## Principles of Security

**Indonesia**  
**December 2011**

### 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

### 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

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

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

Manual (Protective Force Guards)
- Have - Credential (Photo)
- Exchange Credential
- Know - Memorized Number (PIN)
- Are - Personal Characteristics (Biometric)

Automated (Machines)
- Have - Credential (Coded)
- Know - Memorized Number (PIN)
- Are - Personal Characteristics (Biometric)

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

  ![Diagram of Layers]

  - Mitigation of Consequences
  - Physical Security
  - Personnel Reliability
  - Pre-Event Intelligence
  - Deterrence Program

**Principle 2: Balanced Protection**

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

  ![Diagram of Protection Elements]

  - Protected Area
  - Controlled Building
  - Controlled Room
  - Target Enclosure
  - Target

  - Path 1
  - Path 2

**Principle 3: System Integration**

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

![Diagram of Protection Elements]
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

How much Security is enough??

Benefits of Security is Reduced Risk

What is Risk?
- Risk = Consequence Severity * Probability of Consequence

What is Security Risk?
- Probability of Consequence Occurrence
  - Frequency of attempted event
  - Probability of successful attempt

Probability of successful attempt is
- 1 - Probability of security system effectiveness

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
Characterize the facility considering:

- Mission
- Operations
- Budget
- Safety
- Legal Issues
- Regulatory Issues

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

What are possible sources of unacceptable consequences?

- Dispersal
  - Identify areas to protect
- Theft
  - Identify material to protect

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.

Design Basis Threat

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
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

- 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