Chemical

SAFETY AND SECURITY TRAINING

Chemical Industry Safety and Security

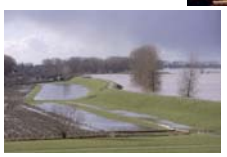
Principles of Security

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

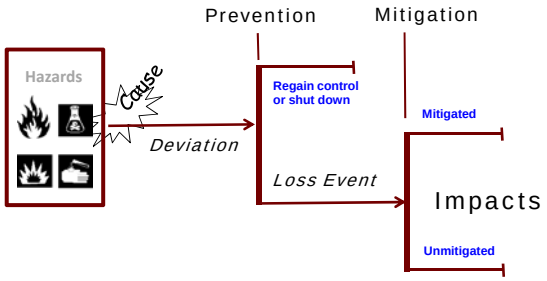
Security is:

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

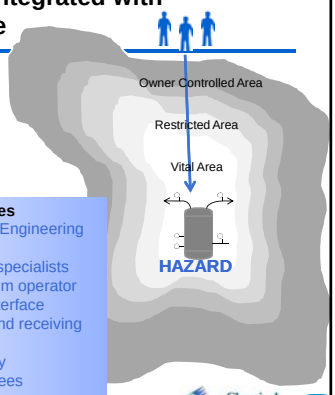
Source: DHS Chemical Security Awareness Training

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

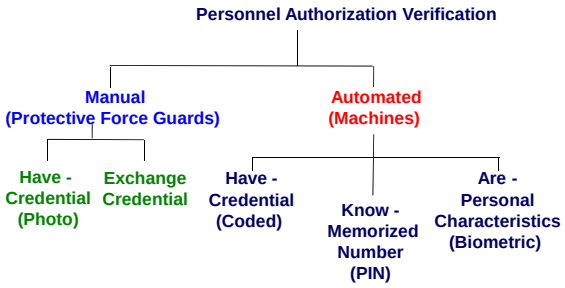
Maintenance
Security / Safety
Special employees



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

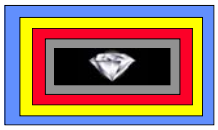
Principles of Physical Security

- General Principles followed to help ensure effective, appropriate security

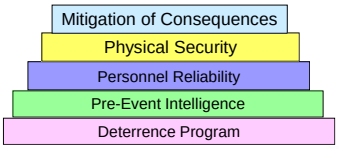
1. Defense in Depth
2. Balanced Security
3. Integrated Security
4. Managed Risk

Principle 1: Defense in Depth

- Layers
  - Physical

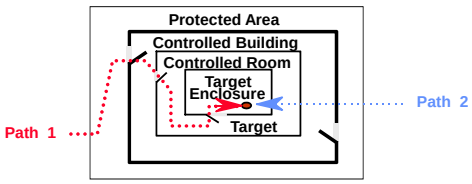


  - Administrative and Programmatic



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??

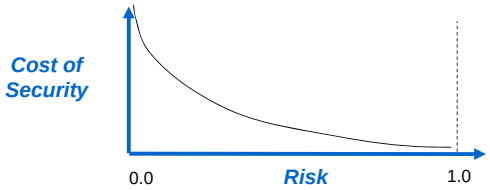
Cost of Security

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??

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

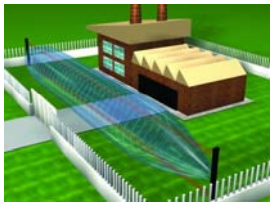
The Physical Protection System Must Have a Basis for Design

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



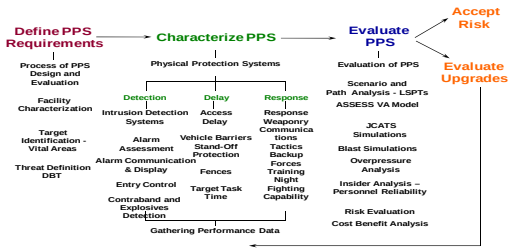
Design Basis Threat

- 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 Safety and Security in the Chemical Industry-the Business Case

