Chemical
SAFETY AND SECURITY TRAINING

Aspects of Chemical Security
Dual-use Chemicals

SAND No. 2009-8395P
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.

Chemical dual-use awareness

Dual use chemicals: **Chemicals used in industry or everyday life that can also be used in a manner to cause harm or injury.**

Dual-use chemical example: Pseudoephedrine

- **Pseudoephedrine is a common ingredient in cold medicines**
- **Precursor to crystal methamphetamine**
- **Recipes for conversion available on web**

Illicit Methamphetamine Laboratory

- **Clandestine meth labs in US during 2002**
  - **Caused 194 fires, 117 explosions, and 22 deaths**
  - **Cost $23.8 million for cleanup**
  - **Dumped chemicals led to**
    - **deaths of livestock**
    - **contaminated streams**
    - **large areas of dead trees and vegetation**

US DEA, http://www.deadiversion.usdoj.gov/pubs/brochures/pseudo/pseudo_trifold.htm, viewed Dec 2007

Dual use chemicals: Chlorine

- **Incidents in which chlorine gas cylinders are blown up with explosives**
  - Chlorine likely stolen/diverted from water purification plants or oil industry
  - Civilians and non-combatants injured
- **Chlorine first used in WWI as a chemical weapon**

From http://www.longwarjournal.org/archives/2007/03/al_qaedas_chlorine_w.php downloaded Jan 2008.

Dual-use chemicals: Cyanide

Therence Koh/AFP/Getty Images

- Widely used in mining and metal plating industries, but is also a well known poison
- Product tampering*
  - Tylenol capsules
    - laced with KCN
    - 7 deaths, fall 1982, Chicago, Illinois, USA
    - Led to tamper-proof product packaging
- Popular with criminals and terrorists because it is relatively easy to obtain
- K/NaCN is an Australian Group CW agent

* "Tylenol Crisis of 1982." *Wikipedia, The Free Encyclopedia.* 22 Nov 2007, 06:04 UTC. Wikimedia Foundation, Inc. 28 Nov 2007 <http://en.wikipedia.org/w/index.php?title=Tylenol_Crisis_of_1982&oldid=173056508>.

Dual-use chemicals: Rodenticides

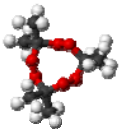
Photo/New York City Poison Control Center

- Zinc phosphide
  - Hydrolyzes to phosphine
  - Suicides in Egypt
- Anticoagulants (warfarin)
  - Suicides, attempted murder, accidental poisoning from corn meal
- Dushuqiang (Tetramethylenedisulfotetramine)
  - Rat poison banned worldwide in 1984, but still available in China
  - Three intentional poisonings in China
  - 5 other incidents reported between 1991 and 2004

Ann. Emerg. Med., Vol. 45, pg. 609, June 2005

Dual use chemicals: TATP

- Triacetone triperoxide (TATP)
- By-product, phenol synthesis
- Invisible to detectors looking for N-based explosives
- Made using acetone, hydrogen peroxide, strong acid (HCl, sulfuric)
- Favored by terrorists "Mother of Satan"
  - Sept 2009 arrest of N. Zazi, NY and Denver
  - July 2005 London suicide bombs
  - 2001 Richard Reid "shoe bomber"
  - 1997 New York subway suicide bomb plot

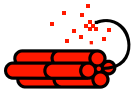


CAS 17088-37-8

Wikipedia downloaded Oct 2009
http://en.wikipedia.org/wiki/Acetone_peroxide

Dual-use Chemicals: Explosives

- Theft of conventional explosives
  - Chemical suppliers
  - Users such as mines or construction sites
- Diversion of industrial or laboratory chemicals
  - Chemical suppliers
  - Chemical factories
  - Academic teaching or research laboratories
  - Disposal sites



Dual use: Fertilizer Bomb

Photo: US DOD

- Ammonium nitrate fertilizer and fuel oil (diesel, kerosene)
- Used to bomb Alfred P. Murrah building in Oklahoma City, OK, USA
  - with nitromethane and commercial explosives
  - 168 dead, including children
  - April 1995

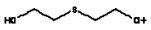
Dual use chemicals: Sodium azide

- Widely available from older automobile airbags
  - 1980s to 1990s
- Toxic by ingestion
- Reacts explosively with metals
  - Biological laboratory drains have exploded from discarded waste solutions containing NaN_3 as a preservative.
- Has been found in possession of terrorists

Dual-use chemicals: Precursors

- Dimethyl methyl phosphonate (DMMP)
  - Flame retardant for:
    - building materials, furnishings, transportation equipment, electrical industry, upholstery
  - Nerve agent precursor

- Thiodiglycol
  - Dye carrier, ink solvent, lubricant, cosmetics, anti-arthritic drugs, plastics, stabilizers, antioxidants, photographic, copying, antistatic agent, epoxides, coatings, metal plating
  - Mustard gas precursor



- Arsenic Trichloride
  - Catalyst in CFC manufacture, semiconductor precursor, intermediate for pharmaceuticals, insecticides
  - Lewisite (Agent L, Schedule 1 CWC) precursor

From: Chemical Weapons Convention: Implementation Assistance Programme Manual (on CD)

Diversion of industrial / laboratory chemicals: Bali bombing

- Amrozi purchased chemicals used to make bombs
- One ton of potassium chlorate* purchased in three transactions from the Toko Tidar Kimia fertilizer and industrial chemicals store in Jalan Tidar, Surabaya, owned by Sylvester Tendean.
  - Claimed he was a chemical salesman.
  - Obtained a false receipt saying he purchased sodium benzoate.
  - Tendean lacked proper permit to sell this chemical, didn't know the chemical would be used to make a bomb.
- Details of Aluminum powder purchases not known

* Some press reports state potassium chloride, but this is clearly an error

http://www.smh.com.au/articles/2003/06/09/1055010930128.html

http://www.thejakartapost.com/news/2002/12/18/amrozi-owns-possessing-chemicals.html

International Chemical Controls

International chemical control groups

ORGANISATION FOR THE PROHIBITION OF CHEMICAL WEAPONS

Chemical weapons convention

The Australia Group

Export controls

Organization for the prohibition of chemical weapons (OPCW)

- International group headquartered in The Hague, Netherlands
  - https://www.opcw.org/index.html
- Chemical weapons convention (CWC)
  - International treaty which bans the development, production, stockpiling, transfer and use of chemical weapons
- Promotes international cooperation in peaceful uses of chemistry
- Protecting each other

OPCW: Promotes international cooperation in peaceful uses of chemistry

- Associates program
- Analytical skills development course
- Conference support program
- Research projects program
- Internship Support Program
- Laboratory Assistance Program
- Equipment Exchange Program

OPCW: Protecting each other

- Each member state can request assistance from other member states in the event of a threat or attack, including chemical terrorism
- This can take the form of expertise, training, materials, and/or equipment

Australia Group

- An informal arrangement to minimize the risk of assisting chemical and biological weapon (C&BW) proliferation.
  - Harmonizing participating countries' national export licensing measures
  - Started in 1985 when Iraq CW program was found to have diverted chemicals and equipment from legitimate trade
- 40 nations plus European Commission participate

Australia Group: Export Controls

- Controls exports of:
  - 63+ Chemical weapon agent precursor chemicals
  - Dual-use chemical manufacturing facilities and equipment and related technology
  - Dual-use biological equipment and related technology
  - Biological agents
  - Plant pathogens
  - Animal pathogens
- Includes no-undercut policy
  - Countries won't approve an export that another member country denied

Chemical
SAFETY AND SECURITY TRAINING

Chemical Transportation Safety & Security

SAND No. 2011-0547C
Sandia is a multi-program laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Introduction

- Chemical transportation
  - Safety risks
  - Security risks
- Chemical transportation risk management
- Resources

Chemical Transportation

- Chemical transportation: In-plant, local, in-country, or international transport
- Chemical transportation is an essential element in the chemical supply chain
- Globalization has resulted in:
  - Increased volume
  - Increased speed
  - Strain on transportation infrastructure

Chemical Transportation Safety Risks

- Transporting hazardous chemicals and hazardous waste
  - Risks to *people, facilities, communities,* and the *environment*
- Transport vehicle may carry both people and product
- Transport companies may outsource and consolidate hazardous materials
  - Package incompatible materials
  - Insecure packaging & improper labeling

Current Complexity in Chemical Transportation Increases Risk

- Thousands of regulated hazardous materials
- Differences in regulations by country
- Use of different hazard classes
- Different modes of transportation
  - Road, rail, air, marine, pipeline
- Multiple packaging types

Recent Chemical Transportation Safety Accidents in the U.S.

- **Road:** June 30, 2010 - two men severely burned when fuel tanker explodes on interstate highway**.**
- **Pipeline:** November 2007-12 inch liquid propane pipeline ruptured. 430,626 gallons released. Two deaths, four houses destroyed.
- **Air:** February 2006-cargo on a DC-8 destroyed in fire caused by lithium batteries on board.
- **Rail:** October 2006-23 rail tank cars derail releasing denatured ethanol. Fire resulted in evacuation of an entire town for 2 days. Soil and water contamination.
- **Rail:** August 2002-railcar unloading hose failed and 48,000 pounds of chlorine gas released. Town evacuated, no deaths or injuries. In 2005, a similar accident caused 9 deaths.

U.S. National Transportation Safety Board. http://www.ntsb.gov/

Chemical Transportation Security Risks

- **In-plant threat**
  - **Sabotage shipments**
  - **Intentional release**
    Theft
- **In-transit threats**
  - **Hijacking**
  - **Theft of materials**
  - **Sabotage**
- **Attacks on pipelines**

Photo credit: NTSB
Pipeline New Mexico, USA

http://www.phmsa.dot.gov/hazmat/security

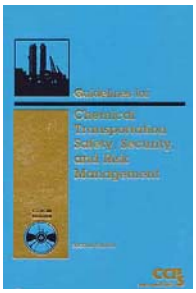
Center for Chemical Process Safety (CCPS) Risk Management Publication

- **Covers transportation safety, security and risk management**
- **Provides tools and methods to assist transportation professionals and other stakeholders**
- **Presents a comprehensive framework for managing transportation risks**
- **Introduces practical techniques for screening, identifying, and managing higher-level risks**
- **Emphasizes the need to balance safety with security**

CCPS (2008). Guidelines for Chemical Transportation Safety, Security, and Risk Management.

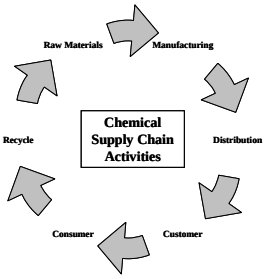
CCPS Transportation Risk Management (TRM)

- **The CCPS TRM process includes the following elements:**
  - **Primary Management System**
  - **Identification and prioritization of hazards**
  - **Risk Analysis**
  - **Risk Reduction**
  - **Program Sustainability**



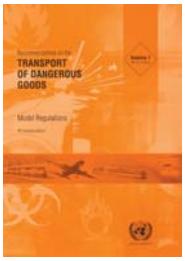
Transportation Risk Management

- Due to the complexity of many supply chains, transportation risk management is a <u>shared responsibility</u>
- Roles and responsibilities may differ for each stakeholder
- Individual activities and actions can impact the risk to the overall ***<u>chemical supply chain</u>***



Transportation Risk Management Primary Management System

- Primary Management Systems
  - Management systems should adhere to regulations and accepted international transportation standards.
    - UN Model Regulations
      http://www.unece.org/trans/danger/publi/unrec/12_e.html
    - International Maritime Organization (IMDG Code)
      http://www.imdgsupport.com/
    - International Air Transport Association (IATA)
      - Dangerous Goods Regulation, 52nd Ed.



Transportation Risk Management Primary Management System

<u>A Primary Management System Should Also Include</u>:

- Management Commitment
  - "Risk Reduction Culture"
- Policies, procedures & practices
- Emergency preparedness & response procedures
- Incident reporting system
- Management of change
- Periodic auditing of the system

Transportation Risk Management Model

Transportation risk management follows a general risk management model

1. <u>Identify and prioritize</u> the transportation safety and security hazards for your facility
2. <u>Risk Analysis</u>: Estimate the level of risk for each scenario
   Risk = f(scenario, consequence, likelihood)
3. <u>Risk Evaluation</u>: decide on the level of risk reduction
4. <u>Risk Reduction</u>: Apply mitigation (controls) to reduce the risk to the appropriate level

Examine the entire chemical supply chain

Transportation Risk Management
Identify Safety Hazards

- Identify the hazardous materials that will be transported
  - What are the physical and chemical properties of the materials?
    - Flammable, toxic, corrosive, reactive?
    - Gas or liquid?
  - Substituted with a less hazardous material?
  - How packaged, contained?

Photos: U.S. Department of Transportation

Transportation Risk Management
Analyze Potential Safety Risks

External (Accidents)

- Collisions-road, rail
- Cargo shift-road, air
- Derailment-rail
- Crash-air
- External impact-pipeline

Internal Events

- Release or spill that is not due to an external impact
- Example: equipment or containment failure

Photos: US National Transportation Safety Board
Vancouver Observer.

Transportation Risk Management
Analyze Potential Safety Risks

Potential Event Causes

- Human factors
- Equipment defects
- Corrosion
- Overpressure
- Overfilling
- Improper packaging
- Vehicle Impact
- Transportation infrastructure

Photo: US National Transportation Safety Board

Transportation Risk Management
Analyze Safety Risk

Risk = f(scenario, consequence, likelihood)

Consequence

- Fatalities/injuries
- Property damage
- Environmental damage
- Business impact/fines
- Negative media
- Distribution system disrupted

Likelihood

- Expected probability and frequency
- *CCPS Guidelines* gives likelihood estimates for:
  - Pipelines
  - Rail
  - Trucks
  - Barges
  - Ocean-going vessels
  - Intermodal transport

Analyze Safety Risk
Qualitative Methodology

Chemicals	Hazards	Potential Impacts	Risk Ranking
Chlorine	Toxic gas	Exposure to people along route	High
Ethylene Oxide	Toxic, flammable gas	Potential toxic exposure, vapor cloud, fire	High
Mineral Acids	Corrosive	Potential Environmental impact	Medium
Acrylonitrile	Flammable liquid	Potential explosion and fire	Medium

CCPS (2008). Guidelines for Chemical Transportation Safety, Security, and Risk Management

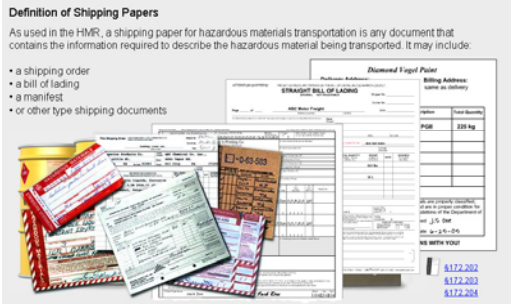
Transportation Risk Management
Risk Reduction

- **Address highest priority safety hazards first**
  - **Written procedures**
  - **Personnel training**
  - **Hazard communication**
  - **Packaging**
  - **Spill containment**
  - **Equipment inspection**
  - **Personnel protection (PPE)**
  - **Emergency response and reporting**

Transportation Risk Management
Risk Reduction

- **<u>Hazard Communication</u>**
  - **Safety data sheets**
  - **Shipping papers**
  - **Labeling**
  - **Placarding**

Transportation Risk Management
Risk Reduction



US Department of Transportation. http://www.dot.gov/

Transportation Risk Management
Risk Reduction/Packaging

Closure Requirements

Closure requirements for containers of liquid hazardous materials include:

- Close tightly and securely
- Inner packaging must remain upright
- Provide cushioning when needed
- Closed in a consistent and repeatable manner
- Closed as required by the manufacturer's closure instructions, if applicable

US Department of Transportation. http://www.dot.gov/

§172.24(a)
§172.24(a)(5)
§172.24(f)

Transportation Risk Management
Risk Reduction/Packaging

UN Standard Packagings

Packagings tested to meet the Part 178 performance requirements are called "UN Standard Packagings."

