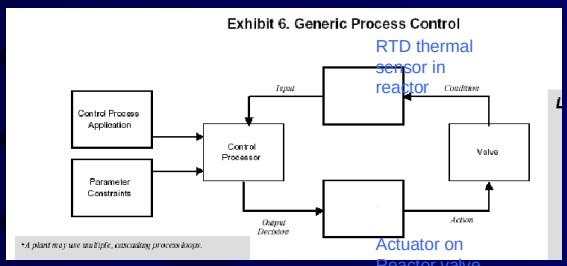
This form can be used to enter the process flow characterization detail about for each stage of a processing activity. Later, this information can be consolidated into the facility characterization matrix table already shown (in exhibit 3).

Planning - Characterizing the Facility
Process Control Flow Diagram



The process control system may be exploited by an adversary to cause an undesired event in a process / activity. If this is true for a process / activity then a process control flow diagram (PCFD) should be made that outlines the process control characteristics that are pertinent to the potential undesired event(s). The above is a generic sample of a PCFD.

Planning - Characterizing the Facility
Process Control Flow Diagram



RTD thermal sensor in reactor

Reactor Water

Actuator on Reactor valve

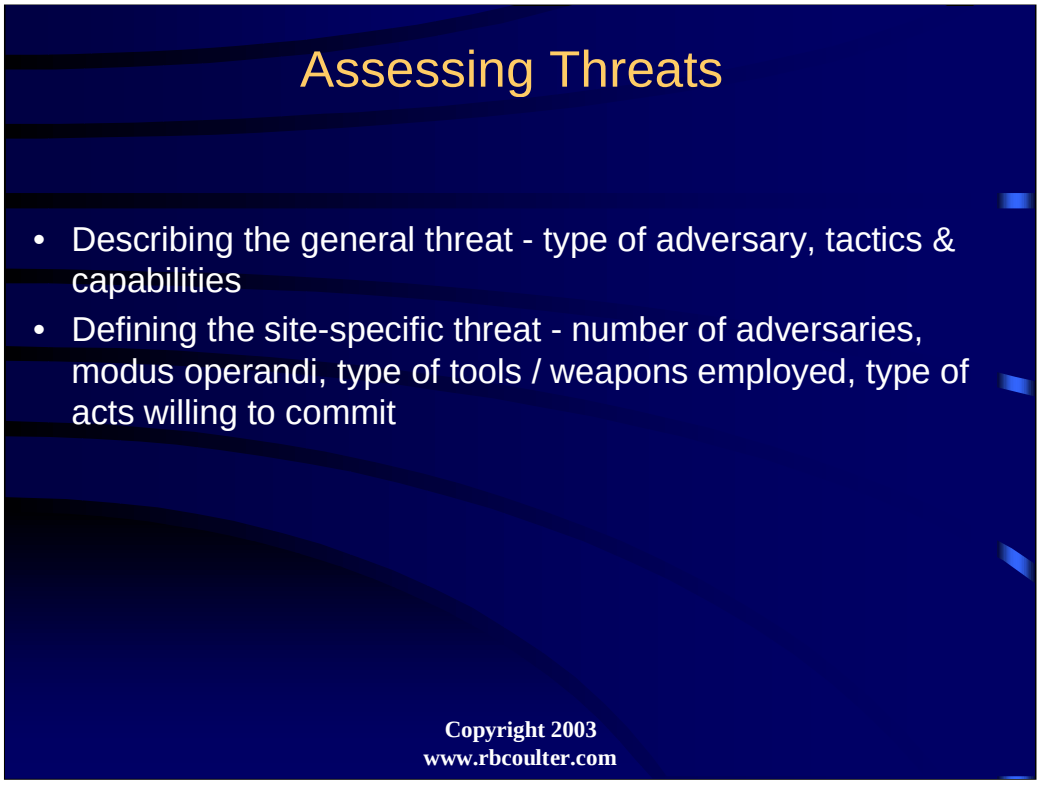
The above is a more specific example of a PCFD. This outlines a basic PCFD for the reactor mentioned earlier in the characterization matrix example.

Deriving Severity Levels

Exhibit 7. Sample Severity Level Definitions

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.

The VA leader needs to decide on the severity levels that will be used in the analysis. Severity is the degree of consequences that may result from a scenario and is not dependent on the likelihood of an event happening. In modeling severity, most analysts (for example, in a PHA) assume that nearly all controls & mitigation do not work. This is roughly equivalent to the WCS done as part of CAP compliance. WCSs can be determined by using EPA's "Risk Management Program Guidance for Offsite Consequence Analysis". (referred to in this course as OCAGD). The above definitions of severity levels may be used during a VA.



At this point the VA leader has characterized or described aspects of the CF concerning consequences & protective features. The next step is to characterize or assess the threats to the facility. The VA leader should consider general & site specific threat characteristics. This should include type of adversaries, tactics & capabilities, modus operandi, type of tools / weapons employed, type of acts willing to commit, etc.

A more objective way of defining threat is to use a concept called "design basis of threat" or DBT. The DBT can be broken down into four parts.

* Type of adversary
* Adversary's potential actions
* Adversary's motivations
* Adversary's capabilities

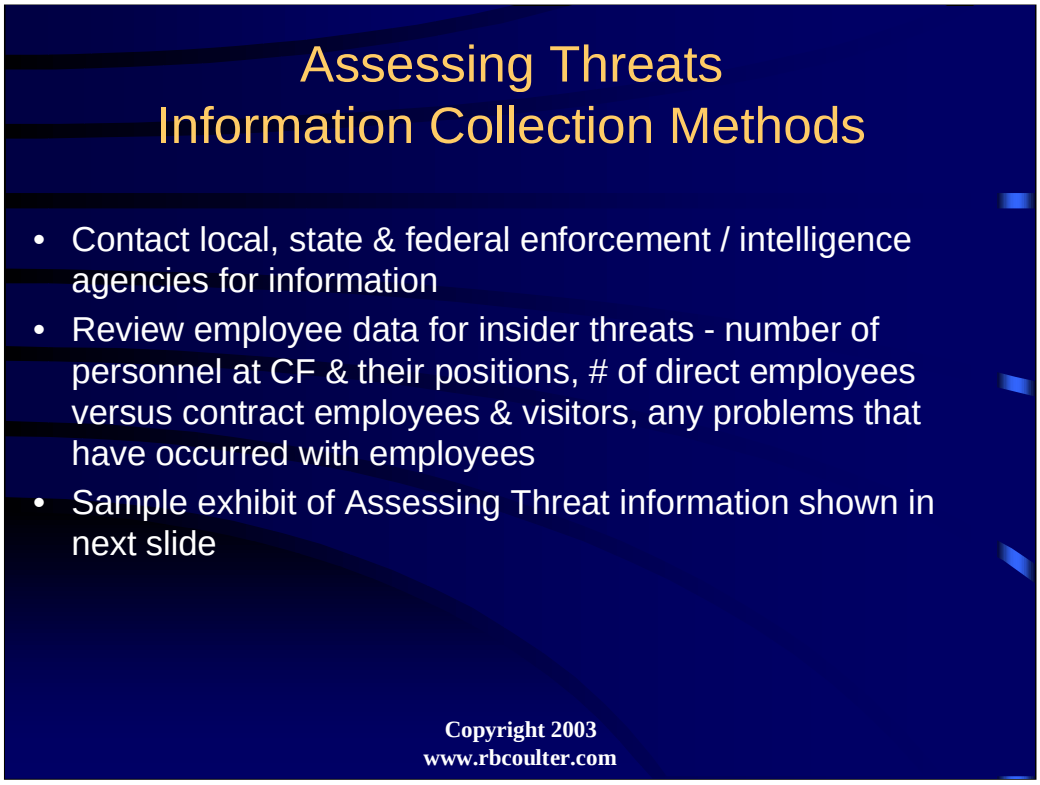
In general, there are three types of adversaries - outsiders, insiders & outsiders in collusion with insiders. Outsiders include terrorists, criminals, & extremists.

Insiders include hostile or psychotic employees.

Potential actions - These are the crimes adversaries are likely to commit (for example, theft, destruction, violence & bombing)

Adversary motivations - This is usually one of the following - ideological (political or religious) reasons, economic or personal motivation (power seeking).

Adversary capabilities - This is the number of attackers, types of weapons / tools, means of transport, technical skills, knowledge of the CF, and access to insider assistance.



Typically, CF personnel are not very knowledgeable of outside threats. Local, state & federal enforcement / intelligence agencies should be contacted for assistance in obtaining this information.