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

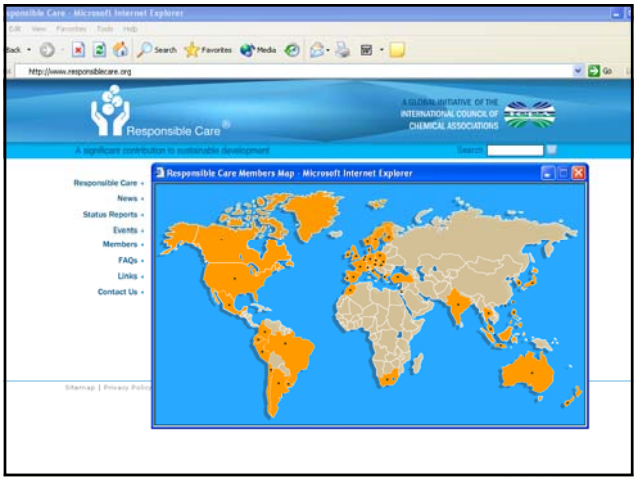
- **Protecting employees, communities and assets from accidents or deliberate actions** is critical to a competitive global chemical industry and to your reputation
- **While different, safety and security practices combine to maximize protection of sites and supply chain**
- **The industry commitment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

What is 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**
- **Mandatory for all American Chemistry Council (ACC) members**
- **Through the International Council of Chemical Associations (ICCA), Responsible Care is being practiced at over 80% of the chemical industry world wide**

Responsible Care® Globally

- **Responsible Care Global Charter (signed February 2006) formalizes broad areas of consistency, defines core Responsible Care elements…a common denominator**
  - **Upgrades performance commitments**
  - **Integrates with sustainable development**
  - **Aims to meet varied needs of individual countries**
- **Each country provides their own tailored program built on the shared basis of the Charter**



American Chemistry Council Member Performance

- Since 1988, US has reduced air, land, water emissions 80%
- Responsible Care® companies' employee safety record is more than 4.5 times safer than the U.S. manufacturing average and twice as safe as rest of the U.S. chemical industry
- Reduced process safety incidents 45% in the last decade
- Since 1995, the number of distribution incidents among Responsible Care® member companies declined 45%, while the volume of chemicals shipped increased 11% for the business of chemistry overall
- Reduced greenhouse gas intensity by over 30% since 1992
- These efforts result in improved 1) public perception, 2) productivity 3) product quality and 4) business performance/sales for the companies

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

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

Common Threads with Federal Programs

- Federal Rules – Chemical Facility Anti-Terrorism Standards, Coast Guard Maritime Transportation Security Act, Customs-Trade Partnership Against Terrorism and Responsible Care® share the following:
  - 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

- Numerous risk-based vulnerability assessment tools to determine risk are readily available and free to anyone – http://www.americanchemistry.com/s_rctoolkit/index.asp
- 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

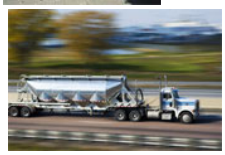
- Security starts with careful screening to hire trustworthy and qualified personnel
  - Personnel identification (e.g., photo ID checks; employee and visitor badges; biometrics)
  - Hand carried items inspection (e.g., visual inspections; x-ray inspections; metal detectors)
- Most threats occur from 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

Business Results

- **US Department of Homeland Security SAFETY Act Designation –**
  - **Recognition of Responsible Care® Security Code as an anti-terrorism technology**
  - **Limits the liability of companies that follow the Responsible Care® Security Code**

Business Results

- **Reduced Insurance premiums for Responsible Care® companies**
- **The Security Code was deemed equivalent to the US Coast Guard Security Rules**
- **The Security Code was the model used for both Federal and State level Security programs**
  - **Reduces additional regulatory costs**
  - **Familiarity with the systems improves compliance**
  - **Significant public and government good will for the early action – improves operating environment**

Resources

- While it makes good business sense, security doesn't come without cost and smaller businesses in particular look for support
- There are numerous guidance documents and approved methodologies/vulnerability assessments that may assist you in developing security practices on site and through your supply chain.
- Government entities are often willing to partner with industry to support training in security/safety enhancements such as the U.S State Department CSP program
- Mentoring programs between larger and smaller companies are prime examples of how these programs can work