- Standards
- Package Marking Requirements

§171.8

US Department of Transportation. http://www.dot.gov/

Transportation Risk Management
Risk Reduction/Packaging

Lab Packs Outer Packaging

For lab packs, the outside packaging must be a:

- UN1A2 or UN1B2 metal drum;
- UN1D plywood drum;
- UN1G fiber drum; or
- UN1H2 plastic drum tested and marked at least for Packing Group III materials.

Metal **Fiber** **Polyethylene**

§173.12(b)(1-2)

US Department of Transportation. http://www.dot.gov/

Transportation Risk Management
Risk Reduction

Leaking or Damaged HM Packages

Repackage leaking or damaged HM packages in metal or plastic salvage drums. The drums must have a removable head. The drums must be compatible with the material.

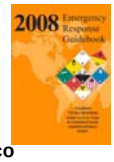
- Standards
- Markings
- Shipping Papers
- Overpack Requirements

§173.3(c)

US Department of Transportation. http://www.dot.gov/

Transportation Risk Management Risk Reduction

Emergency Response Guidebook (ERG)



- Interactive internet version:

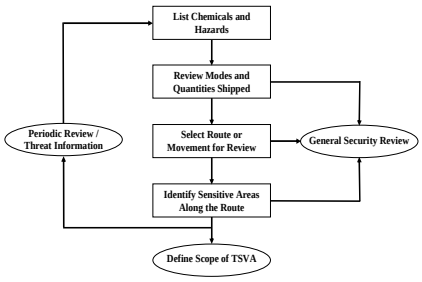
  http://wwwapps.tc.gc.ca/saf-sec-sur/3/erg-gmu/erg/ergmenu.aspx
- Developed jointly by:
  - US DOT, Transport Canada, Secretariat of Communications and Transportation Mexico
- For first responders to transportation incident
- Guide to quickly identify material classification
- Protect initial responders and public

Transportation Risk Management *Security* Risks

- Initiating event is a direct attack
- Incident magnitude is greater
  - Release size larger
  - Effect on larger population or greater environmental damage

Security Risk = *f*(C, V, T)
C = consequence
V = vulnerability
T = threat

Transportation Security Vulnerability Analysis



CCPS (2008). Guidelines for Chemical Transportation Safety, Security, and Risk Management

Transportation Security Risk Management Risk Reduction

Plant Security

- Include internal transfers in plant security plan
- Limit access to facilities and shipping information
- Secure transportation equipment
- Keep an inventory of hazardous materials
  - Use tamper resistant seals
- Personnel Security
  - Background checks
  - Identification cards or badges

Transportation Security Risk Management Risk Reduction

- In transit security threats
  - Vehicle travels on unprotected public roads, rail or sea
  - Surroundings are constantly changing
  - Sabotage or theft is not detected until in progress
  - One person responsible for transport
  - Typically there are no security personnel accompanying shipment

Photo: U. S. Transportation Security Administration

Transportation Security Risk Management Risk Reduction

- Highway Security Sensitive Materials
  - Depends on quantity and packaging
  - ~ ≥ 3000 liters in single container
    - Explosives
    - Flammable Gases
    - Anhydrous Ammonia
    - Toxic Gases
    - Flammable Liquids & Solids
    - Oxidizers
    - Water reactive
    - Corrosives
    - Radioactive, infectious substances

Credit: US TSA Highway Security Sensitive Materials

Transportation Security Risk Management Risk Reduction

High risk shipments require *high-level* controls:

- Increase possibility of detecting an attack
  - Provide for additional security personnel
  - Alarm the shipment
  - Use communication systems

Photo: http://www.securityguardcompanies.us/

Transportation Security Risk Management Risk Reduction

- Increase the possibility of delaying an attack
  - Cargo secured to vehicle
  - Immobilize vehicle
  - Hazardous material in vault
  - Locks, barriers, entanglements

Drum Cage

Photo credit: DOE NNSA Presentation, October 17-November 5, 2010

Transportation Security Risk Management
Risk Reduction

Metal Grating

Smoke Obscurant

Container Tie Down

Photo credit: DOE NNSA Presentation, October 17-November 5, 2010

Transportation Security Risk Management
Risk Reduction

Photos: TSA User's Guide on Security Seals for Domestic Cargo

Transportation Risk Management
Selection of Transportation Contractor

- Evaluation of accident history and transportation safety plans
- Safety training of personnel
- Certifications/licensing
- Condition of equipment
- Confirm the following:
  - Secure packaging
  - Shipping documentation/bill of lading
  - Labelling/placarding
  - Safety data sheets
  - Appropriate PPE for spill response
  - Spill containment kits on board
  - Emergency Contact Information on board

US Federal Motor Carrier Safety Regulations

The US FMCSA regulates:

- Driver qualifications
- Years of service
- Equipment standards
- Driving and parking rules
- Alcohol and controlled substances
- Financial responsibility
- Operational requirements

HAZMAT training required for:

- Personnel who prepare, load/unload, or transport hazardous materials.

Balancing Transportation Security with Safety

Issue	Safety	Security
Placards	Commodity information needed by emergency responders to react appropriately to an accident and minimize any impact.	Commodity information could be used by terrorists to target specific chemicals.
Rerouting	May result in more accidents if there are longer transits or the infrastructure along an alternate route may be less well maintained or contain undesirable features (uncontrolled intersections, no shoulders, etc.).	Eliminating a shipment near a specific location (most likely a highly populated or critical area) may inadvertently transfer the risk from one community to another.
Working with supply chain partners (implementing security countermeasures)	Technology can be used for both safety and security (e.g., GPS to indicate location en route, emergency response to accident, and monitoring time-sensitive chemicals/materials).	Technologies focused on security should not distract the main function of the carriers (e.g., the safe transport of chemicals from point A to B).
Risk Analysis Methods	• Rational and structured results lead to recommendations • Participation and engagement by individuals with different perspectives, roles, and backgrounds/skill sets for safety, security, and transportation • Similar methodology • Same decision metrics (guidelines)	

CCPS (2008). ***Guidelines for Chemical Transportation Safety, Security, and Risk Management***

Always expect the unexpected

Tea Break

Chemical
SAFETY AND SECURITY TRAINING

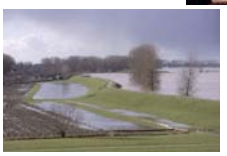
Principles of Security

SAND No. 2010-2286C
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Objectives

- Review the Definition and Objective of Security
- First Steps - Security Awareness
- Describe four Principles of Security
- Impart the importance of Performance-Based Security
- Provide a Model for a Systematic Approach to Security

What is security?



Security Definition

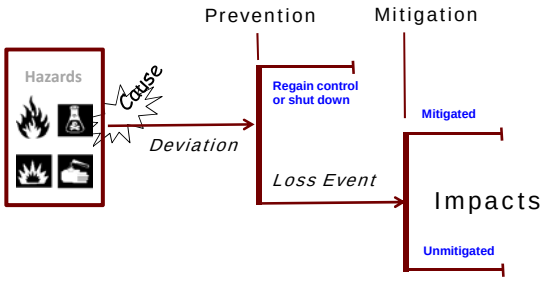
Security is:

a combination of *technical* and *administrative* controls to deter, detect, delay, and respond to an *intentional*, *malevolent* event

Security Objective

- Security intends to prevent *intentional acts* which could result in unacceptable consequences
  - Death/Severe Injury
  - Chemical contamination
    - People
    - Environment
  - Political Instability
  - Economic Loss
  - Industrial capacity loss
  - Negative public psychological effect
  - Adverse media coverage

Process Security is Similar to Process Safety



First Steps in Chemical Security: Low Cost Principles

Chemical Security Awareness
- Property-Vehicles-Information-Personnel
- Work Area - Changes
- Behavior - Suspicious
- Procedures - Followed

Access Controls
- Have (credential), Know (PIN), Are (biometric*)
- Manual (guards), Automated (machines)

* Can be expensive

Basic Security Awareness

- **Work area changes**
  - Hole in fence
  - Suspicious packages
  - Inventory discrepancy
  - Door unlocked
- **Symptoms of others behavior who are attempting to compromise security**
  - Elicitation
  - Surveillance
  - Ordering supplies

Security awareness is the first step to making your facility safe from malevolent acts

Source: DHS Chemical Security Awareness Training

Awareness- Suspicious Behaviors

- Testing security – walking into, wait for discovery
- Mapping, loitering, staging vehicles
- Taking pictures of security system
- Looking in dumpster
- Trying to enter on your credential
- Asking for user name over the phone or by email
- Asking about plant layout – workers names-schedules

Source: DHS Chemical Security Awareness Training

Security Involves Systematic Diligence- even in Small Things

- **Missing badge**
- **Leaving workstation unsecured-fire alarm**
- **Leaving sensitive document**
- **Bypassing security**

Know what to do - who to call
Communicate anything unusual to supervisor

Remember - YOU are the first responder

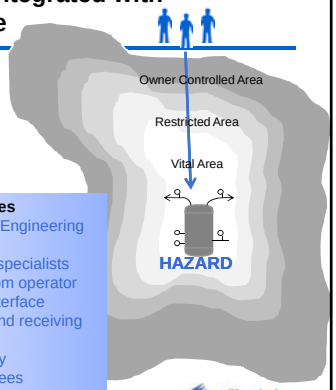
Source: DHS Chemical Security Awareness Training

Access Control Integrated with Areas and People

Plant locations
Administration
Control rooms
Server rooms
Switchgear
Process Units
Rail / truck yards
Stores

Plant employees
Administration /Engineering
Operations
- Computer specialists
- Control room operator
- Process interface
- Shipping and receiving

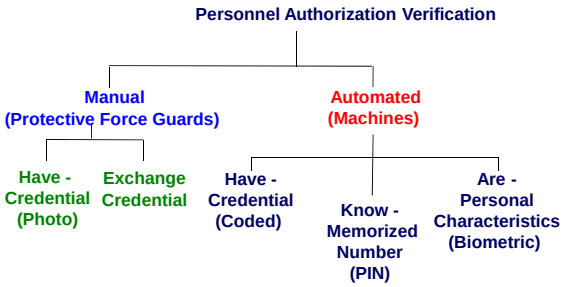
Maintenance
Security / Safety
Special employees



Features of a Good Entry Control System

- **Integration with boundary**
  - **Cannot be bypassed**
  - **Block individuals until access authorization verified**
  - **Interfaces with the alarm system**
- **Integration with the guards/response force**
  - **Protects guard**
  - **Area is under surveillance**
- **Personnel integrate with system**
  - **Easy to use for entry and exit**
  - **Accommodates peak throughput (loads)**
  - **Accommodates special cases**

Types of Personnel Entry Control



What Kinds of Chemical Facilities Need Security?

- Potential consequence severity will determine which facilities need to be secured
  - Small-scale research laboratories
    - Many different chemicals used in small amounts
  - Large-scale manufacturing plants
    - Limited types of chemicals used in large amounts

Chemical Industry Security Based on Release, Theft and Sabotage

- Risk to public health & safety release
  - In-situ release of toxic chemicals
  - In-situ release and ignition of flammable chemicals
  - In-situ release/detonation of explosives chemicals
- Potential targets for theft or diversion
  - Chemical weapons and precursors
  - Weapons of mass effect (toxic inhalation hazards)
  - IED precursors
- Reactive and stored in transportation containers
  - Chemicals that react with water to generate toxic gases

Source: DHS Chemical Security

Principles of Physical Security

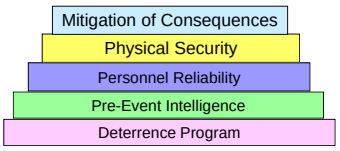
- General Principles followed to help ensure effective, appropriate security

1. Defense in Depth
2. Balanced Security
3. Integrated Security
4. Managed Risk

Principle 1: Defense in Depth

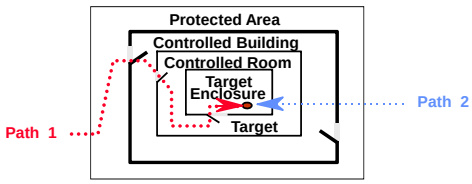
- Layers
  - Physical

  - Administrative and Programmatic



Principle 2: Balanced Protection

- Physical Layers
- Adversary Scenarios
  - Adversary paths (physical)



Balanced Protection

- Each Path is composed on many protection elements
  - Walls, fences, sensors, cameras, access controls, etc
- Protection elements each possess delay and detection components
  - For example:
    - Fence delays adversaries *20* seconds, and provides 50% likelihood that adversary is detected
    - Wall delays adversary 120 seconds and provides a 10% likelihood of detection
    - Guard delays adversary 20 seconds and provides a 30% likelihood of detection
- Balanced protection objective:
  - for every possible adversary path,
  - cumulative detection and delay encountered along path will be the similar
  - regardless of adversary path
  - NO WEAK PATH

Principle 3: System Integration

- Detection alerts Response
- Access Delay slows the adversary to provide time for Response
- Response prevents the consequence

Integrated Security

- Contribution to security system of each can be reduced to its contribution to:
  - Detection of adversary or malevolent event
  - Delay of adversary
  - Response to adversary
- Integrated security evaluates composite contribution of all components to these three elements
  - Assures that overall detection is sufficient and precedes delay
  - Assures that adversary delay time exceeds expected response time
  - Assures that response capability is greater than expected adversary

Principle 4: Managed Risk

- How much Security is enough??

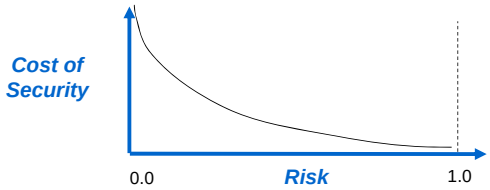
Cost of Security

Benefit of Security

Managed Risk

- Benefits of Security is Reduced Risk
- What is Risk?
  - Risk = Consequence Severity * Probability of Consequence Occurrence
- What is Security Risk?
  - Probability of Consequence Occurrence ⇒
    - Frequency of attempted event
      X
    - Probability of successful attempt
  - Probability of successful attempt is
    - 1- Probability of security system effectiveness

Managed Risk



- The benefit (risk reduction) increases with increased security investment (cost)
- However, there is a point where the increased benefit does not justify the increased cost

Managed Risk

- How much Security is enough??

Government Decision based on Managed Risk

Cost of Security

Level of Risk acceptable

Provides sufficient confidence that materials appropriately protected

Objectives

- Review the Definition and Objective of Security
- First Steps - Security Awareness
- Describe Four Principles of Security
- Impart the Importance of Performance-Based Security
- Provide a Model for a Systematic Approach to Security

Performance-Based Security

- Requirements Driven
- Engineering Principles used for Security
  - What are requirements for system?
  - What are constraints of system?

