



# Principles of Security

Indonesia  
December 2011

SAND No. 2010-2286C  
Sandia is a multprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,  
for the United States Department of Energy's National Nuclear Security Administration  
under contract DE-AC05-04OR21400.





## 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?



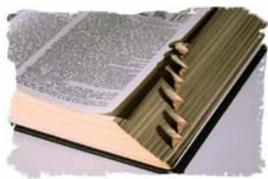







## Security Definition

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





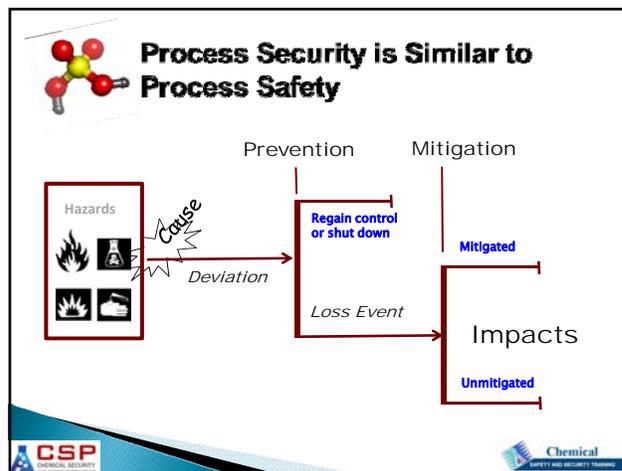


## Security Objective

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




## 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



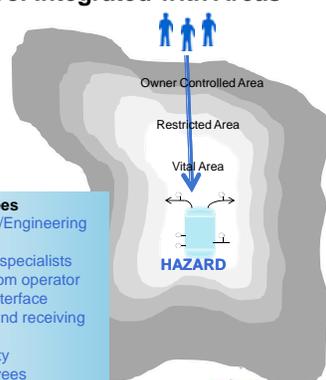
## Access Control Integrated with Areas and People

### Plant locations

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

### Plant employees

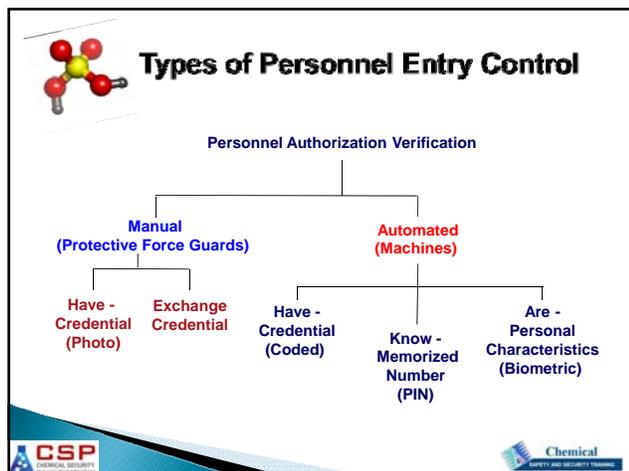
Administration /Engineering  
Operations  
Computer specialists  
Control room operator  
Process interface  
Shipping and receiving  
Maintenance  
Security / Safety  
Special employees