CF personnel may have a better understanding of possible insider adversaries. Review employee data for insider threats. Look at the number of personnel at the CF & their positions, # of direct employees versus contract employees & visitors. Try to find any problems that have occurred with employees that may lead to a threat to the CF.

The threat information can be organized in table form as indicated in the next slide.

Assessing Threats
Information Collection Methods

Exhibit 8. Sample Site-Specific Threat Description

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

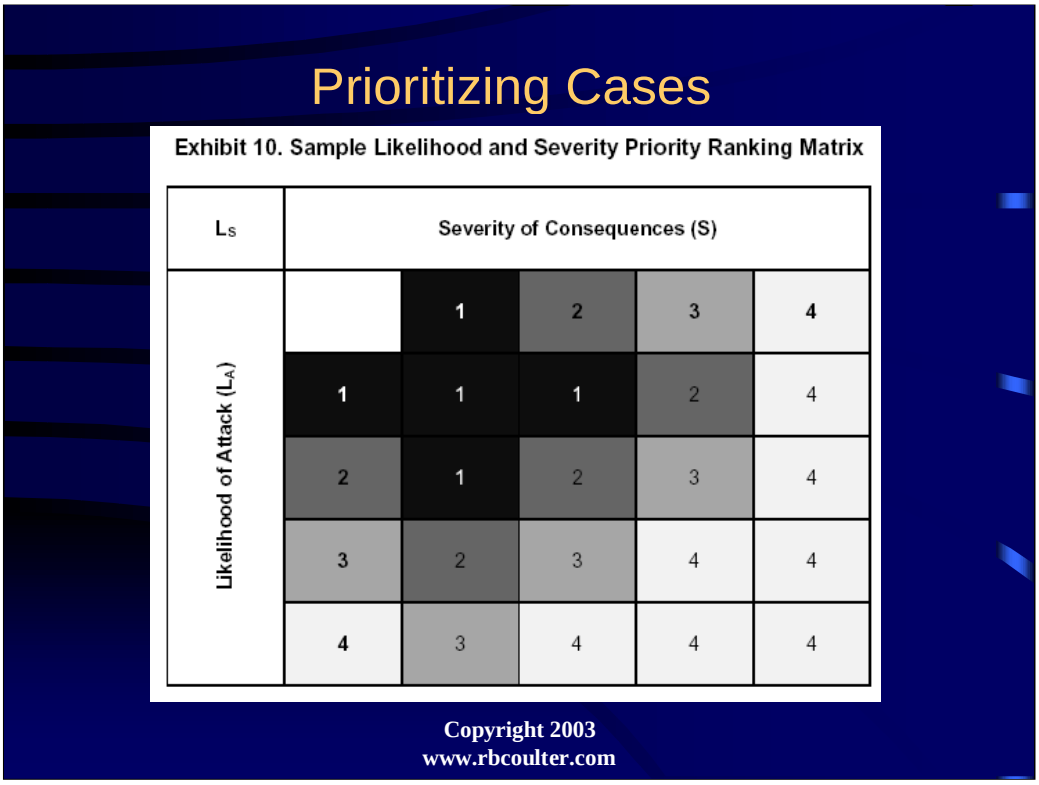
The above is threat description table showing the types of adversaries that could threaten a CF. This should help the VA leader in determining the "threat level" of an adversary. The first column is the type of adversary considered. The attributes / characteristic of the adversaries are listed in the other columns.

Assessing Threats
Definitions of Level of Likelihood of Attack (La)

Exhibit 9. Definitions of Level of Likelihood of Attack (L_A)

L_A	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.

At this point the VA leader should be able to specify a table that indicates the relative rank of threat, La, (or likelihood of attack) to the CF. The above is a sample table defining the La values that can be associated with a specific adversary. Later, the La values will be used with other parameters (severity, likelihood of success) to determine the risk to a CF or its processes.



The VA leader can now use the severity (S) values & La (likelihood of attack) values to compute the Ls values for certain events or scenarios. The Ls value is basically the "risk of an attack" and does not consider if the adversary is actually successful. If a scenario / adversary pair indicates 1, 2, or 3 on this table then the VA leader may want to examine the physical protection system (PPS) associated with the applicable activity or process. If a 4 value is computed, then the VA leader may deem that the attack risk is low & that the PPS need not be reviewed for that activity or process.

If the previous Ls screening indicated a high attack risk for a particular process / activity then the Physical Protection System (PPS) system needs to be analyzed. An Las (or likelihood of adversary success) value can then be determined. This is matrixed with Ls to determine overall risk. Site Analysis is basically an objective means of determining PPS effectiveness and the overall risk.

The basic elements of site analysis are:

Physical Protection System

Protection in Depth

Minimum Consequence of Component Failure

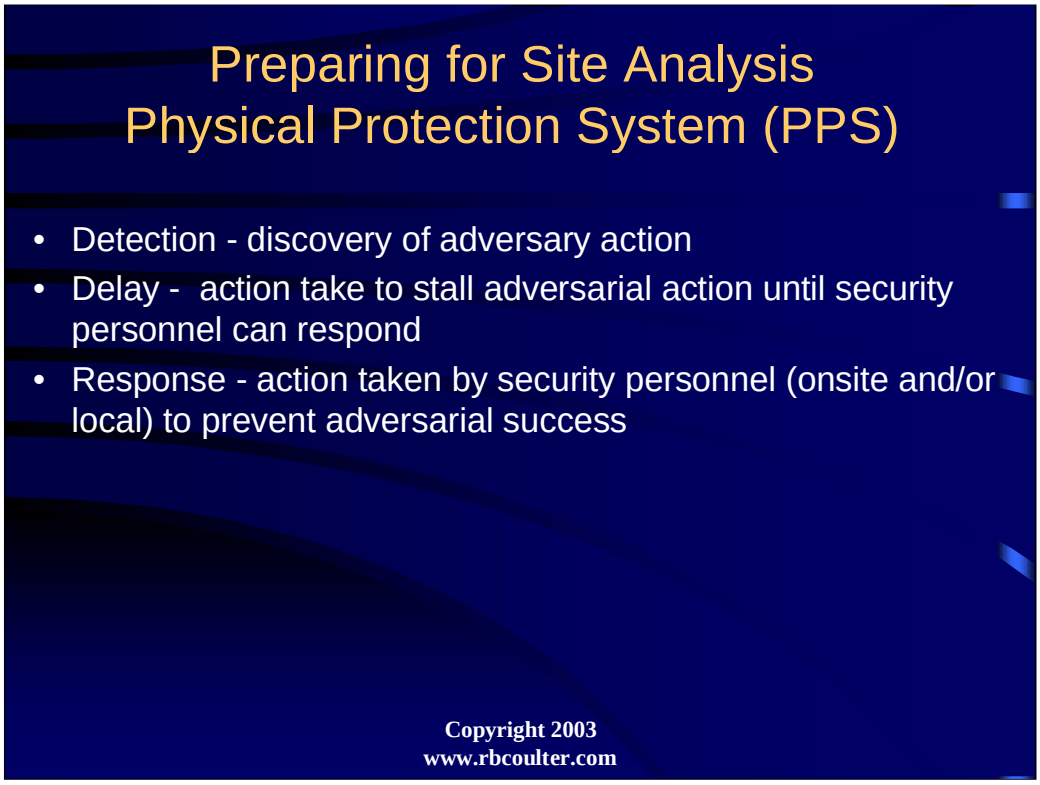
Balanced Protection

Determination of Las

Protection System for Process Control

Mitigation

Risk Priority Ranking Matrix



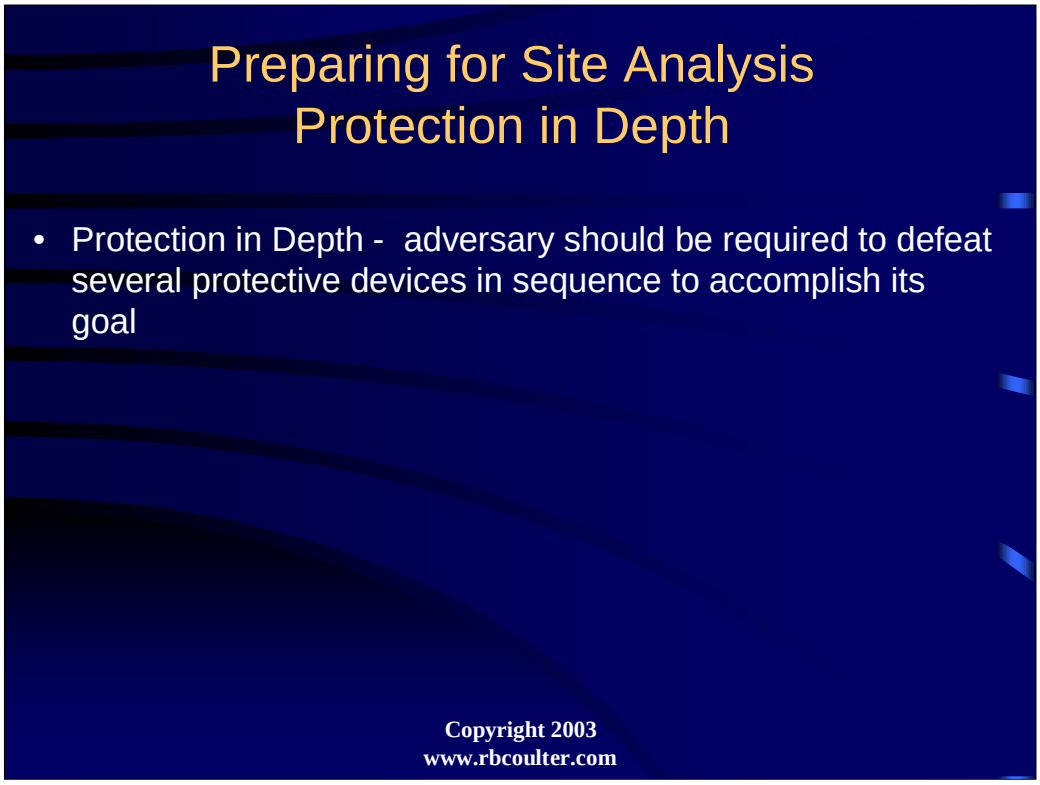
An effective PPS system would have the following traits:

Detection - This is the ability to discover adversarial action. Good detection occurs early and is reliable. Detection devices include security cameras, motion sensors, etc.

Delay - This is the action taken to stall adversarial action until security personnel can respond. Delay devices include walls, locks, barricades, etc.

Response - This is the action taken by security personnel (onsite and/or local) to prevent adversarial success.

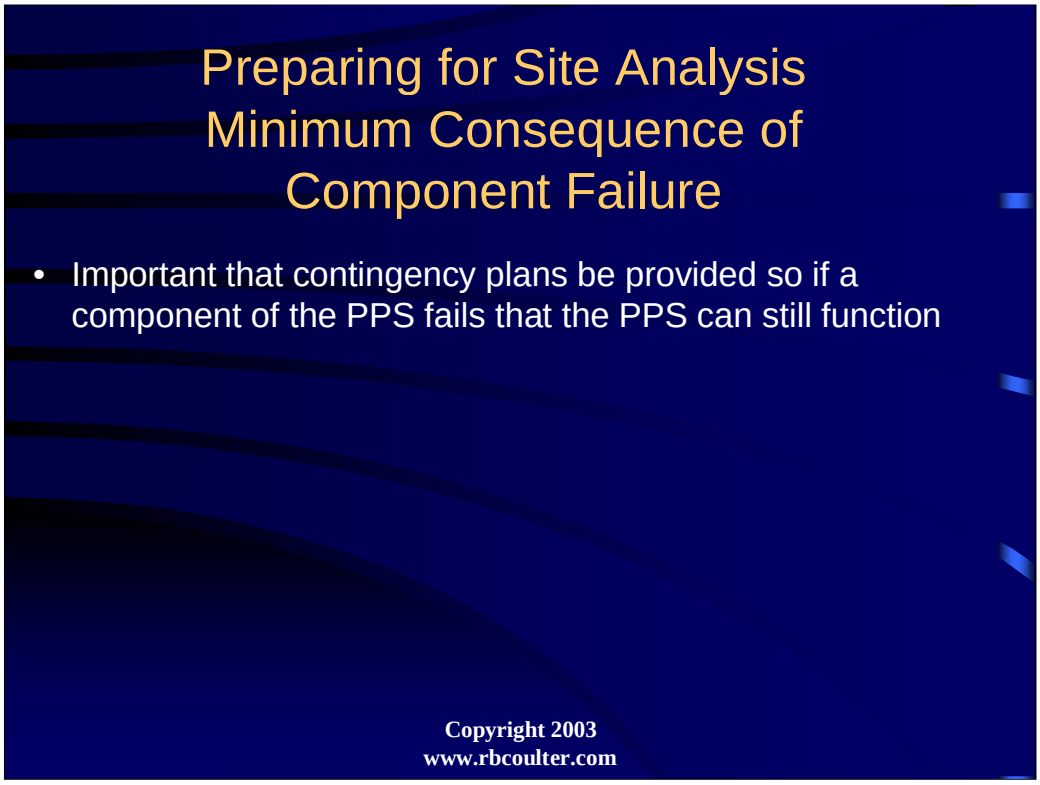
A process / activity with few or none of the above PPS traits would enhance an adversary's success rate. A process/ activity with all or nearly all of these PPS traits would minimize an adversary's success rate.



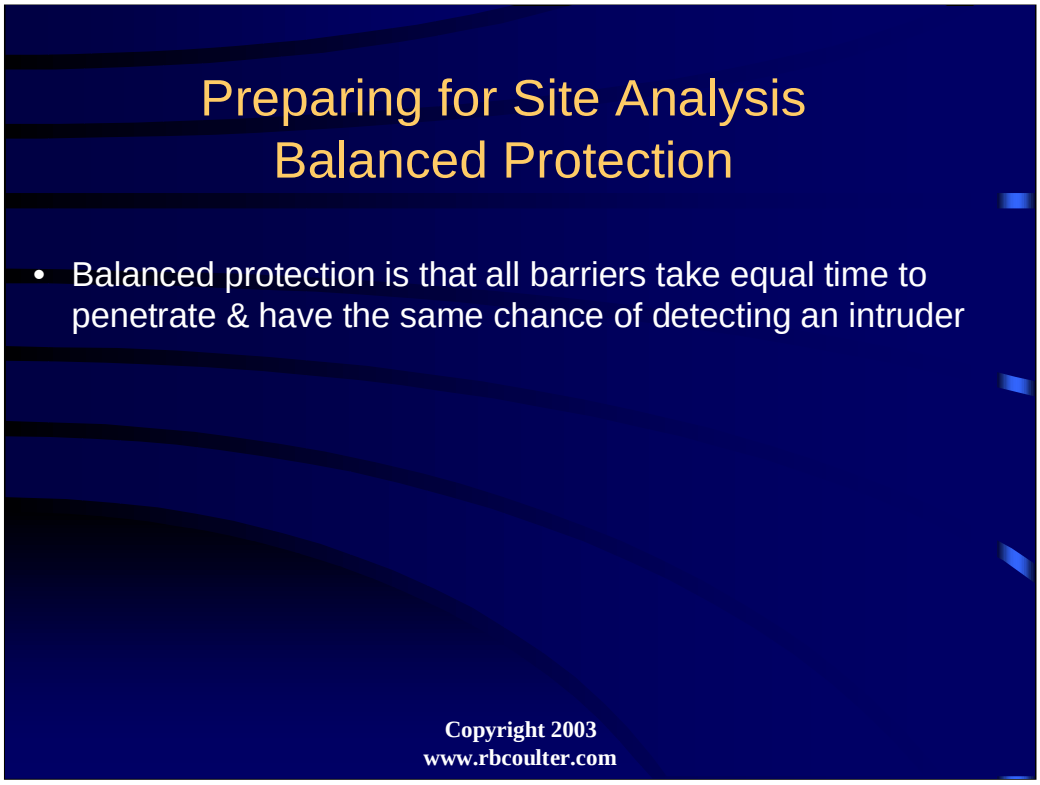
Protection in depth is a PPS feature where the adversary is required to defeat several protective devices in sequence to accomplish its goal. Protection in depth is obviously a desired train in PPS system. Its presence should allow a higher Las rank to be assigned to a PPS system. An example of protection in depth might be as follows:

For an intruder to reach a chemical tank with an outside truck the following must be breached or passed:

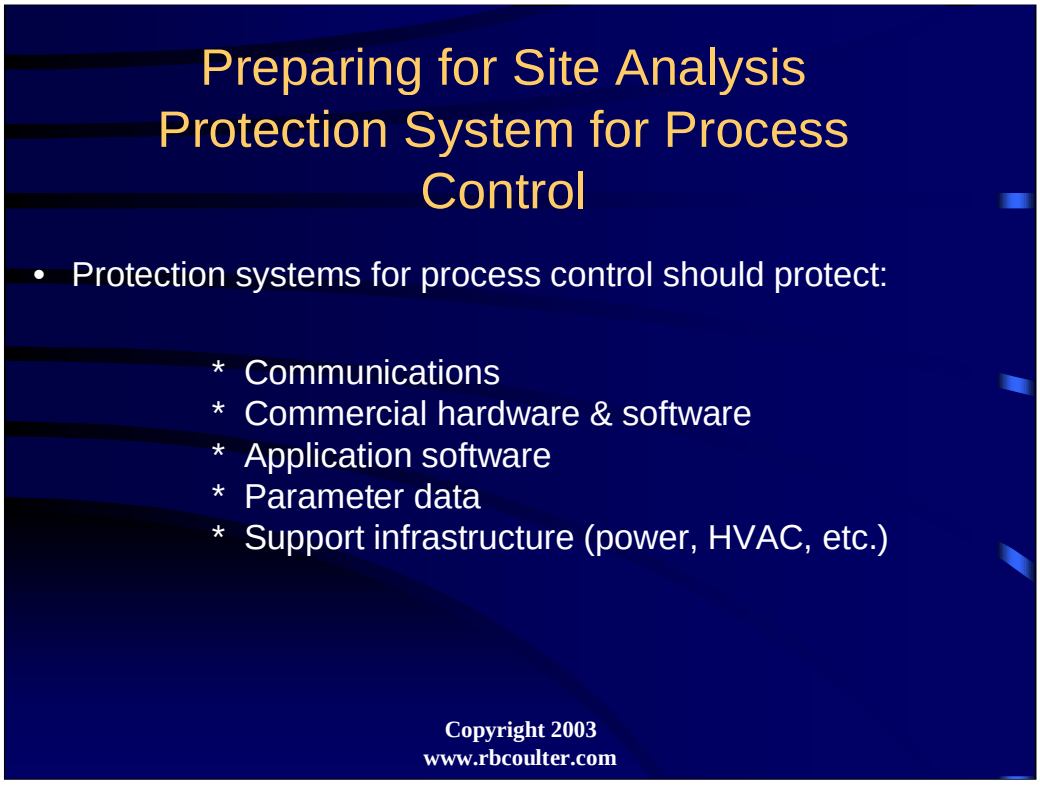
1. Guard at the CF gate.
2. Locked gate at the chemical storage area gate.
3. Dike around the chemical tank.



Another important trait is “minimum consequence of component failure”. A PPS should not be completely defeated by knocking out one component. For example, an alarm system for an entire CF should not be controlled by a central computer if disabling that computer eliminates all protection. A more robust system would allow for some degree of local function or alarm capability if the main computer is disabled by an intruder.



Balanced protection is that all barriers take equal time to penetrate & have the same chance of detecting an intruder. This is another characteristic of a well designed PPS.



Protection systems for process control should address the following:

* Communications -
* Commercial hardware & software
* Application software
* Parameter data
* Support infrastructure (power, HVAC, etc.)

Some questions that should be asked about the soundness of a process control system's (PCS) protective features is:

1. Is programming access to the PCS protected by strong passwords (random letters & digits, not words or names)?

2. Is dialup programming access to the PCS really needed? If dialup is needed, is the firewall around the PCS sufficient?

3. If the main PCS computer is disabled, will other elements of the PCS still operate to prevent or mitigate a scenario?

4. Is programming access limited to only those whose job function is programming the PCS?

5. Is software & data screened for possible viruses or trojan horses that could compromise the system?

6. Can the PCS cause an undesired scenario if it subject to a denial of service attack?

Mitigation is the post action taken to minimize consequences of an attack.

The effectiveness of mitigation systems is a factor in adversarial success if the PPS fails. Some of the mitigation systems that should be reviewed are as follows:

1. Dike & containment systems around storage & processes using applicable hazardous substances.

2. Sprinkler, foam & fire suppression systems

3. Emergency response procedures, emergency notification procedures, & evacuation procedure

The possibility that adversaries can disable mitigation systems must also be considered.

Preparing for Site Analysis Determination of Las

- Las (likelihood of success) is a function of PPS effectiveness

Exhibit 11. Sample Definitions of Likelihood of Adversary Success (L_{AS})

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.

At this point, the VA leader should have consider the traits of the PPS (including process control & mitigation) in relation to specific scenarios or potential events. The above table can then be used by the VA team to rank the PPS system and determine the Las (likelihood of adversary success values). The VA leader may choose to develop a custom Las definition table instead of using this one.

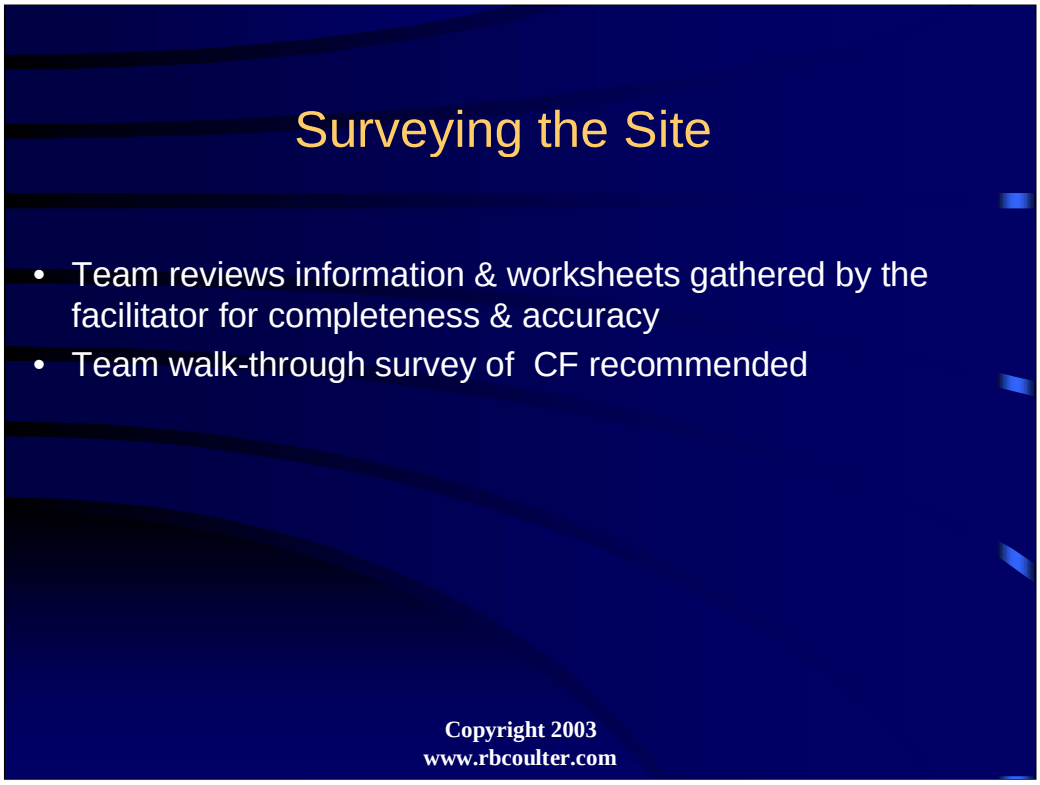
Preparing for Site Analysis
Risk Priority Ranking Matrix

- At this point, a risk priority ranking matrix can be prepared for a process or facility that ranks the risk of an attack
- Risk = f (Las, Ls)

Exhibit 12. Sample Risk Priority Ranking Matrix

Risk	Likelihood of Adversary Success (L_{AS})				
Likelihood and Severity of of Attack (L_S)		1	2	3	4
	1	1	1	2	4
	2	1	2	3	4
	3	2	3	4	4
	4	3	4	4	4

After deciding on the definition table for the Las (likelihood of adversarial success) values then the final matrix table for calculating risk (R) must be made. The above is a sample matrix table that can be used to determine the risk of a scenario. The VA team will later use this table for calculating the risk of scenarios that were 1,2, or 3 on the Ls screening.



The VA leader as now completed the background assessment for the facility's & its critical processes & activities. Definition matrix tables have been defined. The VA team now reviews the information & worksheets gathered by the facilitator for completeness & accuracy.

A VA team walk-through survey of the CF is recommended to ensure the information is correct.