Requirements-Driven Security

- Design Constraints
  - Understand Operational Conditions
- Design Requirements
  - Consequences to be prevented
    - Identify Targets to be protected
  - Define Threats against which targets will be protected

Operational Conditions

- Characterize the facility considering:
  - Mission
  - Operations
  - Budget
  - Safety
  - Legal Issues
  - Regulatory Issues

Target Identification

- What are the unacceptable consequences to be prevented?
  - Death/Severe Injury
  - Chemical contamination
    - People
    - Environment
  - Political Instability
  - Economic Loss
  - Industrial capacity loss
  - Negative public psychological effect
  - Adverse media coverage

Target Identification

- What are possible sources of unacceptable consequences?
  - Dispersal
    - Identify areas to protect
  - Theft
    - Identify material to protect

Target Identification

- Characterize Types of Targets
  - Form
  - Storage manner and location
  - Flow of chemicals
  - Vulnerability of Chemicals
    - Flammable
    - Explosive
    - Caustic

- Criticality / Effect
- Access / Vulnerability
- Recoverability / Redundancy
- Vulnerability

Define the Threats

- The Art of War, Sun Tse
  - If you know neither yourself nor your enemies, you will lose most of the time
  - If you know yourself, but not your enemies, you will win 50%
  - If you know yourself and your enemies, you will win most of the time

Knowing your threats permits proper preparation

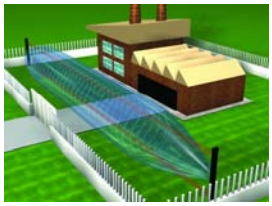
The Physical Protection System Must Have a Basis for Design

Threat Assessment: An evaluation of the threats- based on available intelligence, law enforcement, and open source information that describes the motivations, intentions, and capabilities of these threats

Design Basis Threat: A policy document used to establish performance criteria for a physical protection system (PPS). It is based on the results of threat assessments as well as other policy considerations

Define the Threats

- **In physical security:**
  - **Knowing adversary permits customizing security to maximize effectiveness**
  - **As adversary not known, develop hypothetical adversary to customize security**
  - **Hypothetical adversary description should be influenced by actual threat data**



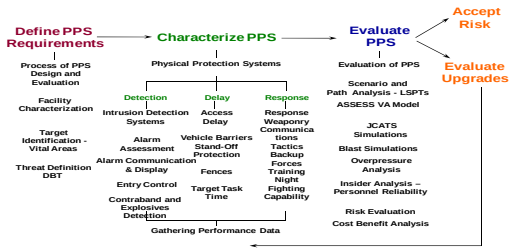
Design Basis Threat

- **A Design Basis Threat is a formalized approach to develop a threat-based design criteria**
- **Design Basis Threat (DBT) consists of the attributes and characteristics of potential adversaries. These attributes and characteristics are used as criteria to develop a customized security system design.**
- **The DBT is typically defined at a national level for a State.**
- **At the facility level, also:**
  - **Consider local threats**
    - **Local criminals, terrorists, protestors**
  - **Consider insider threats**
    - **Employees and others with access**

Objectives

- **Review the Definition and Objective of Security**
- **First Steps - Security Awareness**
- **Describe the Principles of Security**
- **Impart the Importance of Performance-Based Security**
- **Provide a Model for a Systematic Approach to Security**

Model: Design and Evaluation Process Outline (DEPO)



Detect Adversary

- Technology
  - Intrusion Detection
  - Entry Control
  - Contraband Detection
  - Unauthorized action Detection

- Supporting elements
  - Alarm Assessment
  - Alarm Communication
  - Alarm Annunciation

Delay Adversary

Delay Definition :

- The element of a physical protection system designed to slow an adversary after they have been detected by use of
  - Walls, fences
  - Activated delays-foams, smoke, entanglement
  - Responders
- Delay is effective only after there is first sensing that initiates a response

Respond to Adversary

- Guard and Response Forces

***Guards*:** A person who is entrusted with responsibility for patrolling, monitoring, assessing, escorting individuals or *transport*, controlling access. Can be armed or unarmed.

Response forces: Persons, on-site or off-site who are armed and appropriately equipped and trained to counter an attempted theft or an act of sabotage.

Guards can sometimes perform as initial responders as well (both guards and response force)

Summary

- Security systems should attempt to prevent, but be prepared to defeat an intentional malevolent act that could result in unacceptable consequences at a chemical facility
- Security awareness is an essential element
- An effective system depends on an appropriate integration of:
  - Detect
  - Delay
  - Respond

Summary

- Principles for security can lead to more effective security system
  - Defense in depth
  - Balanced security
  - Integrated security
  - Managed risk
- Performance-based approach will yield the greatest confidence that security is adequate
  - Threat criteria
- A model for systematic security design and analysis will enable application of principles and performance based approach

Chemical
SAFETY AND SECURITY TRAINING

Responsible Care
Responsible Care Security Code

SAND No. 2010-4653C
Sandia is a multi-program laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Overview

- Protecting employees, communities and assets from accidents or deliberate actions is critical to a competitive global chemical industry and to your reputation
- While different, safety and security practices combine to maximize protection of sites and supply chain
- The industry commitment is reflected through globally recognized and award winning Responsible Care programs

Responsible Care

- Global (52 countries), voluntary initiative to continuously improve and protect the environment and health, safety, and security (EHSS) of our employees and our communities
- A system to manage and publicly communicate EHSS issues - including performance measures – going *beyond* government requirements
- International Council of Chemical Associations (ICCA):
  - Responsible Care is being practiced at over 80% of the chemical industry world wide
  - Ukrainian Union of Chemists RC seminars

Securing Facilities = Good Business

- Levels of U.S. Security
  - Before 9/11/01 U.S. chemical security emphasis on:
    - Sabotage (insiders or outsiders)
    - Accidental releases, process safety and employee safety
    - Theft and diversion (for economic reasons, weapons or illegal drug manufacture)
    - Disgruntled employees (targeting other employees or company)
    - Industrial espionage (competitors stealing/spying)
  - After 9/11/01 the emphasis broadened to include terrorism
    - Prevention and mitigation of deliberate attacks on facilities added

Securing Facilities = Good Business

- ACC Responsible Care ® Security Code was approved within the U.S. Chemical industry within 6 months of 9/11/01 and provided the basis for more recent national and state regulations
- Existing employee safety and process safety principles and practices provided the platform to develop and enhance a comprehensive security code program

http://responsiblecare.americanchemistry.com/Responsible-Care-Program-Elements/Responsible-Care-Security-Code

Securing Facilities = Good Business

- Combined, the ACC Responsible Care ® Management System and addition of the Security Code have:
  - Improved security against all threats
  - Reduced waste
  - Reduced theft and diversion of our products
  - Enhanced emergency response capabilities
  - Protected vital intellectual capital and cyber systems

ACC Responsible Care® Security Code

- Driven from the CEO level at the company and focuses on three areas of security:
  - — Site
  - — Value Chain
  - — Cyber security
- Designed to protect people, property, products, processes, information and information systems
- Covers activities associated with design, procurement, manufacturing, marketing, distribution, transportation, customer support, use, recycle, and disposal of chemical products

U.S Regulations

- US Department of Homeland Security and Industry working to implement the Chemical Facility Anti-Terrorism Standards –
  - 40,000 sites assessed security risks
  - 7,000 sites were deemed "high-risk" and required to take action
- Coast Guard's Maritime Transportation Security Act regulations cover additional facilities
- These two programs are very similar to implementations made under the Responsible Care® Security Code
- Legislation from US Congress was required to implement the two Federal Programs
  - 3 of the 50 US States also have security programs in place

ACC Responsible Care Security Code Commonalities with U.S. Regulations

- Assess and prioritize risks
- Restrict access
- Prevent theft/diversion and sabotage
- Know your customer/supply chain
- Cyber/information security
- Report incidents
- Coordinate with local law enforcement and emergency response community
- Personnel surety – hire/train/retain quality people
- Verification of appropriate security actions

Basic Security Practices – Affordable and Effective

- The basis of security starts with hiring, training and retaining good employees
- Employee awareness training and drills are important elements to prevent incidents, or mitigate those that occur
- Community and employee involvement – reporting suspicious or unusual behavior or even un-ethical activities through regular or anonymous hotlines – prevents accidents, or deliberate events

Save by Limiting Theft and Diversion

Preventing theft or diversion of chemicals and process information can include a range of chemicals and activities throughout the manufacturing site and supply chain

- Chemical weapons or their precursors
- Explosives or their precursors
- Drug precursors
- Information

Preventing Theft and Diversion

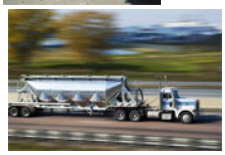
- Security starts with careful screening to hire trustworthy and qualified personnel
  - Personnel identification (e.g., photo ID checks; employee and visitor badges; biometrics)
  - Hand carried items inspection (e.g., visual inspections; x-ray inspections; metal detectors)
- Most threats occur from either inside jobs, or outsiders working with someone on the inside – stop that and your security risk will be dramatically lower
- Minimally - avoid having less qualified personnel working in highly sensitive areas and restrict access to those areas

Keep watch on critical assets

- Surveillance through guards, monitoring systems, bar code tracking etc. help manage key processes and inventory
  - lessens theft/diversion which reduces cost of stolen goods
  - Tracks products to ensure they reach the customer
  - Reduces likelihood of sabotage or employee violence

Save on Transportation - GPS

- Fleet tracking cuts costs and product losses:
  - Tracked vehicles are driven more safely, stay on time and on route
  - If diverted, tracking system allows quicker response to protect personnel and recover products
  - Valuable equipment/products can be monitored to ensure no tampering
  - Keep tabs on rail shipments



Save by Tracking Inventory

- Evaluation of up and downstream supply chain to ensure they meet your standards
- Verification of purchasers having "legitimate use" for your products
- Reviewing and auditing your distributors
- Evaluating facility and corporate cyber security – protecting processes and critical information from cyber crimes - www.chemitc.com

Cost of Inaction

- **Costs to avoid –**
  - If diverted/stolen, the average tanker truck inventory costs US $35,000, a rail car US $140,000
  - **Intellectual capital thefts could run in the millions, or eliminate your competitiveness**
  - **Public outcry over an incident hurts the industry credibility and severely damages the company's profitability**
    - **Property damage**
    - **Employee injury/death**
    - **Added regulation**

Chemical
SAFETY AND SECURITY TRAINING

Security Vulnerability Assessments

SAND No. 2011-0786C
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.

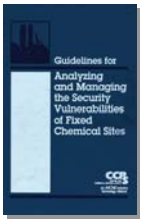
Key acronyms

SVA = *security vulnerability assessment*

PPS = *physical protection system*

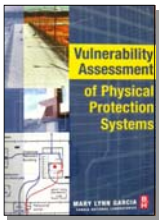
SVA resources

CCPS 2003. Center for Chemical Process Safety, ***Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites***. NY: American Institute of Chemical Engineers.



SVA resources

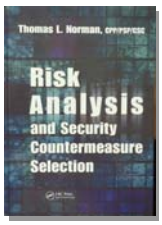
M.L. Garcia 2003. ***Vulnerability Assessment of Physical Protection Systems***. Amsterdam: Elsevier.



Also: **M.L. Garcia 2008**. ***The Design and Evaluation of Physical Protection Systems, Second Edition***. Amsterdam: Butterworth Heinemann.

SVA resources

T.L. Norman 2010. ***Risk Analysis and Security Countermeasure Selection***. Boca Raton, Florida: CRC Press.



Definition

SVA **Security Vulnerability Assessment:**

A systematic evaluation process in which qualitative and/or quantitative techniques are applied to detect vulnerabilities and to arrive at an effectiveness level for a security system to protect specific targets from specific adversaries and their acts.

Garcia 2008

Security Vulnerability Assessments

1. SVA objectives and overview
2. Identify targets and critical assets
3. Identify and assess likelihood of threats
4. Assess severity of consequences
5. Evaluate effectiveness of safeguards
6. Determine adequacy of safeguards
7. Identify and implement improvements
8. Compare with process safety

Security Vulnerability Assessments

1. SVA objectives and overview

SVA objectives

SVA **Security Vulnerability Assessment:**

A systematic evaluation process in which qualitative and/or quantitative techniques are applied to detect vulnerabilities and to arrive at an effectiveness level for a security system to protect specific targets from specific adversaries and their acts.

Ultimate goal

SVA **Security Vulnerability Assessment:**

A systematic evaluation process in which qualitative and/or quantitative techniques are applied to detect vulnerabilities and to arrive at an effectiveness level for a security system to protect specific targets from specific adversaries and their acts.

CCPS Center for Chemical Process Safety — An AIChE Industry Technology Alliance

Process Safety Beacon

http://www.aiche.org/CCPS/Publications/Beacon/index.aspx

Messages for Manufacturing Personnel

Sponsored by CCPS Supporters

Plant Security

September 2008

On this anniversary of terrorist attacks on the United States in September 2001, we remember that such attacks have occurred in many other places throughout the world, before and after the New York and Washington attacks (for example, the Tokyo subway; London; Madrid; Bali, Indonesia; Ahmedabad, India; several attacks in Russia, many incidents in various countries in the Middle East). There are few countries which have not had experience with sabotage or terrorist attack. The hazardous nature of the materials handled in the process industries requires everyone's vigilance to ensure that our plants are secure, to protect ourselves, our fellow employees, and our neighbors. If you work in a chemical storage or processing facility, you are in the best position to observe and address potential security vulnerabilities in your plant. As you go about your work, look for potential security problems, and report them to management so they can be corrected.

(continued on next slide)

Plant security is everybody's responsibility!

AIChE © 2008. All rights reserved. Reproduction for non-commercial, educational purposes is encouraged. However, reproduction for the purpose of resale by anyone other than CCPS is strictly prohibited. Contact us at ccps_beacon@aiche.org or 212-591-7319

What can you do?

As you work in the plant every day, you have opportunities to see potential security problems. Look for them, and report them. Here are a few examples, and you and your management can easily develop a much longer list:

- Security lights which are not working, or are inadequate if they are working
- Broken latches on gates or doors in the plant fence
- Loose gates, or gates with large gaps under them
- Gaps in or under fences, damage to fences, fences which are too low, erosion of the ground under fences
- Objects near fences on the outside which would assist in climbing over the fence
- Chains and locks improperly secured
- Gates, doors, or windows on the outside boundary of the plant left open, or propped open.
- Gates or doors to the outside which get stuck without fully closing

Also, you should know and follow the security procedures at your plant – for example:

- Always wear required identification badges, and, if you see somebody without proper identification, report it to your supervisor or security officers.
- Don't let other people borrow your plant access card or identification card.

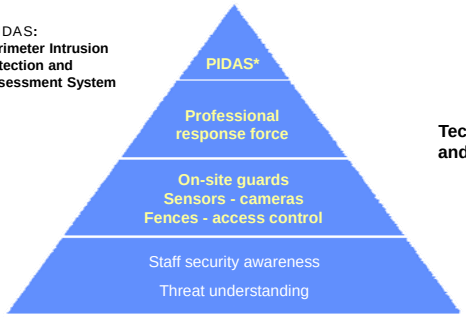
A fence overgrown with bushes and trees

Cars parked near a fence can help intruders climb the fence

A lock on the web of a chain link fence – not as strong as if chained and locked around the fence post

Higher-integrity security measures need careful design and implementation

*PIDAS: Perimeter Intrusion Detection and Assessment System



Technology and/or Cost

SVA objectives, restated

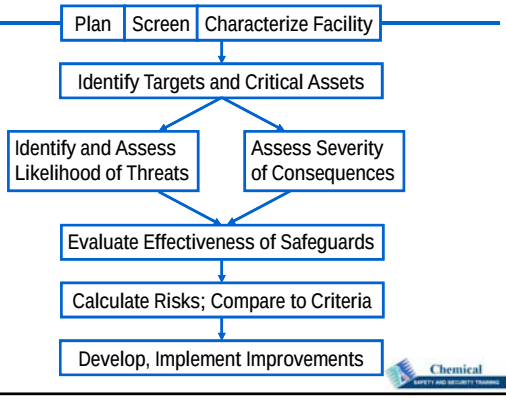
- **Detect vulnerabilities (weaknesses) in a facility's ability to protect critical assets against adversaries**
- **Design security systems to achieve a desired level of effectiveness**
  - **Physical protection systems**
  - **Cyber security protection systems**
- **Can also extend to mitigation systems**
  - **Emergency response**
  - **Fire protection etc.**

SVA overview

SVA **Security Vulnerability Assessment:**

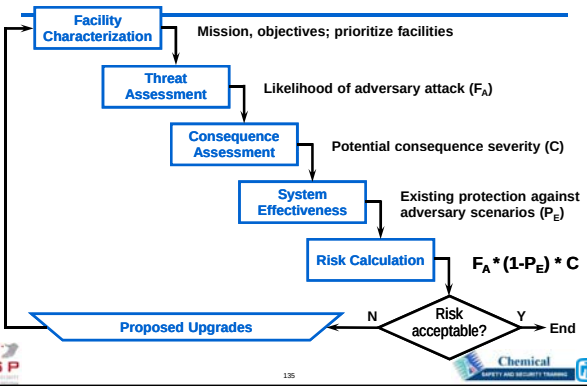
A systematic evaluation process in which qualitative and/or quantitative techniques are applied to detect vulnerabilities and to arrive at an effectiveness level for a security system to protect specific targets from specific adversaries and their acts.