## 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





## 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

**CSP** CHEMICAL SECURITY  
UNIVERSITY OF CALIFORNIA

**Chemical**  
SAFETY AND SECURITY TRAINING

## 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

**CSP** CHEMICAL SECURITY  
UNIVERSITY OF CALIFORNIA

**Chemical**  
SAFETY AND SECURITY TRAINING

## Principles of Physical Security



General Principles followed to help ensure effective, appropriate security

- Defense in Depth
- Balanced Security
- Integrated Security
- Managed Risk

**CSP** CHEMICAL SECURITY  
UNIVERSITY OF CALIFORNIA

**Chemical**  
SAFETY AND SECURITY TRAINING

## Principle 1: Defense in Depth



- Layers
  - Physical
  - Administrative and Programmatic




**CSP**  
CHEMICAL SECURITY  
REGULATORY PROGRAM

**Chemical**  
SAFETY AND SECURITY TRAINING

## Principle 2: Balanced Protection



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

**CSP**  
CHEMICAL SECURITY  
REGULATORY PROGRAM

**Chemical**  
SAFETY AND SECURITY TRAINING

## 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



**CSP**  
CHEMICAL SECURITY  
REGULATORY PROGRAM

**Chemical**  
SAFETY AND SECURITY TRAINING

## Principle 3: System Integration



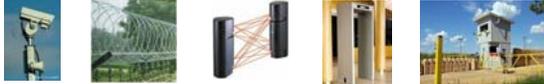
- Detection alerts Response
- Access Delay slows the adversary to provide time for Response
- Response prevents the consequence



**CSP**  
CHEMICAL SECURITY  
REGULATORY PROGRAM

**Chemical**  
SAFETY AND SECURITY TRAINING

## 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

**CSP** CHEMICAL SECURITY EDUCATIONAL PROGRAM

Chemical SAFETY AND SECURITY TRAINING

## Principle 4: Managed Risk



How much Security is enough ???



Cost of Security

Benefit of Security

**CSP** CHEMICAL SECURITY EDUCATIONAL PROGRAM

Chemical SAFETY AND SECURITY TRAINING

## Managed Risk

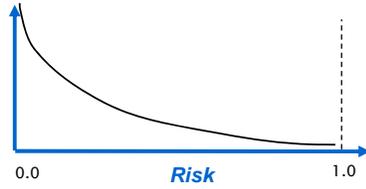


- Benefits of Security is Reduced Risk
- What is Risk?
  - Risk = Consequence Severity \* Probability of Consequence
- What is Security Risk?
  - Probability of Consequence Occurrence  $\Rightarrow$ 
    - Frequency of attempted event
    - Probability of successful attempt
  - Probability of successful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

**CSP** CHEMICAL SECURITY EDUCATIONAL PROGRAM

Chemical SAFETY AND SECURITY TRAINING

## 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

**CSP** CHEMICAL SECURITY EDUCATIONAL PROGRAM

Chemical SAFETY AND SECURITY TRAINING



## 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

**CSP** CHEMICAL SECURITY EDUCATIONAL PROGRAM

**Chemical** SAFETY AND SECURITY TRAINING



## 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

**CSP** CHEMICAL SECURITY EDUCATIONAL PROGRAM

**Chemical** SAFETY AND SECURITY TRAINING



## Performance-Based Security

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



**CSP** CHEMICAL SECURITY EDUCATIONAL PROGRAM

**Chemical** SAFETY AND SECURITY TRAINING



## 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





**CSP** CHEMICAL SECURITY EDUCATIONAL PROGRAM

**Chemical** SAFETY AND SECURITY TRAINING



## 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

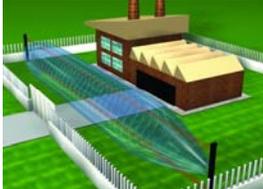




## Define the Threats

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 (DBT) is a formalized approach to develop a threat-based design criteria
- ▶ 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

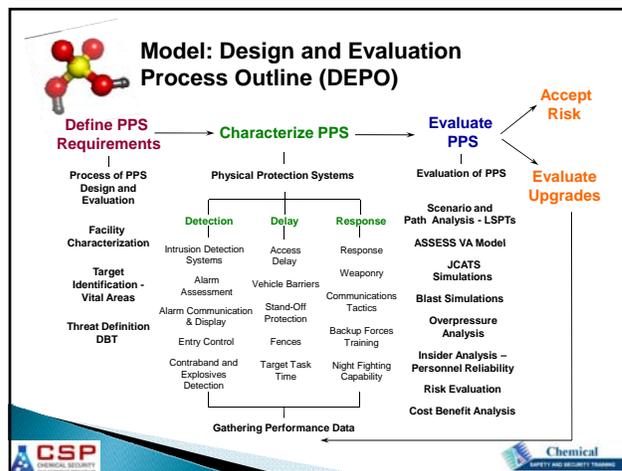





## Objectives

- 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






## 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