The VA team can estimate the Las (likelihood of adversary success) by following these steps (which will be discussed in more detail in the slides to come).

Most Vulnerable Adversary Scenario - A Physical Path

Physical Protection Features for Scenario

Likelihood of Adversary Success for Scenario - Physical

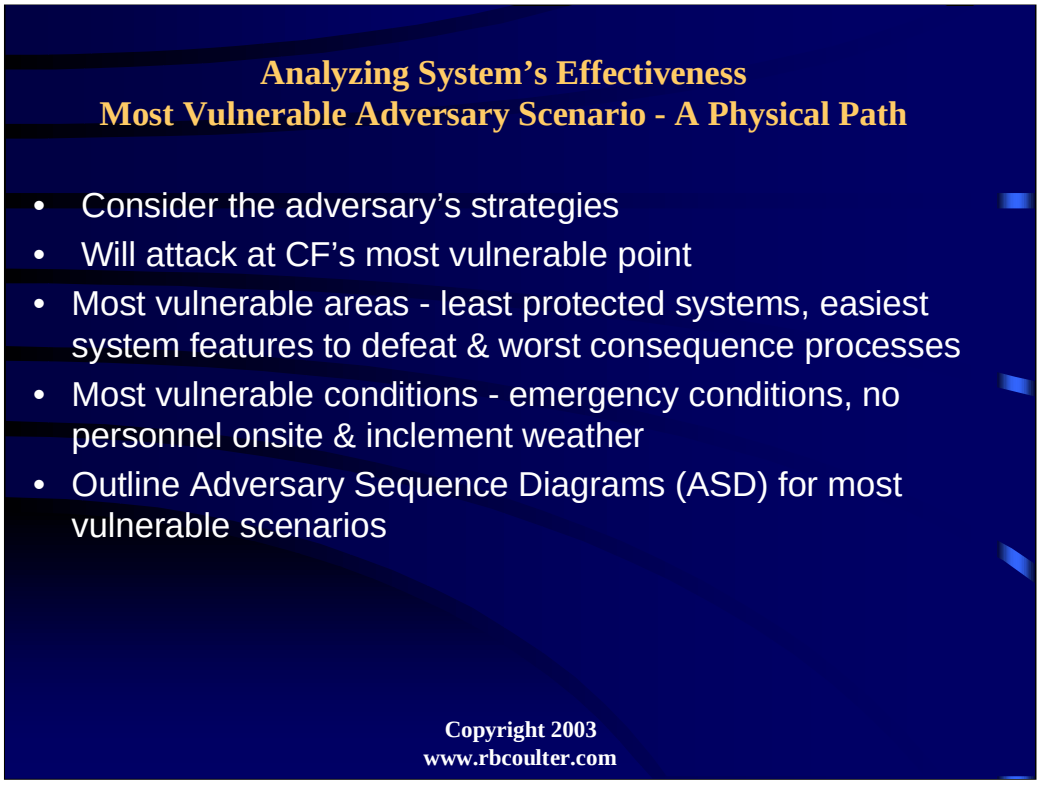
Most Vulnerable Adversary Scenario - A Process Control Path

Protection for Process Control Scenario

Likelihood of Adversary Success for Process Control Scenario

Note that the VA team will be examining a hypothetical attack on the physical system directly and a hypothetical attack on the process control system.

The team should consider both the ability to prevent the attack and the ability to mitigate the consequences if the attack occurs.



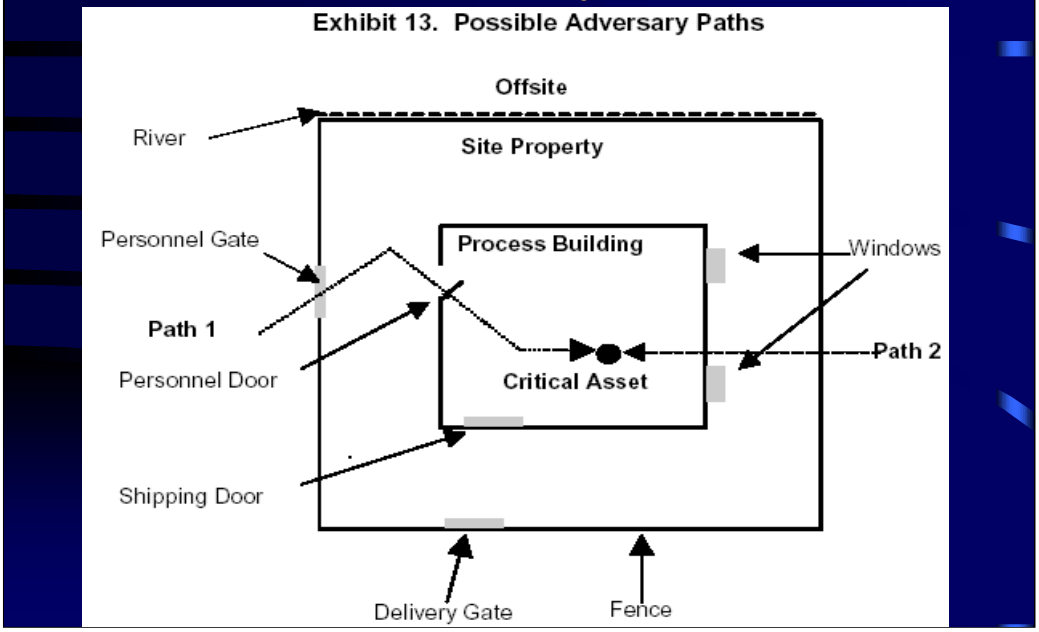
Consult exhibit 8 (the threat descriptions) and consider the adversary's strategies. In all likelihood the adversary will attack at the CF's most vulnerable point. Focus the VA team's attention here.

The most vulnerable areas have the least protected systems, the easiest system features to defeat and/or the worst consequences.

The most vulnerable times or conditions are during emergency conditions, when little or no personnel are onsite and/or during inclement weather.

Have the team outline an Adversary Sequence Diagrams (ASD) that indicates the path and steps involved in the most vulnerable scenarios. An ASD is a flow chart that indicates all known paths that an adversary may take to a critical asset.

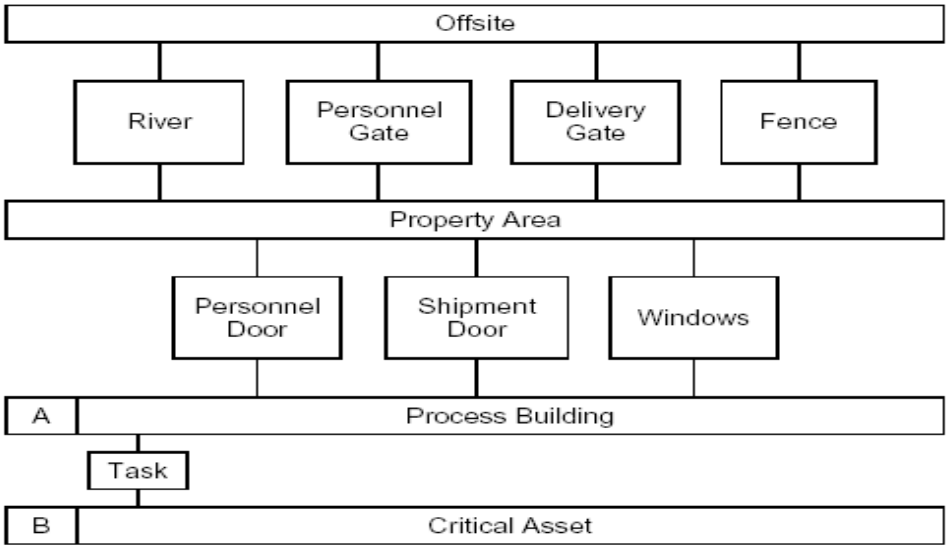
Analyzing System's Effectiveness
Most Vulnerable Adversary Scenario - A Physical Path
Possible Adversary Paths



To assist in preparing an ASD, try creating a plot plan showing the area surrounding a critical asset. The above is a sample plan indicating two possible paths to a critical asset. One route is through the main entrance & the other route is through the windows. The VA team should try to identify any other possible routes.

Analyzing System's Effectiveness
Most Vulnerable Adversary Scenario - A Physical Path ASD

Exhibit 14. Sample Facility Adversary Sequence Diagram



A possible ASD for the facility on the previous slide is shown above. Note how it clearly demonstrates multiple paths to a critical asset. The VA team at this point should be able to identify the most vulnerable scenarios.