SVA Process



SVA Process

ALTERNATIVE FLOWCHART



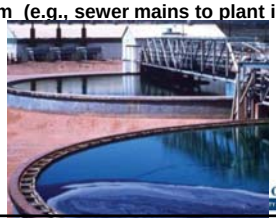
SVA planning and getting started

- **Requires management commitment of resources**
- **Generally performed by a knowledgeable team**
- **May require specialized resources or experts**
- **Will involve data and information collection**
- **May require months to fully complete**
- **Should have a means of updating**

See Garcia 2003 for getting started, collecting data

System characterization: Scope

- Carefully define what is included and excluded from the SVA.
- For example, for a wastewater system, the scope may include either or both of:
  - Collection system (e.g., sewer mains to plant inlet)
  - Treatment plant



System characterization: Mission

- An example mission statement for a wastewater treatment plant might be:

The Wastewater Treatment Plant is committed to treating wastewater from the City in such a way that the treatment plant effluent and bio-solid residual is safe for the environment, meets permit limits, and is aesthetically pleasing to the community.

System characterization: Criteria

- Specific criteria can define successful achievement of the plant's mission, such as:

Success Criterion		Description / Explanation
1	Nutrient Removal and Residual DO	C-BOD, NH3-N, and DO within NPDES permit limits (concentration and loading)
2	Suspended Solids and Oil & Grease Removal	TSS within NPDES permit limits (concentration and loading); O&G (mg/L) within NPDES permit limits
3	Metals and TTOs Removal	Cd, Cr, Cu, Ni, Zn, Hg, Ag, and cyanide within NPDES permit limits (concentration and loading); 136 different organic liquids within critical normal habitat limits in receiving creek (scanned once/year)
4	Coliform Bacteria in Effluent	Fecal coliform bacteria in effluent within NPDES permit limit
5	Biosolids	pH, metals, vector attraction, and vector reduction within state and federal EPA regulatory limits

- These criteria can also be prioritized.

Security Vulnerability Assessments

1. SVA objectives and overview
2. **Identify targets and critical assets**

Categories of possible targets

- **Property** – Laptop or desktop computer, jump drive, personal digital assistant, television, etc.
- **Vehicles** – Facility vehicle, access to areas, passes removed
- **Information** – Computer control access, stored data, intellectual property
- **Personnel** – Identification, access codes

Original list from DHS Chemical Security Awareness Training

Examples of possible targets

Wastewater system key vulnerabilities:

- Collection systems
- Treatment chemicals
- Key components of treatment plant
- Control systems
- Pumping/lift stations

U.S. GAO report GAO-05-165

Wastewater plant - disinfection chemicals

Sulfur Dioxide

Liquid Chlorine

Examples of possible targets

Other possible targets:

- Key personnel
- Valuable assets (e.g. catalysts, copper)
- Vehicles
- Personal computers

Keep in mind the plant's mission statement and success criteria when brainstorming targets and critical assets.

SVA EXERCISE

Consider a typical process facility in your industry.

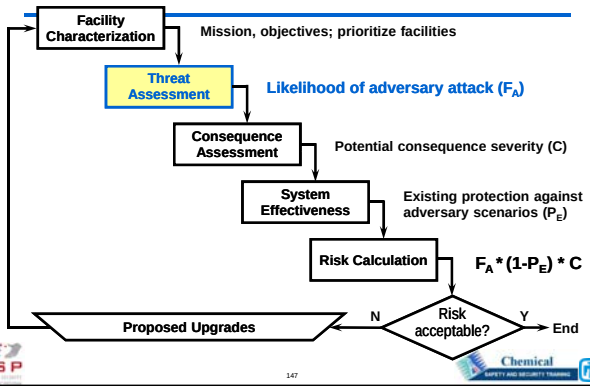
Write down at least 6 possible targets of malevolent human actions at the facility.

1	4
2	5
3	6

Security Vulnerability Assessments

1. SVA objectives and overview
2. Identify targets and critical assets
3. **Identify and assess likelihood of threats**

SVA Process



"Swiss cheese model"

Do you remember this graphic?

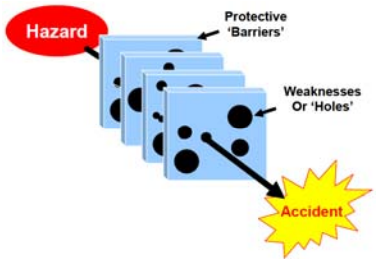
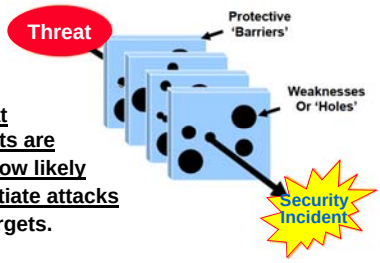


Image credit: CCPS, "Process Safety Leading and Lagging Indicators," New York: American Institute of Chemical Engineers, January 2011, www.aiche.org/ccps.

"Swiss cheese model"

The "Swiss cheese model" can be applied to security risks as well as process safety risks.

The threat assessment identifies what security threats are present and how likely they are to initiate attacks on specific targets.



A PPS design is based on *threat*

Threat Assessment: An evaluation of the threats, based on available intelligence, law enforcement, and open source information, that describes the motivations, intentions, and capabilities of these threats.

Design Basis Threat: A policy document used to establish performance criteria for a physical protection system (PPS). It is based on the results of threat assessments as well as other policy considerations.

Threat assessment

- **Motivation**
  - **Political, ideological, financial, personal**
  - **Willingness to get caught or die**
- **Intention**
  - **Theft, sabotage**
  - **Other: stop operations, social disruption, political instability, economic harm**

Threat assessment (continued)

- **Capabilities**
  - Numbers
  - Weapons, equipment, tools
  - Explosives
  - Knowledge, skills, training
  - Tactics
  - Transportation methods
  - Insider assistance

Threat assessment (continued)

Identify all potential threats

(intentional, malevolent human actions)

E.g.:

- Vandals
- Gangs, thieves
- Computer hackers
- Militia / Paramilitary
- Environmental terrorists
- Rogue international terrorists
- Insider threats; disgruntled employee

DISCUSSION

- What are some examples of *insider threats*?
- What makes the *insider threat* particularly difficult to analyze and protect against?
- What are some things that can be done to protect against *insider threats*?

Threat assessment (continued)

Some methods define "Design Basis Threats" for each identified potential adversary

- Helpful in later analysis and determining security upgrades
- Not feasible to protect every critical asset against every possible threat
- Example:

Adversary	Design Basis Threat Description
Vandals	One or two outsiders, with no authorized access or inside information. Might use hand tools or small firearms or fireworks. Opportunity taken to deface or damage assets of the utility. Does not intend to cause physical harm to utility employees or end-users. Does not want to get caught.

Assess likelihood of attack

Likelihood of an attack* can be assessed using *frequency categories*.

Options:

- **Purely qualitative, such as** `High / Medium / Low`
- **Qualitative with descriptors**
- **Order of magnitude**
- **Fully quantitative**

*Initiation of an attempt to penetrate the facility's physical or virtual boundary

Example of qualitative-with-descriptors likelihood categories

Probability Category	Level	Specific Event
A	Frequent	Possibility of repeated incidents
B	Probable	Possibility of isolated incidents
C	Occasional	Possibility of occurring sometime
D	Remote	Not likely to occur
E	Improbable	Practically impossible

From ExxonMobil "Chemical Facilities Safeguards and Security Risk Assessment Methodology, June 2002, adapted from the risk assessment matrix of MIL-STD-882B. Part of ACC Responsible Care® Toolkit, http://www.americanchemistry.com/s_rctoolkit

Example of order-of-magnitude likelihood categories

Frequency Magnitudes		
Frequency Magnitude	**Order-of-Magnitude Likelihood**	**Comparison with Experience**
+2	Twice a week	Routine; predictable
+1	Once a month	Expected; occasional
0	Once a year	Unpredictable as to when it will occur, but within realm of most employees' experience
-1	1 in 10 (10% likelihood) per year of operation	Likely to happen one or more times during the lifetime of the plant
-2	1 in 100 (1% likelihood) per year of operation	Not expected to happen during plant lifetime, but may happen occasionally within the broader industry
-3	1 in 1,000 per year of operation	Very unlikely to happen during plant lifetime

pH Scale

- **pH = 2.5**
- …
- **pH = 11.5**

- $[H^+] = 0.003$ g-mol/L
- …
- $[H^+] = 3 \times 10^{-12}$ g-mol/L

Orders of Magnitude

- 44 magnitudes between radius of proton and radius of universe
- 25 magnitudes between brightness of 40 watt light bulb and brightness of the sun
- 11 magnitudes between snail's pace and speed of light

Image Credit: National Solar Observatory/ Sacramento Peak, Sunspot, New Mexico

Assess likelihood of attack

Likelihood assessment:

- Consensus of plant personnel, fire department, local law enforcement, etc.
- Assess the likelihood of attack by each potential adversary using the selected frequency scale
- Example:

Possible Adversary	Number	Equipment	Vehicles	Weapons	Tactics	F_A	Knowledge; History; Targeting
Outsider Threat: **Ecological Terrorist**	1 - 25	Standard tools	SUV; personally owned vehicle (POV)	Small arms; semiautomatic weapons	Demonstrations, property damage	Low	Ecological groups are active in Ohio and surrounding states. Limited incidents of violence from these groups. Local law enforcement monitors these groups. No indication to target City Wastewater Dept.

Assess likelihood of attack

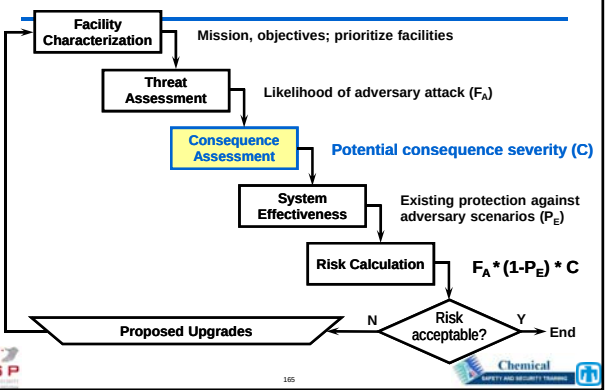
Key considerations affecting likelihood:

- *Presence in the area of the facility*
- *Access to the facility*
- *Stated/assessed intent to conduct attack*
- *History of attacks/threats*
- *Credible information indicating adversary has actually targeted facility*
- *Capability to achieve successful attack*

Security Vulnerability Assessments

1. SVA objectives and overview
2. Identify targets and critical assets
3. Identify and assess likelihood of threats
4. **Assess severity of consequences**

SVA Process

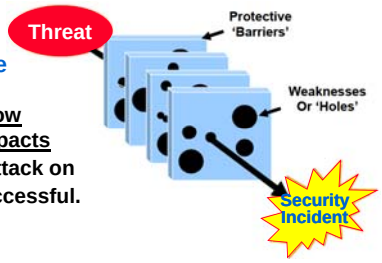


Consequence severity

Potential consequence severity (C) is assessed as the *potential* impact if an attack is successful.

- Must consider intent and capabilities of each specific threat
- Can be evaluated as a matrix of threats vs targets or as a listing of scenarios
- Consider screening out those with lesser severity

The **consequence assessment** determines how severe the impacts can be if an attack on a target is successful.



Assess severity of consequences

Chemical release scenarios:

- Essentially the same as for unintentional releases *(see Day 2 "Identification of Hazards" notes)*
  - Fires
  - Explosions
  - Toxic gas releases
- Also, theft of chemicals for release or use elsewhere (e.g., precursor chemicals)

Assess severity of consequences

Chemical release scenarios:

- Fires, explosions, toxic gas releases
- Theft of chemicals for release or use elsewhere (e.g., precursor chemicals)

Other scenarios:

- Some loss events can be assessed monetarily
  - Business interruption
  - Property damage
- Severity can be difficult to assess for other loss events
  - Trade secret information loss
  - Fear/panic impact
  - etc.

Assess severity of consequences

Loss event impact is generally assessed using *severity categories*.

Options:

- Purely qualitative, such as `High / Medium / Low`
- Qualitative with descriptors
- Order of magnitude
- Fully quantitative

Severity	Characteristics
I Critical	▪ Fatality (Loss of life) ▪ Loss of critical proprietary information ▪ Loss of essential assets ▪ Significant impairment of mission ▪ Loss of system ▪ Loss of more than $XXM USD
II Serious	▪ Nonfatal Lost Time Incident or Injury requiring hospitalization (severe injury, in-patient care needed, did not return to work) ▪ Serious loss of proprietary information and physical equipment ▪ Unacceptable mission delays ▪ Unacceptable system and operations disruption ▪ Loss of $YM to $XXM USD
III Moderate	▪ Medical Treatment Incident (MTI) other than First Aid - non lost workday (out patient, but returned to work) ▪ Undetected or delay in the detection of unauthorized entry resulting in moderate loss of assets or sensitive materials ▪ Moderate mission impairment ▪ Moderate system and operations disruption ▪ Loss of $ZZZK-$YM USD
IV Minor	▪ First Aid (treated on-site and immediately returned to work) ▪ Undetected or delay in the detection of unauthorized entry with access to sensitive materials ▪ Minor system or operations disruption ▪ Loss of $ZZK to $ZZZK USD

Example of qualitative-with-descriptors severity categories

From ExxonMobil "Chemical Facilities Safeguards and Security Risk Assessment Methodology, June 2002, adapted from the risk assessment matrix of MIL-STD-882B. Part of ACC Responsible Care® Toolkit, http://www.americanchemistry.com/s_rctoolkit

Example of order-of-magnitude severity categories

	Severity Magnitude					
Impact Type	3	4	5	6	7	8
On-Site (Worker) Health Effects	Recordable injury	Lost-time injury	Multiple or severe injuries	Permanent health effects	Fatalities	Many fatalities
Off-Site (Public) Effects	Odor; exposure below limits	Exposure above limits	Injury	Hospitalization or multiple injuries	Severe injuries or permanent effects	Fatalities
Environmental Impacts	Reportable release	Localized and short-term effects	Intermediate effects	Widespread or long-term effects	Widespread and long-term effects	Disastrous
Property/Material Loss, Business Interruption	US$ 1,000	$10,000	$100,000	$1,000,000	$10,000,000	$100,000,000
Accountability; Attention/ Concern/Response	Plant	Division; Regulators	Corporate; Neighborhood	Local/State	State/National	International

Earthquake Magnitudes (Richter Scale)

9.0	
8.0	"Great"
7.0	"Major"
6.0	"Large"
5.0	"Moderate"
4.0	
3.0	
2.0	

Magnitude of Service Disruption	Number of Customers Impacted
	Duration of Loss
	Critical Users Impacted
Total $ Impact to Wastewater Utility	
# Resulting Illnesses / Deaths	
Public Confidence Impact	
Chronic Problems	
Other Impacts	

Example consequence categories for a wastewater treatment plant

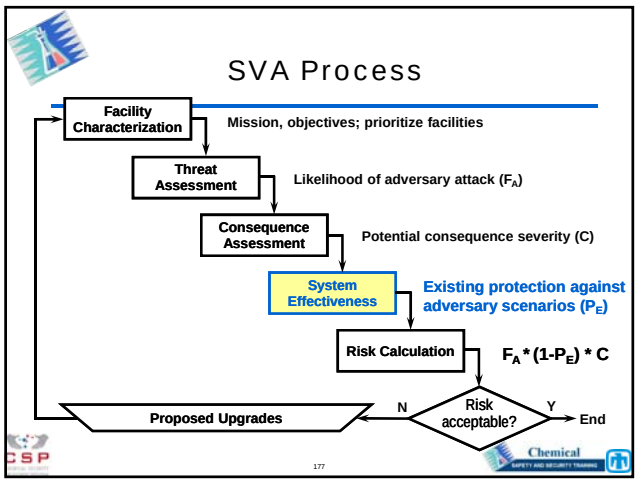
SVA EXERCISE

- **Identify key consequence categories for a typical plant in your industry**
- **Choose <u>one</u> of the consequence categories**
- **Develop an impact scale for the category**

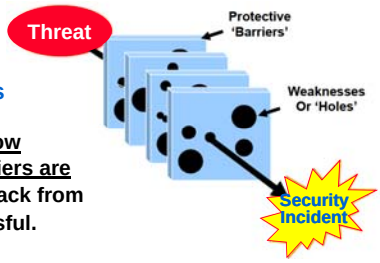
Security Vulnerability Assessments

1. SVA objectives and overview
2. Identify targets and critical assets
3. Identify and assess likelihood of threats
4. Assess severity of consequences
5. **Evaluate effectiveness of safeguards**

SVA Process



The **system effectiveness** assessment determines <u>how good the barriers are</u> to keep an attack from being successful.



Protective barriers

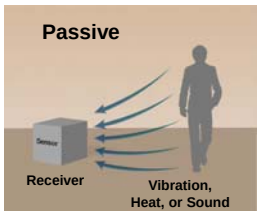
Physical Protection Systems (PPS)

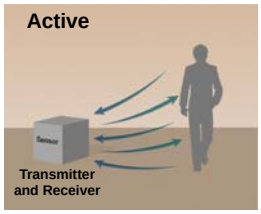
Detection | Delay | Response

Attack detection

- Intrusion detection systems
  - Detectors (sensors, cameras, guard patrols)
  - Detection signal processing and alarming
  - Alarm assessment
  - Alarm communication and display
- Entry control
- Contraband and explosives detection
- Cyber attack detection; system monitoring
- Security-aware employees

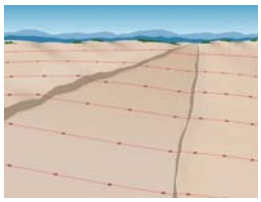
Passive or *active* physical detection





Covert or *visible*

Covert



- Sensors hidden from view
- More difficult for intruder to detect

Visible

- Sensors in plain view of intruder
- Simpler to install and repair

Volumetric or *line detection*

Volumetric

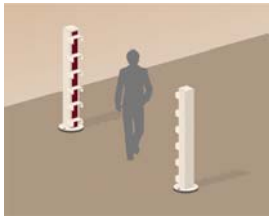
- Detection in a volume of space
- Detection volume is not visible

Line detection

- Detection along a line or plane
- Detection zone easily identified

Line-of-sight or *terrain-following*

Line-of-sight



- No obstacles in the detection space
- Requires flat ground surface

Terrain-following

- Sensors detect over flat or irregular terrain

Pictures of line (vibration) and volumetric (μwave)

Assessment vs Surveillance

Assessment - Video display triggered by sensor alarm to determine if an intruder has penetrated a sensored area.

Surveillance- Continuous video monitoring of an area that that does NOT have sensors.

Fixed and PTZ Cameras

- Fixed Camera
  - **Non-motorized mount**
  - **Fixed focal length lens**

- Pan Tilt Zoom (PTZ) Camera
  - **Motorized mount**
  - **Motorized zoom lens**

Attack delay barriers

- **Access delay**
- **Vehicle barriers**
  - **Around perimeter**
  - **Around key assets**
  - **"Serpentine" arrangement to limit approach speed**
  - **Pop-up barriers**
- **Traverse time**
- **Fences, barbed wire**
- **Doors, windows**
- **Walls**
- **Locks**
- **Strong passwords**
- **Biometrics**
- **Target task time**

Attack response

- Communications
- Weaponry, tactics
- Internal or external
- Backup forces
- Training
- Night-fighting capability
- Cyber response capability

Protection performance objective

Security-protective barriers must

(1) ***detect*** an attack soon enough and

(2) put sufficient time ***delays*** in the path of the attacker(s)

(3) for a sufficiently potent ***response*** force to arrive and interrupt the attack

before the attack succeeds in stealing, releasing, destroying or otherwise compromising the facility's critical asset(s).

SVA EXERCISE

Translate this to apply to *cyber security.*

Security-protective barriers must

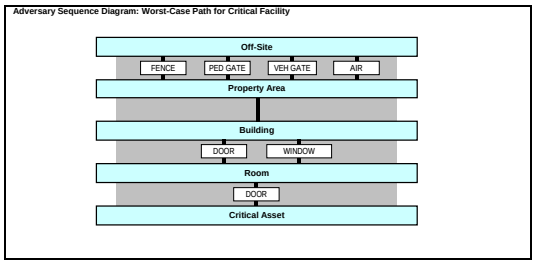
(1) ***detect*** an attack soon enough and

(2) put sufficient time ***delays*** in the path of the attacker(s)

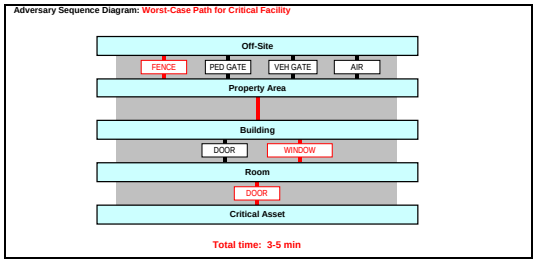
(3) for a sufficiently potent ***response*** force to arrive and interrupt the attack

before the attack succeeds in stealing, releasing, destroying or otherwise compromising the facility's critical asset(s).

Scenario and path analysis



Scenario and path analysis



EASI calculation (method from Garcia 2008)

Last Updated: City / County ☐ Water Treatment Plant Vulnerability Assessment

Estimate of Adversary Sequence Interruption (EASI)

RESULT: *Probability of Interruption by Response Force Before Adversary Task Sequence is Completed*	Probability of Response Force Communication	Response Force Time (seconds)	
		Mean	Standard Deviation
Probability of Interruption = 0.48	0.95	300	90

Sequence Number	Adversary Task	Probability of Being Detected	When Would Detection Occur?	Delay Time (seconds)	
				Mean	Standard Deviation
1	Cut fence	0		10	3
2	Run to building	0		12	3.6
3	Open door	0.9	Before the Delay	90	27
4	Run to vital area	0		10	3
5	Open door	0.9	Before the Delay	90	27
6	Sabotage target	0		120	36
7					
8					
9					
10					
11					
12					

Safeguards effectiveness

- The effectiveness of safeguards is maintained by *performance testing.*
- If any safeguard is not tested, do not count on it working!

DISCUSSION

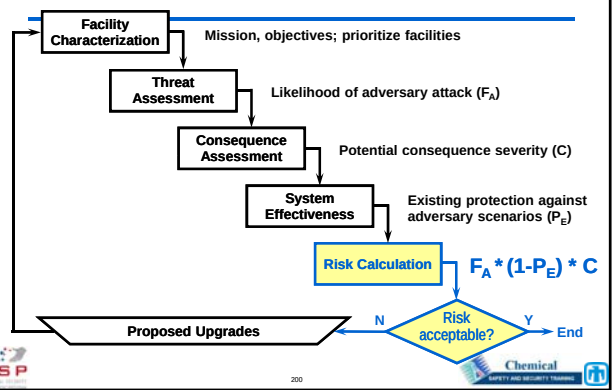
How can the performance of these physical protection system components be ensured?

- CCTV camera system
- Security guards visual detection
- Perimeter fence
- Access-control door locks
- Response force

Security Vulnerability Assessments

1. SVA objectives and overview
2. Identify targets and critical assets
3. Identify and assess likelihood of threats
4. Assess severity of consequences
5. Evaluate effectiveness of safeguards
6. **Determine adequacy of safeguards**

SVA Process



Security risk equation

$$Risk = F_A * (1 - P_E) * C$$

where F_A = Frequency of attack[1]

P_E = Protection system effectiveness

C = Consequence severity

[1]or probability of attack for a given timeframe or mission

Example risk calculation

$$Risk = F_A * (1 - P_E) * C$$

Assume P_A = One attack per year attempted

P_E = 0.90 effective protection

C = $50,000 loss

Example risk calculation (continued)

$$Risk = 1/yr * (1 - 0.9) * \$50K$$

= $5,000 / year

annualized loss rate

Another example

$$Risk = F_A * (1 - P_E) * C$$

Assume P_A = 0.1 attack per year attempted

P_E = 0.99 effective protection

C = Fire/explosion with 10 fatalities

What is *Risk* equal to?

Another example (continued)

Risk = 0.1/yr * (1 - 0.99) * 10

= **0.01 fatality / year**

point risk estimate

Make risk decision

Determining whether existing or proposed safeguards are adequate can be done in various ways.

Options:

- **Purely qualitative, team-based judgment**
- **Risk matrix**
- **Risk magnitude**
- **Fully quantitative**

Example of risk matrix with qualitative-with-descriptors likelihood and severity categories

Severity Categories	Probability of Occurrence				
	(A) Frequent	(B) Probable	(C) Occasional	(D) Remote	(E) Improbable
I	IA	IB	IC	ID	IE
II	IIA	IIB	IIC	IID	IIE
III	IIIA	IIIB	IIIC	IIID	IIIE
IV	IVA	IVB	IVC	IVD	IVE

Risk Category (RC)	Risk Index	RI Number (RI)
IA, IB, IC, IIA, IIB, IIIA	Implement countermeasures that reduce risk to an SSRI of a level 2, at a minimum	1
ID, IIC, IID, IIIB, IIIC	Not acceptable without management re-evaluation	2
IE, IIE, IIID, IIIE, IVA, IVB	Acceptable with review by management	3
IVC, IVD, IVE	Acceptable without review	4

From ExxonMobil "Chemical Facilities Safeguards and Security Risk Assessment Methodology, June 2002, adapted from the risk assessment matrix of MIL-STD-882B. Part of ACC Responsible Care® Toolkit, http://www.americanchemistry.com/s_rctoolkit

Example of risk matrix with qualitative-with-descriptors likelihood and severity categories

Severity Categories	Probability of Occurrence				
	(A) Frequent	(B) Probable	(C) Occasional	(D) Remote	(E) Improbable
I	IA	IB	IC	ID	IE
II	IIA	IIB	IIC	IID	IIE
III	IIIA	IIIB	IIIC	IIID	IIIE
IV	IVA	IVB	IVC	IVD	IVE

Risk Category (RC)	Risk Index	RI Number (RI)
IA, IB, IC, IIA, IIB, IIIA	Implement countermeasures that reduce risk to an SSRI of a level 2, at a minimum	1
ID, IIC, IID, IIIB, IIIC	Not acceptable without management re-evaluation	2
IE, IIE, IIID, IIIE, IVA, IVB	Acceptable with review by management	3
IVC, IVD, IVE	Acceptable without review	4

From ExxonMobil "Chemical Facilities Safeguards and Security Risk Assessment Methodology, June 2002, adapted from the risk assessment matrix of MIL-STD-882B. Part of ACC Responsible Care® Toolkit, http://www.americanchemistry.com/s_rctoolkit

NOTE:
Determining where the risk boundaries are set is a risk management function

Example of order-of-magnitude risk decisions

Risk calculations can be simplified by using <u>orders of magnitude</u> and <u>exponents</u>.

Exponential risk calculations

Scenario Frequency x ***Scenario Impact*** = ***Scenario Risk***

(loss events / year) x (impact / loss event) = (impact / year)

Example: "Hundred-year flood"

(0.01 flood / year) x ($10,000,000 / flood) = $100,000 / year

Multiply frequency x impact

(10^{-2} flood / year) x ($\$10^{7}$ / flood) =

$\$10^{5}$ / year

Exponents

-2 7

5

Exponents

-2 7

5

Add/subtract exponents

-2 + 7 = 5

EXERCISE

Risk = 0.1/yr * (1 - 0.99) * 10

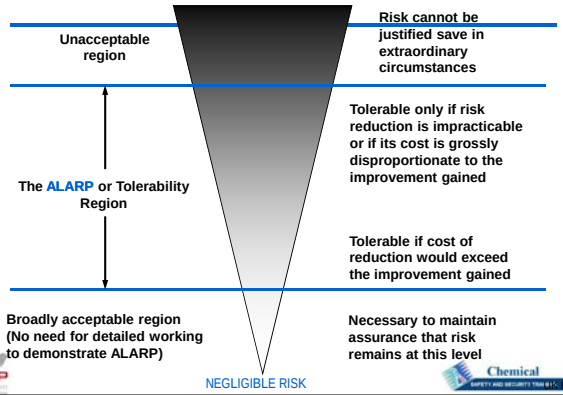
= 0.01 fatality / year

point risk estimate

What is the *risk magnitude* (exponent) for this risk?

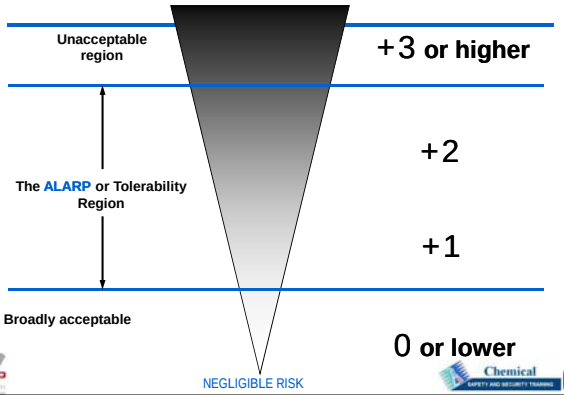
Risk Tolerance and the ALARP Principle

(As Low As Reasonably Practicable)



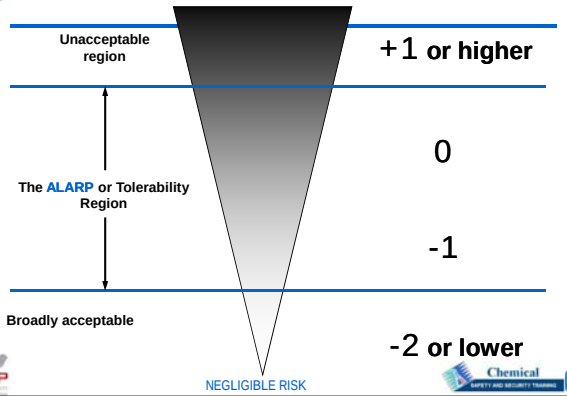
Company #1 risk boundaries

Risk Magnitude



Company #2 risk boundaries

Risk Magnitude



SVA EXERCISE

Describe <u>one complete security scenario</u> involving

- a particular threat and its likelihood,
- a particular consequence and its severity, and
- a reasonable set of safeguards and their effectiveness.