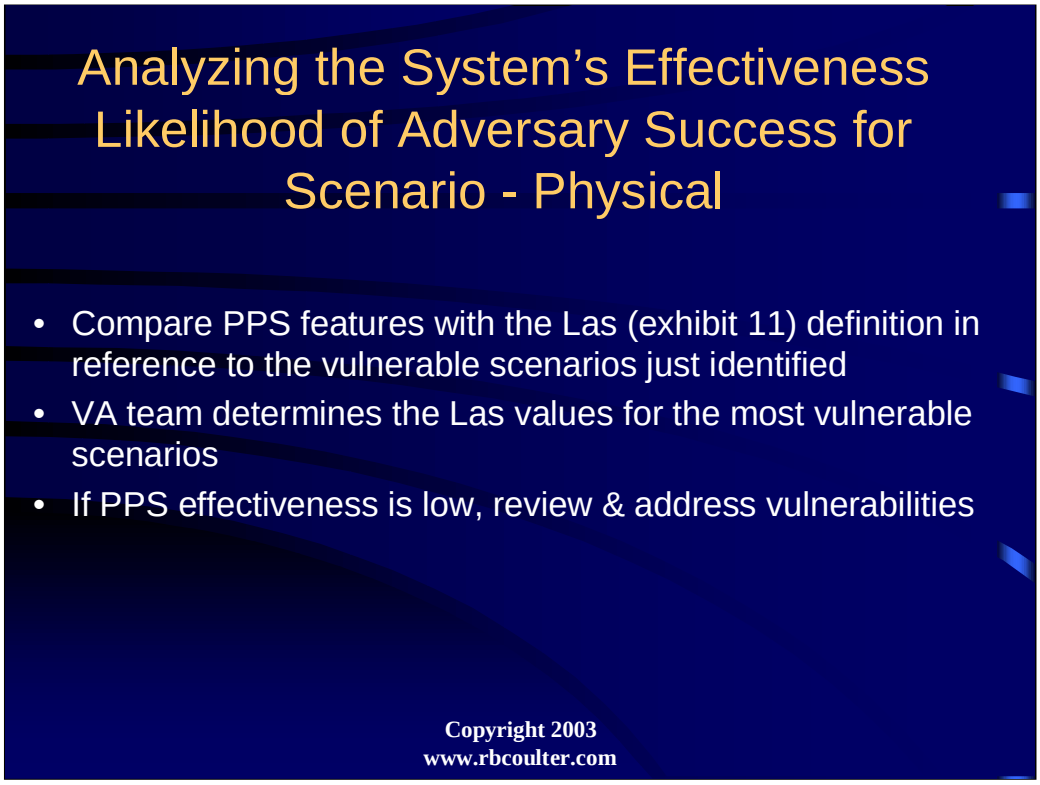
Analyzing System's Effectiveness
Physical Protection Features for Scenario

Exhibit 15. Sample Scenario and Protection System Features

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

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

To assist the team in grading or ranking the Las values of the most vulnerable scenarios, the PPS features of these scenarios can be tabulated as shown above in exhibit 15.



Compare PPS features with the Las definition (exhibit 11) for each vulnerable scenario to determine risk. Score an Las (likelihood of adversary success) for each scenario.

If Las values are low (1,2,3 for example) then the team may want to review & address the PPS vulnerabilities & document a recommendation at this point in the analysis.

The analysis of the process control path vulnerabilities is similar to the physical path except that it occurs in the "cyber" world. Passwords are like locks. Firewalls are like guard stations, etc. The VA team may want to bring in IT or process control experts at this point in the analysis. The VA team can examine the process control adversary paths (exhibit 4) for the most vulnerable scenarios.

The team should consider the ability of the process control system to mitigate consequences (for example, fail/safe feature or distributed control where parts on the control system would still function if other parts are disabled).

Analyzing the System's Effectiveness Protection for Process Control Scenario

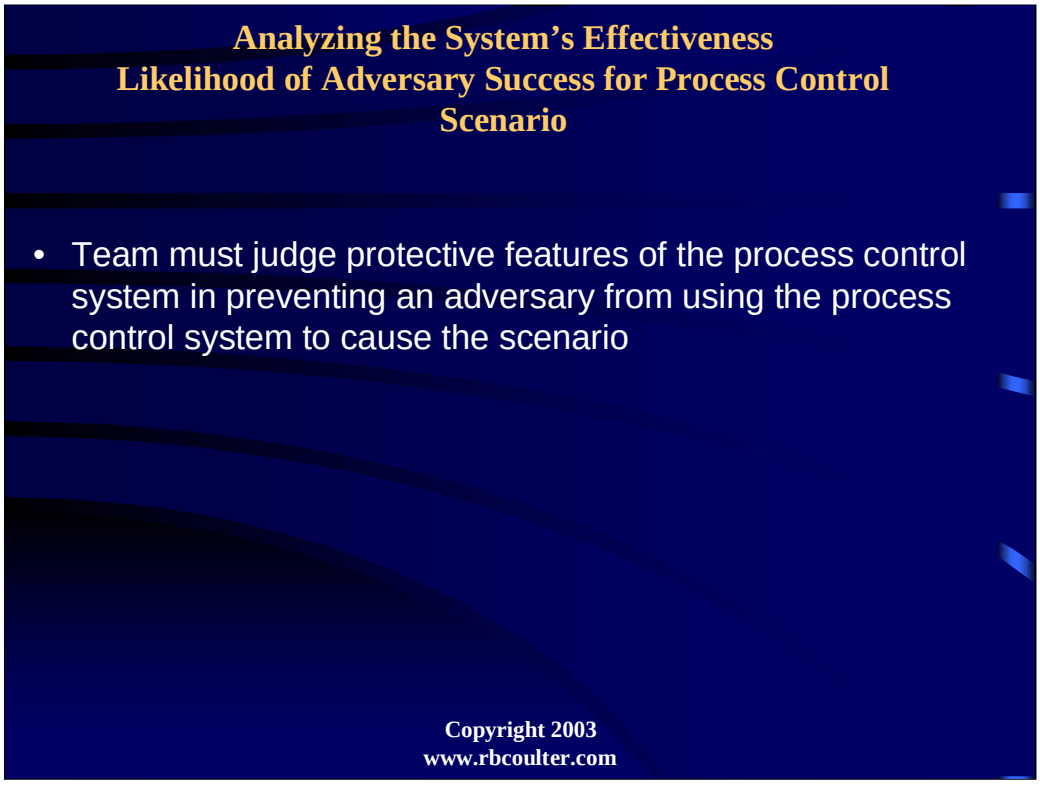
- Features of process control system that could affect the outcome of a scenario should be noted

Exhibit 16. Sample Process Control Protection Features

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

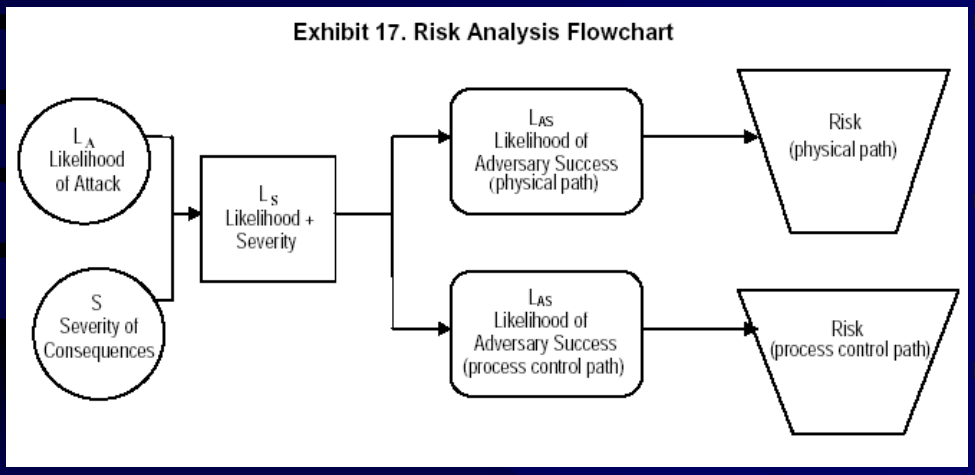
Communications	Commercial Hardware and Software	Application Software	Parameter Data	Support Infrastructure
• Encryption • Lock and sensor communications rooms • Supervised lines • Authentication • Redundant systems	• Current security patches • Strong passwords • Audits • Monitoring unusual use	• Configuration 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

Features of process control system that could affect the outcome of a scenario should be noted. The VA team should now be able to identify the most vulnerable process control scenarios. (Note the similarity of this diagram to the PPS diagram for the vulnerable scenarios in the physical path.)



Team must judge protective features of the process control system in preventing an adversary from using the process control system to cause a scenario. Assign Las values to the vulnerable process control scenarios as one done for the physical path scenarios.

Analyzing Risks



The above flow chart shows the calculation path that leads to determining the risk of scenario(s). Note that risk calculation paths for a direct physical attack & a process control attack are shown.

Analyzing Risks

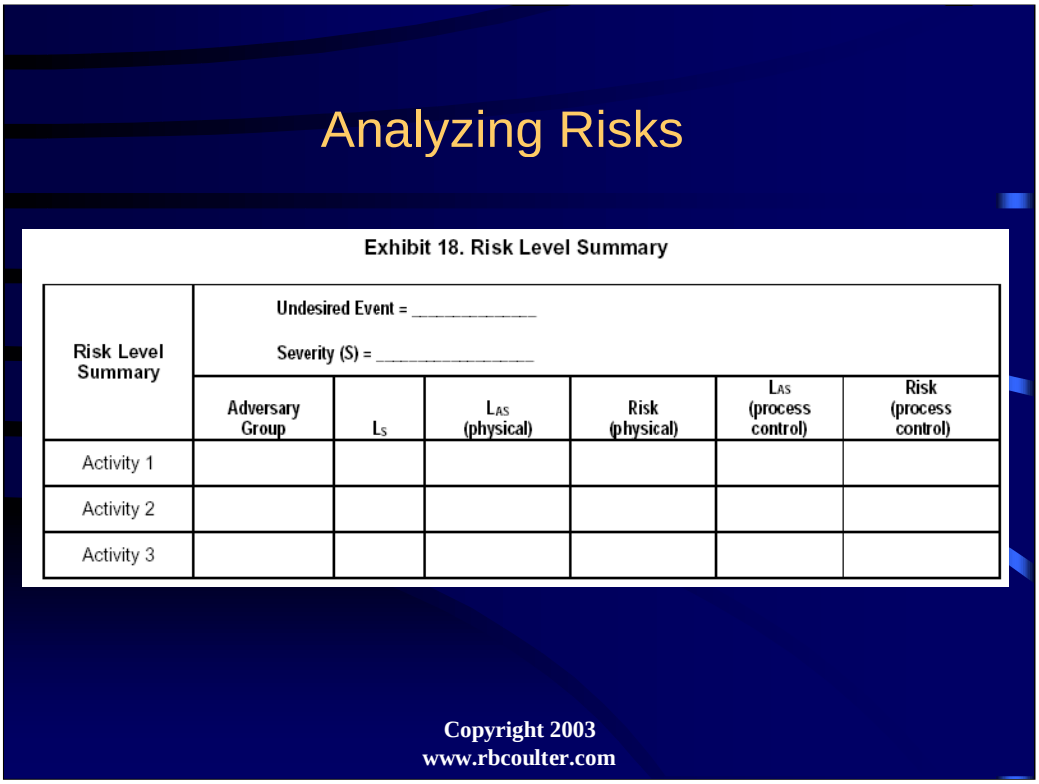
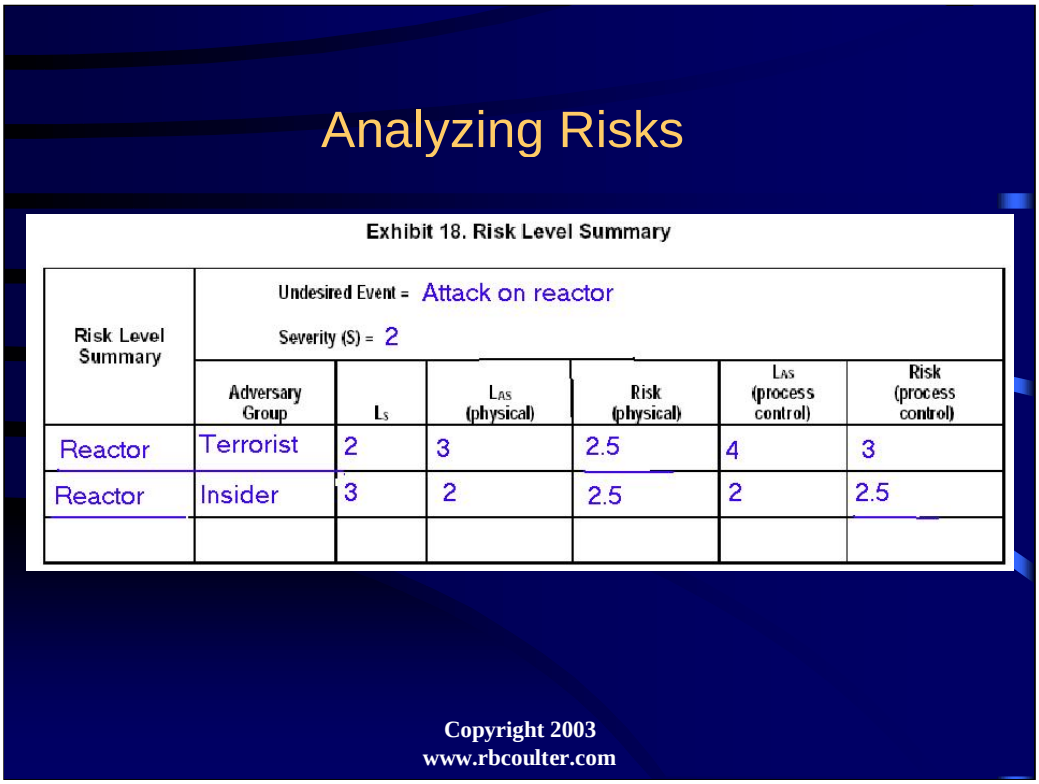


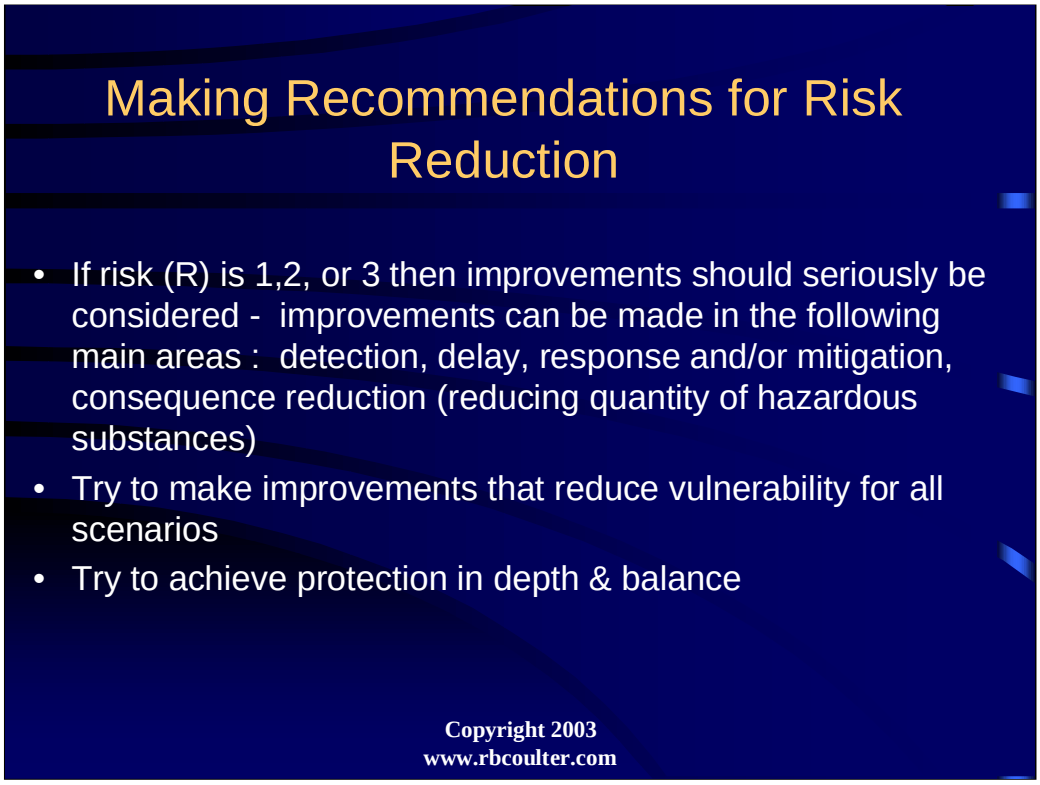
Exhibit 18. Risk Level Summary

Risk Level Summary	Undesired Event = _____ Severity (S) = _____					
	Adversary Group	L_S	L_{AS} (physical)	Risk (physical)	L_{AS} (process control)	Risk (process control)
Activity 1						
Activity 2						
Activity 3						

The actual values or scores of the various VA parameters determined for the analyzed scenarios can be summarized in a chart as shown above. The important values are the risk numbers (both physical and process control).