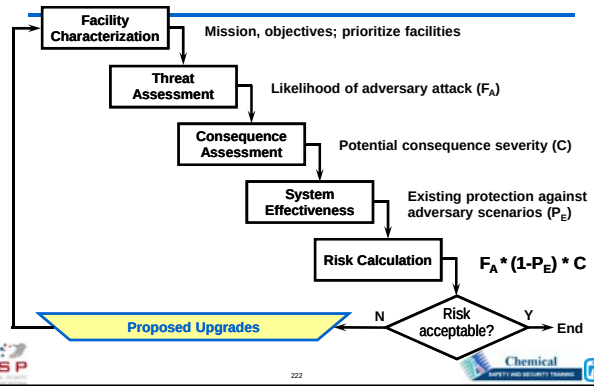
Using any one risk evaluation approach, calculate the scenario risk and determine its acceptability.

Be prepared to present your results and findings, including important assumptions.

Security Vulnerability Assessments

1. SVA objectives and overview
2. Identify targets and critical assets
3. Identify and assess likelihood of threats
4. Assess severity of consequences
5. Evaluate effectiveness of safeguards
6. Determine adequacy of safeguards
7. **Identify and implement improvements**

SVA Process



Develop and implement improvements

- **Address specific vulnerabilities identified in the SVA**
- **Address scenarios assessed to pose the highest security risk**

Possible improvements

- **Tendency:** ***Add more physical safeguards*** **(fences, cameras, locks, etc.).**
- **First priority:** ***Make sure what you have will work.***
  - **Performance testing**
  - **Drills, tabletop exercises**
- **Also a priority:** ***Make the facility inherently safer.***
  - Minimize
  - Substitute
  - Attenuate
  - **Simplify, limit effects, etc.**

Example strategies

Some wastewater security-enhancing activities:

- Replacing gaseous chemicals with less hazardous alternatives
- Improving local/state/regional collaboration efforts
- Completing SVAs for individual wastewater systems
- Expanding training for wastewater utility operators, administrators
- Improving national communication efforts
- Installing early warning in collection systems
- Hardening plants and collection facilities against attack
- Strengthening procedures
- Increasing R&D to improve detection, assessment and response

SVA report

The SVA is generally captured in a report and/or management presentation.

- **Objectives**
- **Team**
- **Approach**
- **Data and Analysis**
- **Results and Conclusions**
- **Recommended improvements**

See Garcia 2003 and Normal 2010 for suggested presentation formats

Updating the SVA

Keep in mind:

"The search for static security, in the law and elsewhere, is misguided. The fact is, security can only be achieved through constant change, adapting old ideas that have outlived their usefulness to current facts."

- William O. Douglas, as quoted in Garcia 2003

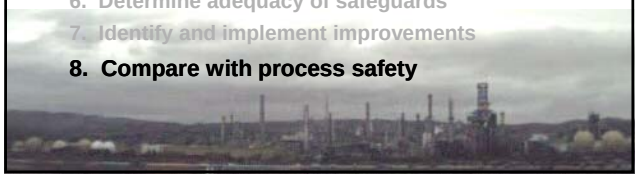
SVA EXERCISE

List five reasons why last year's SVA may need to be, or would benefit from being, updated.

1
2
3
4
5

Security Vulnerability Assessments

1. SVA objectives and overview
2. Identify targets and critical assets
3. Identify and assess likelihood of threats
4. Assess severity of consequences
5. Evaluate effectiveness of safeguards
6. Determine adequacy of safeguards
7. Identify and implement improvements
8. **Compare with process safety**



Comparison between site security and process safety scenario elements *(differences italicized)*

Consideration	Site security	Process safety
Hazards requiring containment and control	Hazardous process materials and energies and potential chemical interactions	Hazardous process materials and energies and potential chemical interactions
Containment and control systems	Various means of making abnormal situation initiating events less likely, including e.g. *deterrence, vigilance, site access controls, perimeter guards and barriers*	Various means of making abnormal situation initiating events less likely, including e.g. *operating discipline, mechanical integrity program, equipment guards and barriers*
Abnormal situation initiating event	*Facility intrusion by unauthorized person or weapon with malevolent intent*	*Unintentional, unplanned human error, mechanical failure, or external event*
Initial detection systems	*Intrusion detection*	*Process deviation detection*

Continued on next slide

Comparison between site security and process safety scenario elements (continued)

Consideration	Site security	Process safety
Preventive safeguards	*Means to delay intruder until sufficiently potent response force can arrive to stop intruder before consequence occurs*	*Means to bring process back under control or safely shut down process before consequence occurs*
Loss events	Fire, explosion, toxic release, unplanned shutdown, *chemical theft, vandalism*	Fire, explosion, toxic release, unplanned shutdown
Mitigative safeguards	Fire fighting, blast shielding, secondary containment, vapor release countermeasures, site and community emergency response	Fire fighting, blast shielding, secondary containment, vapor release countermeasures, site and community emergency response
Impacts	Injuries/fatalities, environmental damage, property damage, business interruption, *fear/panic*	Injuries/fatalities, environmental damage, property damage, business interruption

Source: CCPS 2008a p. 207

Hazards are mostly the same

Comparison between site security and process safety scenario elements *(differences italicized)*

Consideration	Site security	Process safety
Hazards requiring containment and control	Hazardous process materials and energies and potential chemical interactions	Hazardous process materials and energies and potential chemical interactions
Containment and control systems	Various means of making abnormal situation initiating events less likely, including e.g. *deterrence, vigilance, site access controls, perimeter guards and barriers*	Various means of making abnormal situation initiating events less likely, including e.g. *operating discipline, mechanical integrity program, equipment guards and barriers*
Abnormal situation initiating event	*Facility intrusion by unauthorized person or weapon with malevolent intent*	*Unintentional, unplanned human error, mechanical failure, or external event*
Initial detection systems	*Intrusion detection*	*Process deviation detection*

Threats are intentional, malevolent

Comparison between site security and process safety scenario elements *(differences italicized)*

Consideration	Site security	Process safety
Hazards requiring containment and control	Hazardous process materials and energies and potential chemical interactions	Hazardous process materials and energies and potential chemical interactions
Containment and control systems	Various means of making abnormal situation initiating events less likely, including e.g. *deterrence, vigilance, site access controls, perimeter guards and barriers*	Various means of making abnormal situation initiating events less likely, including e.g. *operating discipline, mechanical integrity program, equipment guards and barriers*
Abnormal situation initiating event	*Facility intrusion by unauthorized person or weapon with malevolent intent*	*Unintentional, unplanned human error, mechanical failure, or external event*
Initial detection systems	*Intrusion detection*	*Process deviation detection*

Threats are intentional, malevolent

Threat of:

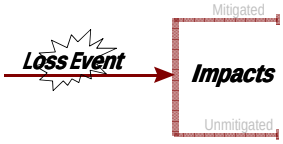
- **Release of hazardous material**
- **Destruction of critical assets**
- **Harm to key personnel**
- **Vandalism**
- **Theft**
- **etc.**

Threats are intentional, malevolent

Threat of:
- Release of hazardous material
- Destruction of critical assets
- Harm to key personnel
- Vandalism
- Theft
- etc.

By:
- Vandal
- Gang, thief
- Militia / paramilitary
- Environmental terrorist
- Rogue international terrorist
- Insider threat; disgruntled employee

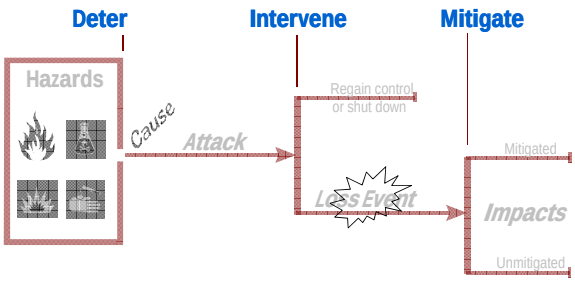
Loss events, impacts are similar



Comparison between site security and process safety scenario elements (continued)

Consideration	Site security	Process safety
Preventive safeguards	*Means to delay intruder until sufficiently potent response force can arrive to stop intruder before consequence occurs*	*Means to bring process back under control or safely shut down process before consequence occurs*
Loss events	Fire, explosion, toxic release, unplanned shutdown, *chemical theft, vandalism*	Fire, explosion, toxic release, unplanned shutdown
Mitigative safeguards	Fire fighting, blast shielding, secondary containment, vapor release countermeasures, site and community emergency response	Fire fighting, blast shielding, secondary containment, vapor release countermeasures, site and community emergency response
Impacts	Injuries/fatalities, environmental damage, property damage, business interruption, *fear/panic*	Injuries/fatalities, environmental damage, property damage, business interruption

Key strategies: *Deter, Intervene, Mitigate*



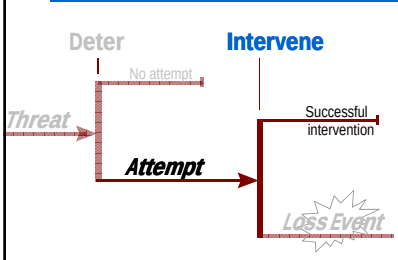
Deter: make attack less likely

- **Deter**
  - **Make target less attractive**
  - **Maintain visible defenses**
  - **Lower perceived likelihood of success**

Comparison between site security and process safety scenario elements *(differences italicized)*

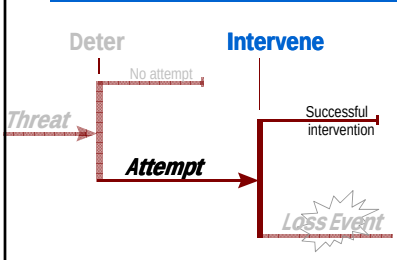
Consideration	Site security	Process safety
Hazards requiring containment and control	Hazardous process materials and energies and potential chemical interactions	Hazardous process materials and energies and potential chemical interactions
Containment and control systems	Various means of making abnormal situation initiating events less likely, including e.g. *deterrence, vigilance, site access controls, perimeter guards and barriers*	Various means of making abnormal situation initiating events less likely, including e.g. *operating discipline, mechanical integrity program, equipment guards and barriers*
Abnormal situation initiating event	*Facility intrusion by unauthorized person or weapon with malevolent intent*	*Unintentional, unplanned human error, mechanical failure, or external event*
Initial detection systems	*Intrusion detection*	*Process deviation detection*

Intervene: Interrupt attack



Intervene
- **Detect**
  AND
- **Delay**
  AND
- **Respond**

Intervene: Interrupt attack

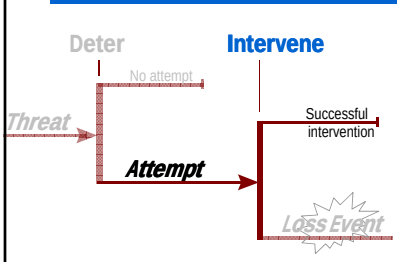


- **Detect**
  - **Identify threat**
  - **Communi-cate to response force**

Comparison between site security and process safety scenario elements *(differences italicized)*

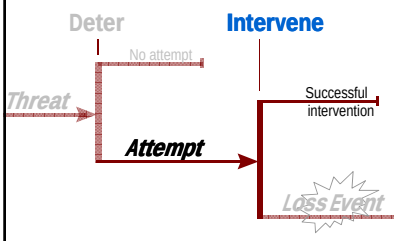
Consideration	Site security	Process safety
Hazards requiring containment and control	Hazardous process materials and energies and potential chemical interactions	Hazardous process materials and energies and potential chemical interactions
Containment and control systems	Various means of making abnormal situation initiating events less likely, including e.g. *deterrence, vigilance, site access controls, perimeter guards and barriers*	Various means of making abnormal situation initiating events less likely, including e.g. *operating discipline, mechanical integrity program, equipment guards and barriers*
Abnormal situation initiating event	*Facility intrusion by unauthorized person or weapon with malevolent intent*	*Unintentional, unplanned human error, mechanical failure, or external event*
Initial detection systems	*Intrusion detection*	*Process deviation detection*

Intervene: Interrupt attack



- Detect
- **Delay**
  - **Slow down attack with barriers**
  - **Give response force time to interrupt attack**

Intervene: Interrupt attack

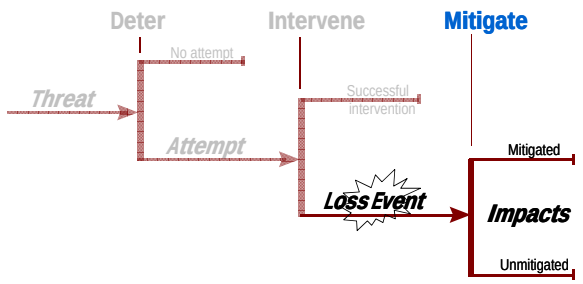


- Detect
- Delay
- **Respond**
  - **Receive alarm**
  - **Arrive in time with sufficient force to interrupt attack**

Comparison between site security and process safety scenario elements (continued)

Consideration	Site security	Process safety
Preventive safeguards	*Means to delay intruder until sufficiently potent response force can arrive to stop intruder before consequence occurs*	*Means to bring process back under control or safely shut down process before consequence occurs*
Loss events	Fire, explosion, toxic release, unplanned shutdown, *chemical theft, vandalism*	Fire, explosion, toxic release, unplanned shutdown
Mitigative safeguards	Fire fighting, blast shielding, secondary containment, vapor release countermeasures, site and community emergency response	Fire fighting, blast shielding, secondary containment, vapor release countermeasures, site and community emergency response
Impacts	Injuries/fatalities, environmental damage, property damage, business interruption, *fear/panic*	Injuries/fatalities, environmental damage, property damage, business interruption

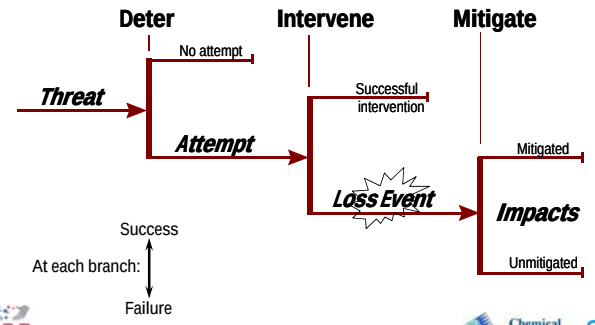
Mitigate:
Reduce successful attack impacts



Comparison between site security and process safety scenario elements (continued)

Consideration	Site security	Process safety
Preventive safeguards	*Means to delay intruder until sufficiently potent response force can arrive to stop intruder before consequence occurs*	*Means to bring process back under control or safely shut down process before consequence occurs*
Loss events	Fire, explosion, toxic release, unplanned shutdown, *chemical theft, vandalism*	Fire, explosion, toxic release, unplanned shutdown
Mitigative safeguards	Fire fighting, blast shielding, secondary containment, vapor release countermeasures, site and community emergency response	Fire fighting, blast shielding, secondary containment, vapor release countermeasures, site and community emergency response
Impacts	Injuries/fatalities, environmental damage, property damage, business interruption, *fear/panic*	Injuries/fatalities, environmental damage, property damage, business interruption

The big picture



Chemical
SAFETY AND SECURITY TRAINING

Incident Investigation and Reporting

SAND No. 2011-1036C
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.

Key acronyms

RCA = *root cause analysis*

SVA = *security vulnerability analysis*

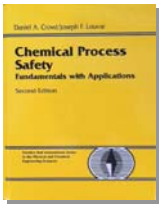
Incident investigation resources

CCPS 2003. Center for Chemical Process Safety, *Guidelines for Investigating Chemical Process Incidents, 2nd Edition*, NY: American Institute of Chemical Engineers.

Chapter
1 Introduction
2 Designing an incident investigation management system
3 An overview of incident causation theories
4 An overview of investigation methodologies
5 Reporting and investigating near misses
6 The impact of human factors
7 Building and leading an incident investigation team
8 Gathering and analyzing evidence
9 Determining root causes–structured approaches
10 Developing effective recommendations
11 Communication issues and preparing the final report
...

Incident investigation resources

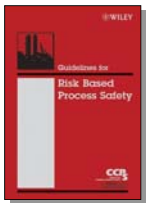
D.A. Crowl and J.F. Louvar 2001. *Chemical Process Safety: Fundamentals with Applications, 2nd Ed.*, Upper Saddle River, NJ: Prentice Hall.



Chapter 12 • Accident Investigations
12.1 Learning from accidents
12.2 Layered investigations
12.3 Investigation process
12.4 Investigation summary
12.5 Aids for diagnosis
12.6 Aids for recommendations

Incident investigation resources

CCPS 2007a. Center for Chemical Process Safety, *Guidelines for Risk Based Process Safety*, NY: American Institute of Chemical Engineers.



Chapter 19 • Incident Investigation
19.1 Element Overview
19.2 Key Principles and Essential Features
19.3 Possible Work Activities
19.4 Examples of Ways to Improve Effectiveness
19.5 Element Metrics
19.6 Management Review

Incident Investigation and Reporting

1. What is an *incident investigation*?
2. How does incident investigation fit into PSM?
3. What kinds of incidents are investigated?
4. When is the incident investigation conducted?
5. Who performs the investigations?
6. What are some ways to investigate incidents?
7. How are incident investigations documented?
8. What is done with findings & recommendations?
9. How can incidents be counted and tracked?

Photo credit: U.S. Chemical Safety & Hazard Investigation Board

Incident Investigation and Reporting

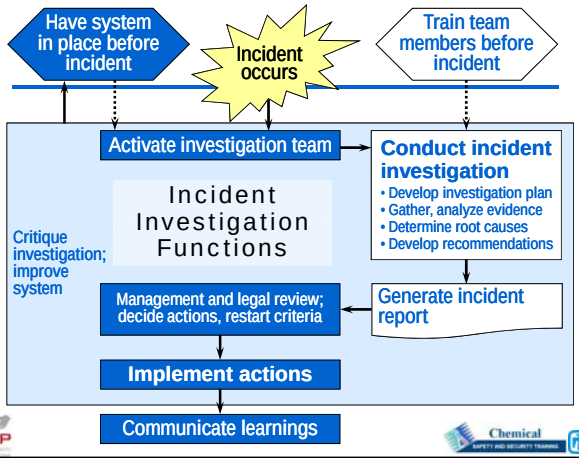
1. What is an *incident investigation*?

Results of explosion and fire at a waste flammable solvent processing facility
(U.S. CSB Case Study 2009-10-I-OH)

What is an *incident investigation*?

An *incident investigation* is the management process by which underlying causes of undesirable events are uncovered and steps are taken to prevent similar occurrences.

- CCPS 2003



Learning from incidents

Investigations that will enhance learning

- are **fact-finding**, not fault-finding
- must get to the ***root causes***
- must be reported, **shared** and retained.

Definition - Root cause

Root Cause: **A fundamental, underlying, system-related reason why an incident occurred that identifies a correctable failure or failures in management systems.**

There is typically more than one root cause for every process safety incident.

- CCPS 2003

Incident Investigation and Reporting

1. What is an *incident investigation*?
2. How does incident investigation fit into PSM?

How does incident investigation fit into PSM?

Risk-Based Process Safety (CCPS 2007a)

Commit to Process Safety	Understand Hazards and Risks	Manage Risk	Learn from Experience
• Process safety culture • Compliance with standards • Process safety competency • Workforce involvement • Stakeholder outreach	• Process knowledge management • Hazard identification and risk analysis	• Operating procedures • Safe work practices • Asset integrity and reliability • Contractor management • Training and performance assurance • Management of change • Operational readiness • Conduct of operations • Emergency management	• Incident investigation • Measurement and metrics • Auditing • Management review and continuous improvement

Historical

Potential

Four perspectives for designing, building and operating a safe, secure and profitable facility

Actual

Hypo-thetical

Historical

Codes, Standards, RAGAGEPs

- **The historical perspective tells us what to do based on codes, standards and best practices that represent our accumulated experience and lessons learned from previous industry incidents.**

Potential

Hazards, Consequences

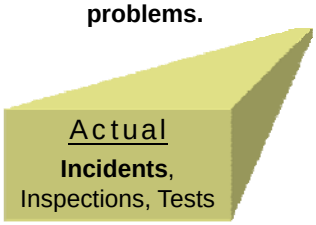
- **The potentials are what could happen if containment or control of a process hazard was lost or if a security incident occurred.**

- **The hypothetical, or predictive, perspective looks at what could go wrong, even if it has never happened before. This is a probabilistic perspective, based on hypothetical loss event scenarios.**

Hypothetical

What-If, HAZOP, SVA

• The actual or real-time perspective can inform us of previously unrecognized or uncorrected problems, as they are manifested in actual incidents and near misses, as well as by ongoing inspections and tests that can detect incipient problems.



Incident Investigation and Reporting

1. What is an *incident investigation*?
2. How does incident investigation fit into PSM?
3. What kinds of incidents are investigated?

What kinds of incidents are investigated?

- The first step in an incident investigation is recognizing that an "incident" has occurred!

What kinds of incidents are investigated?

- The first step in an incident investigation is recognizing that an "incident" has occurred!

Yes

What kinds of incidents are investigated?

- The first step in an incident investigation is recognizing that an "incident" has occurred!

?

Definitions

Incident: **An unplanned event or sequence of events that either resulted in or had the potential to result in adverse impacts.**

Incident sequence: **A series of events composed of an initiating cause and intermediate events leading to an undesirable outcome.**

Source: CCPS 2008a

Incident types

Three categories of incidents, based on outcomes:

Loss event | **Near miss** | **Operational interruption**

Incident types

Three categories of incidents, based on outcomes:

Loss event

- Actual loss or harm occurs (also termed *accident* when not related to security)

Near miss

Operational interruption

- Actual impact on production or product quality occurs

Incident types

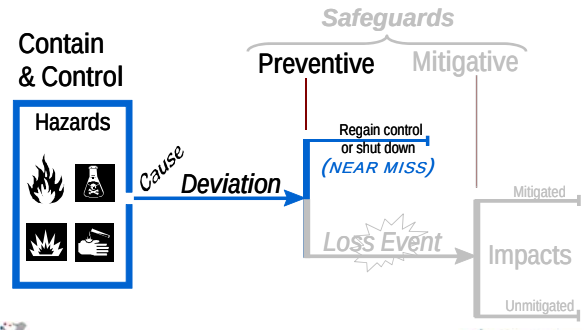
Three categories of incidents, based on outcomes:

Loss event | **Near miss** | Operational interruption

Near miss: **An occurrence in which an accident (i.e., property damage, environmental impact, or human loss) or an operational interruption could have plausibly resulted if circumstances had been slightly different.** - CCPS 2003

(Same concept for security incidents also)

One type of near miss



DISCUSSION

Give three or four examples of simple near-miss scenarios that would fit the graphic on the previous slide.

Include at least one related to facility security.

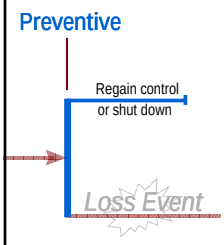
___

___

___

___

Preventive safeguards revisited



Operational Mode: **Abnormal operation**

Objective: **Regain control or shut down; keep loss events from happening**

Examples of Preventive Safeguards:

- Operator response to alarm
- Safety Instrumented System
- Hardwired interlock
- Last-resort dump, quench, blowdown
- Emergency relief system

REVIEW

What are the equivalent of *preventive safeguards* for facility security physical protection systems?

___

___

___

___

Incident Investigation and Reporting

1. What is an *incident investigation*?
2. How does incident investigation fit into PSM?
3. What kinds of incidents are investigated?
4. **When** is the incident investigation conducted?

When is the incident investigation conducted?

- Basic answer: **As soon as possible.**
- Reasons:
  - Evidence gets lost or modified
    - Computer control historical data overwritten
    - Outside scene exposed to rain, wind, sunlight
    - Chemical residues oxidize, etc.
  - Witness memories fade or change
  - Other incidents may be avoided
  - Restart may depend on completing actions to prevent recurrence
  - Regulators or others may require it
    - E.g., U.S. OSHA PSM: Start within 48 h

When is the incident investigation conducted?

Challenges to starting as soon as possible:

- Team must be selected and assembled
- Team may need to be trained
- Team may need to be equipped
- Team members may need to travel to site
- Authorities or others may block access
- Site may be unsafe to approach/enter

DISCUSSION

What might be done to overcome some of the challenges to starting an investigation sooner?

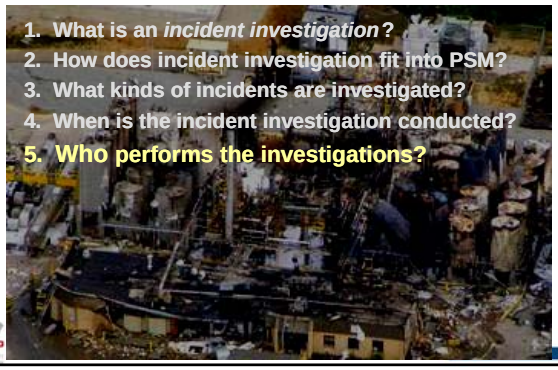
–

–

–

–

Incident Investigation and Reporting



1. What is an *incident investigation*?
2. How does incident investigation fit into PSM?
3. What kinds of incidents are investigated?
4. When is the incident investigation conducted?
5. **Who performs the investigations?**

Who performs the investigations?

Options:

- **Single investigator**
- **Team approach**

Who performs the investigations?

Options:

- Single investigator
- **Team approach**

Advantages of team approach: (CCPS 2003)

- Multiple technical perspectives help analyze findings
- Diverse personal viewpoints enhance objectivity
- Internal peer reviews can enhance quality
- More resources are available to do required tasks
- Regulatory authority may require it

Who performs the investigations?

The "best team" will vary depending on the nature, severity and complexity of the incident.

Some possible team members:

- Team leader / investigation method facilitator
- Area operator
- Process engineer
- Safety/security specialist
- I&E / process control or computer systems support
- Union safety representative
- Contractor representative
- Other specialists (e.g., metallurgist, chemist)

Train team members before incident

Training site management, potential team members and support personnel ahead of time will speed up the start of the investigation.

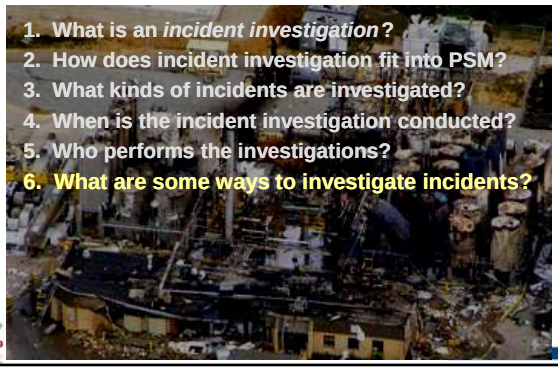
- **Larger companies may have one or more specially trained persons available for major incident investigations**
- **<u>All personnel</u> need to be familiar with the basic incident recognition and reporting requirements**

Conduct incident investigation

- Develop investigation plan
- Gather, analyze evidence
- Determine root causes
- Develop recommendations

Generate incident report

Incident Investigation and Reporting



1. **What is an *incident investigation*?**
2. **How does incident investigation fit into PSM?**
3. **What kinds of incidents are investigated?**
4. **When is the incident investigation conducted?**
5. **Who performs the investigations?**
6. **What are some ways to investigate incidents?**

<u>Older</u> investigations

- **Only identified obvious causes; e.g.,**
  - **"The line plugged up"**
  - **"The operator screwed up"**
  - **"The whole thing just blew up"**
- **Recommendations were superficial**
  - **"Clean out the plugged line"**
  - **"Re-train the operator"**
  - **"Build a new one"**

Layered investigations

- Deeper analysis
- Additional layers of recommendations:
  1. Immediate technical recommendations
     - *e.g., replace the carbon steel with stainless steel*
  2. Recommendations to avoid the hazards
     - *e.g., use a noncorrosive process material*
  3. Recommendations to improve the management system
     - *e.g., keep a materials expert on staff*

Investigation process

1. Choose investigation team
2. Make brief overview survey
3. Set objectives, delegate responsibilities
4. Gather, organize pre-incident facts
5. Investigate, record incident facts
6. Research, analyze unknowns
7. Discuss, conclude, recommend
8. Write clear, concise, accurate report

Discovery phase

- Develop a plan
- Gather evidence
  - Take safety precautions; use PPE
  - Preserve the physical scene and process data
  - Gather physical evidence, samples
  - Take photographs, videos
  - Interview witnesses
  - Obtain control or computer system charts and data

Analysis of facts

- Develop a timeline
- Analyze physical and/or electronic evidence
  - Chemical analysis
  - Mechanical testing
  - Computer modeling
  - Data logs
  - etc.
- Conduct multiple-root-cause analysis

Some analysis methods

- **Five Why's**
- **Causal Tree**
- **RCA** (Root Cause Analysis)
- **FTA** (Fault Tree Analysis)
- **MORT** (Management Oversight and Risk Tree)
- **MCSOII** (Multiple Cause, Systems Oriented Incident Investigation)
- **TapRooT®**

Some analysis methods

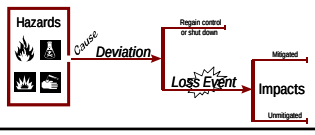
General analysis approach:

- Develop, by brainstorming or a more structured approach, possible **incident sequences**
- Eliminate as many incident sequences as possible based on the available evidence
- Take a closer look at those that remain until the actual incident sequence is discovered (if possible)
- Determine the underlying **root causes** of the actual incident sequence

Incident sequence questions

Determine, for the incident being investigated:

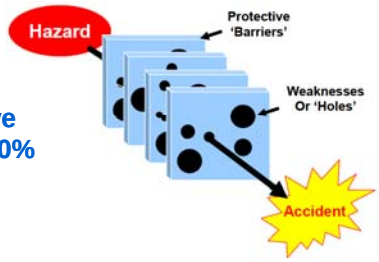
- What was the ***cause*** or ***attack*** that changed the situation from "normal" to "abnormal"?
- What was the actual (or potential, if a near miss) ***loss event***?
- What **safeguards** failed? What did not fail?



"Swiss cheese model" revisited

REMEMBER:

No protective barrier is 100% reliable.



EXERCISE

Conduct "Five Why's" on the most recent loss event that has happened to you personally.