The above is how the VA team may enter values in to the Risk Level Summary table. The above may have been scenarios that made it through the VA leader's initial screening when the Ls (threat risk) was calculated for these scenarios. This analysis shows the insider having a greater threat to the control system & the terrorist having a greater threat by physical means.



If risk (R) is 1,2, or 3 then improvements should seriously be considered - improvements are usually made in the following main areas : detection, delay, response and/or mitigation, consequence reduction (reducing quantity of hazardous substances)

Some effective guidelines for reducing risk are:

Try to make improvements that reduce vulnerability for all scenarios. (For example, installing a facility wide intruder alert system)

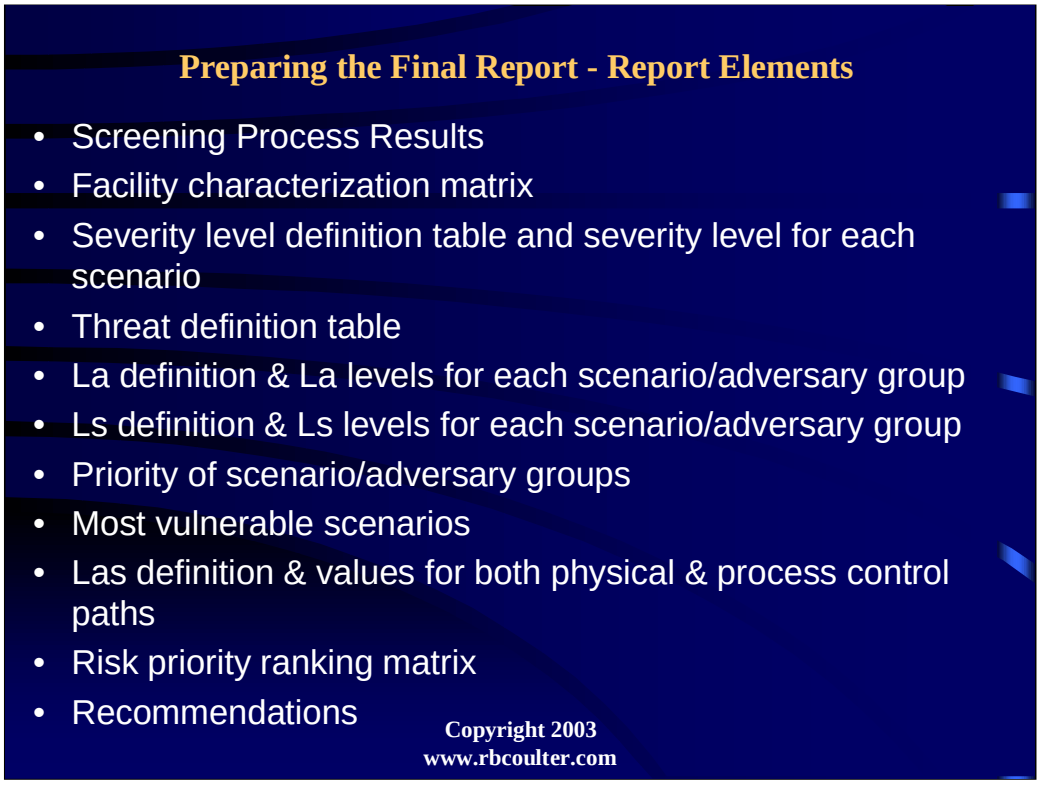
When considering changes to the PPS, try to achieve protection in depth (multiple barriers that attackers must overcome) & balance (the barriers take equal time to overcome).

The following are more specific areas that a VA team may want to consider for recommendations to reduce risk:

Physical Protection Improvements - sensors, cameras, security alarm stations, hardened doors/locks, access “PIN” control, compartmentalized facility

Consequence reduction improvement (mitigation) - Reduction in quantity or toxicity of hazardous substances, dispersion of substances or reducing the quantity of substances in one location, dikes, etc.

Process Control protection improvements - chemical process sensors, strong passwords, electronic firewalls, virus protection, encryption / authentication, emergency backup, redundant communication, process control isolated from external information system



The VA leader or appointed person should summarized the team's findings in a final report. The final report may include the following items (or summaries of each):

Screening Process Results

Facility characterization matrix

Severity level definition table and severity level for each scenario

Threat definition table

La definition & La levels for each scenario/adversary group

Ls definition & Ls levels for each scenario/adversary group

Priority of scenario/adversary groups

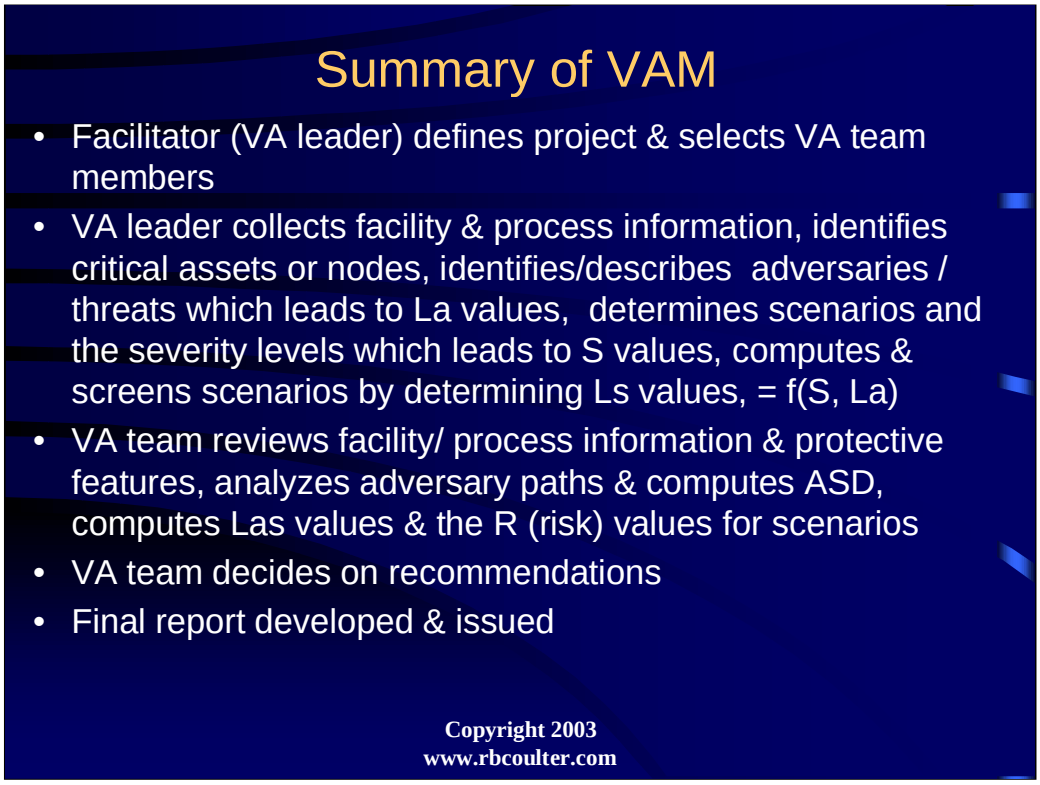
Most vulnerable scenarios

Las definition & values for both physical & process control paths

Risk priority ranking matrix

Recommendations

Recommendations should be routed through a recommendation resolution system to ensure their likelihood of being resolved.



The following is a brief summary of the VAM:

The facilitator (VA leader) defines the project & selects the VA team members.

The VA leader collects facility & process information, identifies critical assets or nodes (chemical storage tanks, pipes, reactors, etc.), identifies/describes adversaries / threats which leads to La (likelihood of attack) values, determines scenarios and the severity levels which leads to S values, and then computes & screens the scenarios by determining Ls (threat risk) values, = f(S, La).

The VA team reviews the facility/ process information & protective features, analyzes adversary paths & computes ASDs. Finally, the VA team computes Las values & the R (risk) values for the scenarios.

VA team decides on recommendations to reduce the CF vulnerability risk.

The final report is developed & issued.