Why did the loss event happen? Because _____

_____

Why? Because _____

Why? Because _____

Why? Because _____

Why? Because _____

Discuss, conclude, recommend

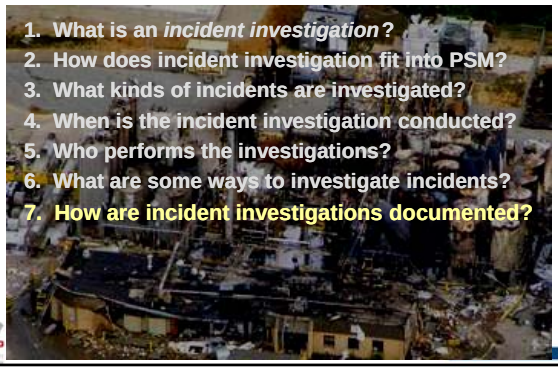
- **Find the most likely scenario that fits the facts**
- **Determine the underlying management system failures**
- **Develop layered recommendations**

Aids for diagnosis

- **Location of fire ignition?**
- **Deflagration or detonation?**
- **Hydraulic or pneumatic failure?**
- **Pressure required to rupture containment?**
- **Medical evidence?**

See Crowl and Louvar 2001 Section 12.5 for details

Incident Investigation and Reporting



1. **What is an *incident investigation*?**
2. **How does incident investigation fit into PSM?**
3. **What kinds of incidents are investigated?**
4. **When is the incident investigation conducted?**
5. **Who performs the investigations?**
6. **What are some ways to investigate incidents?**
7. **How are incident investigations documented?**

How are incident investigations documented?

A written report documents, as a minimum:

- **Date of the incident**
- **When the investigation began**
- **Who conducted the investigation**
- **A description of the incident**
- **The factors that contributed to the incident**
- **Any recommendations resulting from the investigation**

Typical report format

1. Introduction
2. System description
3. Incident description
4. Investigation results
5. Discussion
6. Conclusions
7. Layered recommendations

Investigation summary

- **The investigation report is generally too detailed to share the learnings to most interested persons**
- **An Investigation Summary can be used for broader dissemination, such as to:**
  - **Communicate to management**
  - **Use in safety or security meetings**
  - **Train new personnel**
  - **Share lessons learned with sister plants**

(See also: Crowl & Louvar 2001, Figure 12-1 and Example 12-2)

Investigation summary example

Accident involving contractors' injury during the operation of opening of a vessel for standard maintenance

Description: This accident occurred in May 2003 during repair work in a propylene reactor at a European Petrochemicals site. The cover of a manhole was ejected 5 metres by a residual pressure inside the reactor.

Consequences: 5 operators from the maintenance department were evaded to hospital. Nobody was seriously injured.

History: Work had to be done in the vessel. Before the work could start, the vessel must be put into safe conditions and the manhole must be opened. That has been decided during the safety preparation meeting.

Preparation: The putting into safe conditions started on Wednesday. The drawings of this part of the plant have been taken; the valves to be closed are noted on the drawing and then closed in the field. Then, a nitrogen flush is installed in the entire installation (vessel and lines) to assure that all flammable gases are removed from the system. Flushing means that nitrogen pressure is applied and then the vessel out is released to a safe location. This operation goes on for several days.

After that, on Friday, before opening the vessel, blinds had to be placed into the lines (to assure that no product could enter the vessel). The entire system has been depressurised. These blinds are indicated on the drawing and the maintenance people started to put in the blinds (opening the lines to put them in).

The accident: Having started this operation, all of a sudden, they smell some gas odour and called the shift supervisor. They find out that a valve on a small line has not been closed. They close this valve and decided to flush 5 additional times. After that and while monitoring the depressurisation of the vessel via the manometer on the outside of the tank (from zero to 25 bars, impossible to read lower that 0.5), they opened the manhole. A whistling sound has been heard indicating a residual pressure in the vessel. When the noise was ended, they continued to open the manhole. At a certain moment the manhole was sprung heavily out by the residual pressure in the vessel, it was ejected and fell to the ground striking two employees.

Lesson Learned

- The application of the procedure has to be strictly followed and supervised.
- Monitoring has to be done using multiple devices or means, so as to be sure of the indication.
- The equipment handling has to be done using the principles of inherent safety.

Source: **S2S** - A Gateway for Plant and Process Safety, www.safety-s2s.eu

Accident involving contractors' injury during the operation of opening of a vessel for standard maintenance

Description: This accident occurred in May 2003 during repair work in a propylene reactor at a European Petrochemicals site. The cover of a manhole was ejected 5 metres by a residual pressure inside the reactor.

Consequences: 5 operators from the maintenance department were rushed to hospital. Nobody was seriously injured.

History: Work had to be done in the vessel. Before the work could start, the vessel must be put into safe conditions and the manhole must be opened. That has been decided during the safety preparation meeting.

Preparation: The putting into safe conditions started on Wednesday. The drawings of this part of the plant have been taken; the valves to be closed are noted on the drawing and then closed in the field. Then, a nitrogen flush is installed in the entire installation (vessel and lines) to ensure that all flammable gases are removed from the system. Flushing means that nitrogen pressure is applied and then the wash out is released to a safe location. This operation goes on for several days.

out is released to a safe location. This operation goes on for several days.

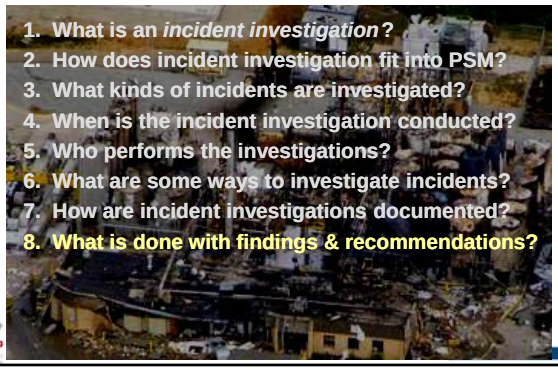
After that, on Friday, before opening the vessel, blinds had to be placed into the lines (to ensure that no product could enter the vessel). The entire system has been depressurised. These blinds are indicated on the drawing and the maintenance people started to put in the blinds (opening the lines to put them in).

The accident: Having started this operation, all of a sudden, they smell some gas odour and called the shift supervisor. They find out that a valve on a small line has not been closed. They close the valve and decided to flush 5 additional times. After that and while monitoring the depressurisation of the vessel via the manometer on the outside of the tank (from zero to 25 bars, impossible to read lower that 0.5), they opened the manhole. A whistling sound has been heard indicating a residual pressure in the vessel. When the noise was ended, they continued to open the manhole. At a certain moment the manhole was sprang heavily out by the residual pressure in the vessel, it was ejected and fell to the ground striking two employees.

Lesson Learned:

- The application of the procedure has to be strictly followed and supervised.
- Monitoring has to be done using multiple devices or means, so as to be sure of the indicators.
- The equipment handling has to be done using the principles of inherent safety.

Incident Investigation and Reporting



1. What is an *incident investigation*?
2. How does incident investigation fit into PSM?
3. What kinds of incidents are investigated?
4. When is the incident investigation conducted?
5. Who performs the investigations?
6. What are some ways to investigate incidents?
7. How are incident investigations documented?
8. What is done with findings & recommendations?

Findings and recommendations

What is the most important product of an incident investigation?

1. The incident report
2. Knowing who to blame for the incident
3. Findings and recommendations from the study

Findings and recommendations

What is the most important product of an incident investigation?

1. The incident report
2. Knowing who to blame for the incident
3. **Findings and recommendations from the study**
4. **The actions taken in response to the findings and recommendations from the study**

Findings and recommendations

Example form to document recommendations:

ORIGINAL STUDY FINDING / RECOMMENDATION			
Source: ☐ PHA ☐ Incident Investigation ☐ Compliance Audit ☐ Self-Assessment ☐ Other			
Source Name			
Finding No.		**Risk-Based Priority** *(A, B, C or N/A)*	
Finding / Rec-ommendation			
Date of Study or Date Finding / Recommendation Made			

Aids for recommendations

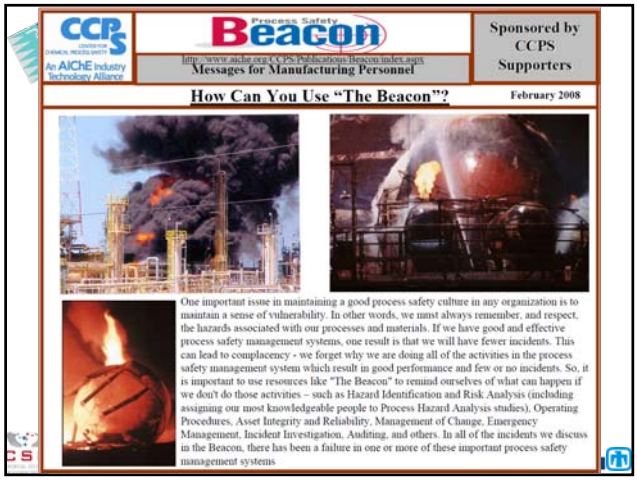
Overriding principles (Crowl and Louvar 2001, p. 528)**:**

- **Make safety [and security] investments on cost and performance basis**
- **Improve management systems**
- **Improve management and staff support**
- **Develop layered recommendations, especially to eliminate underlying causes**

Aids for recommendations

Overriding principles:

- **Make safety [and security] investments on cost and performance basis**
- **Improve management systems**
- **Improve management and staff support**
- **Develop layered recommendations, especially to eliminate underlying causes and hazards**



CCPS Center for Chemical Process Safety — An AIChE Industry Technology Alliance

Process Safety Beacon

http://www.aiche.org/CCPS/Publications/Beacon/index.aspx

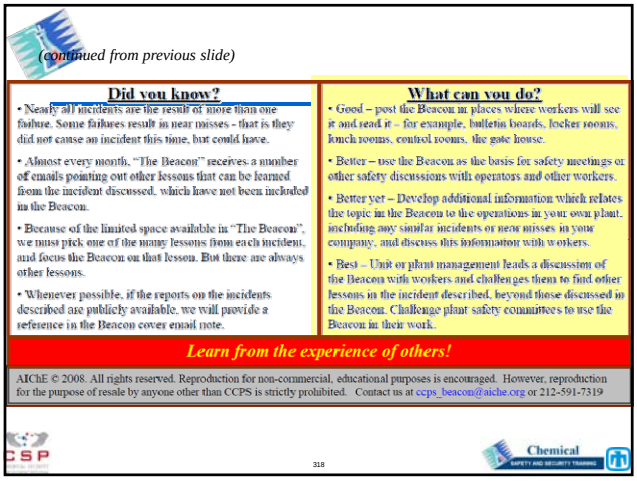
Messages for Manufacturing Personnel

Sponsored by CCPS Supporters

How Can You Use "The Beacon"?

February 2008

One important issue in maintaining a good process safety culture in any organization is to maintain a sense of vulnerability. In other words, we must always remember, and respect, the hazards associated with our processes and materials. If we have good and effective process safety management systems, one result is that we will have fewer incidents. This can lead to complacency - we forget why we are doing all of the activities in the process safety management system which result in good performance and few or no incidents. So, it is important to use resources like "The Beacon" to remind ourselves of what can happen if we don't do those activities – such as Hazard Identification and Risk Analysis (including assigning our most knowledgeable people to Process Hazard Analysis studies), Operating Procedures, Asset Integrity and Reliability, Management of Change, Emergency Management, Incident Investigation, Auditing, and others. In all of the incidents we discuss in the Beacon, there has been a failure in one or more of these important process safety management systems.



(continued from previous slide)

Did you know?

- Nearly all incidents are the result of more than one failure. Some failures result in near misses - that is they did not cause an incident this time, but could have.
- Almost every month, "The Beacon" receives a number of emails pointing out other lessons that can be learned from the incident discussed, which have not been included in the Beacon.
- Because of the limited space available in "The Beacon", we must pick one of the many lessons from each incident, and focus the Beacon on that lesson. But there are always other lessons.
- Whenever possible, if the reports on the incidents described are publicly available, we will provide a reference in the Beacon cover email note.

What can you do?

- Good – post the Beacon in places where workers will see it and read it – for example, bulletin boards, locker rooms, lunch rooms, control rooms, the gate house.
- Better – use the Beacon as the basis for safety meetings or other safety discussions with operators and other workers.
- Better yet – Develop additional information which relates the topic in the Beacon to the operations in your own plant, including any similar incidents or near misses in your company, and discuss this information with workers.
- Best – Unit or plant management leads a discussion of the Beacon with workers and challenges them to find other lessons in the incident described, beyond those discussed in the Beacon. Challenge plant safety committees to use the Beacon in their work.

Learn from the experience of others!

AIChE © 2008. All rights reserved. Reproduction for non-commercial, educational purposes is encouraged. However, reproduction for the purpose of resale by anyone other than CCPS is strictly prohibited. Contact us at ccps_beacon@aiche.org or 212-591-7319

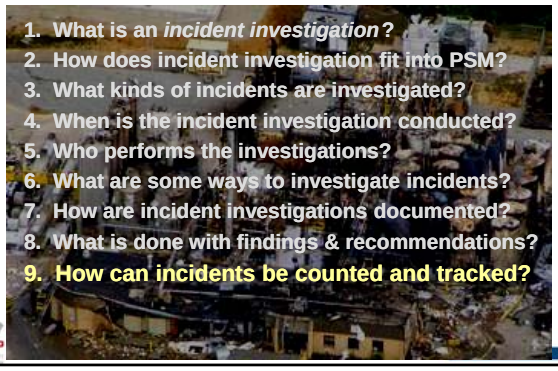
Implementation

As for PHA action items,

a system must be in place to ensure all incident investigation action items are completed on time and as intended.

- **Same system can be used for both**
- **Include regular status reports to management**
- **Communicate actions to affected employees**

Incident Investigation and Reporting



1. What is an *incident investigation*?
2. How does incident investigation fit into PSM?
3. What kinds of incidents are investigated?
4. When is the incident investigation conducted?
5. Who performs the investigations?
6. What are some ways to investigate incidents?
7. How are incident investigations documented?
8. What is done with findings & recommendations?
9. How can incidents be counted and tracked?

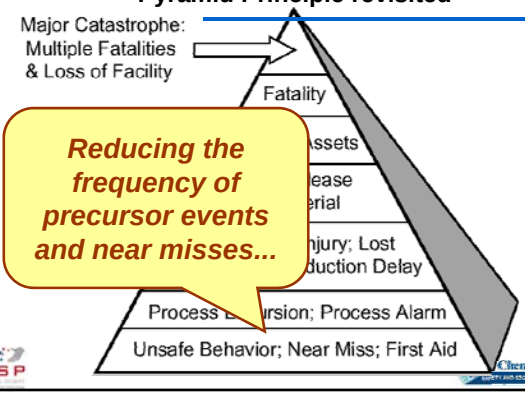
How can incidents be counted and tracked?

- **"Lagging indicators"** — ***actual loss events***
  - **Major incident counts and monetary losses**
  - **Injury/illness rates**
  - **Process safety incident rates**

How can incidents be counted and tracked?

- "Lagging indicators" — *actual loss events*
  - Major incident counts and monetary losses
  - Injury/illness rates
  - Process safety incidents rate
- **"Leading indicators"** — ***precursor events***
  - **Near misses**
  - **Abnormal situations**
    - **E.g., Overpressure relief events**
    - **Safety alarm or shutdown system actuations**
    - **Flammable gas detector trips**
  - **Unsafe acts and conditions**
  - **Other PSM element metrics**

Pyramid Principle revisited



Reducing the frequency of precursor events and near misses...

Pyramid Principle revisited

… will reduce the likelihood of a major loss event

Additional resources

- AIChE *Loss Prevention Symposium,* Case Histories session (every year)
- www.csb.gov reports and videos
- CCPS 2008b, Center for Chemical Process Safety, ***Incidents that Define Process Safety***, NY: American Institute of Chemical Engineers
- CCPS, "**Process safety leading and lagging metrics – You don't improve what you don't measure**," available at www.aiche.org/uploadedFiles/CCPS/Publications/CCPS_ProcessSafety2011_2-24.pdf