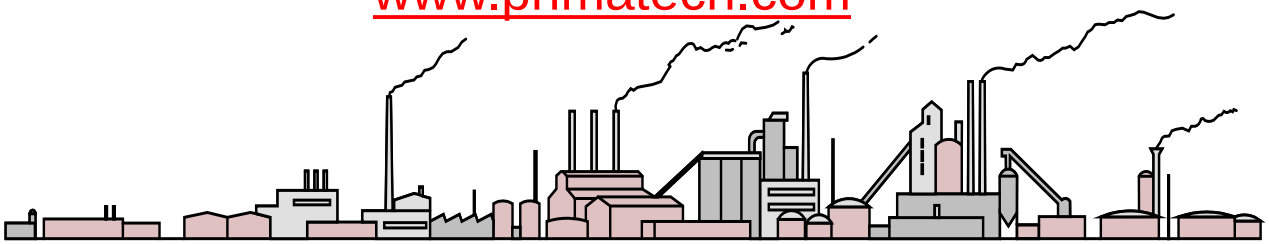
INHERENT SAFETY AND SECURITY

Paul Baybutt, Primatech Inc.

Presented at the seminar on Safer Facilities:
Chemical Security and Hazard Reduction,
Cuyahoga County LEPC,
Berea, Ohio, May 24, 2006

paulb@primatech.com
www.primatech.com



OUTLINE

- Background
- Definition of inherent safety
- Requirements
- Guidance
- Examples
- Inherent security principles

"There is one thing more painful than
learning from experience,
and that is not learning from experience."

Anon

BACKGROUND

- Use of inherently safer / securer technologies (IST) is a key element in managing safety and security
- Government legislation and regulations favor use of IST
  - New Jersey, Best Practices Standards at TCPA / DPCC Chemical Sector Facilities November, 2005

NJ DEFINITION OF IST

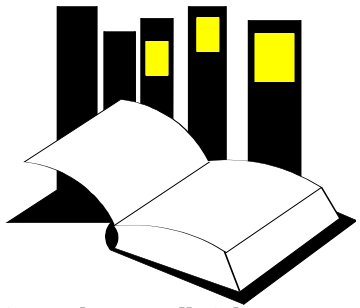
- Principles or techniques incorporated in a process to minimize or eliminate the potential for a hazardous substance release including:
  - Reducing inventories
  - Substituting less hazardous materials
  - Using less hazardous process conditions or chemical forms
  - Designing equipment and processes to minimize the potential for equipment failure and human error

NJ REQUIREMENTS - IST

- Review the practicability and potential for adopting inherently safer technology (IST)
- Analyze whether adoption of IST alternatives is practicable
- Provide the basis for any determination that IST implementation is impracticable
- IST review must be conducted by a qualified expert in chemical process safety
- Prepare a report

NJ GUIDANCE

- Review method not specified
  - Consider process hazard analysis
  - Evaluate the process cycle as a whole and specific sections and pieces of equipment
  - Expect that research required to identify available IST alternatives
- Recognizes challenge of implementing IST for operating plants
  - Practicability and cost effectiveness



NJ GUIDANCE (CONTD.)

- Address 3 questions for each of the four types of IST:

1. Are there any available IST alternatives over the current process? If so, what are they?

2.A Is adoption of IST alternatives practicable?

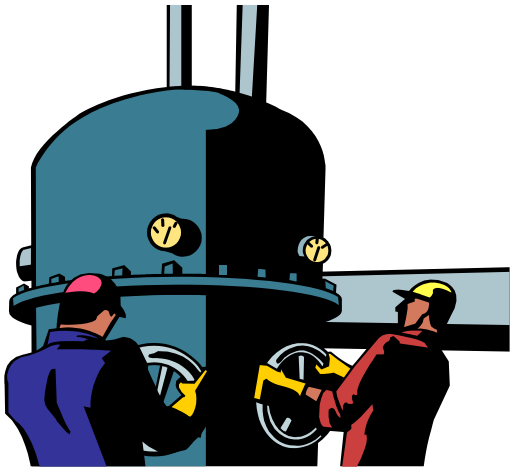
2.B What is the basis for any determination that implementation of IST is impractical?

3. What past IST and risk reduction measures have already been incorporated into the current process?

Inherently Safer Chemical Processes – A Life Cycle Approach, AIChE/CCPS, 1996

QUESTION 2.A Is adoption of IST alternatives practicable?

- Technology should have been successfully proven in commercial or pilot operation
- Any unproven technology should be reviewed and evaluated so that additional hazards are not introduced into the process



QUESTION 2.B What is the basis for determination that IST implementation is impractical?

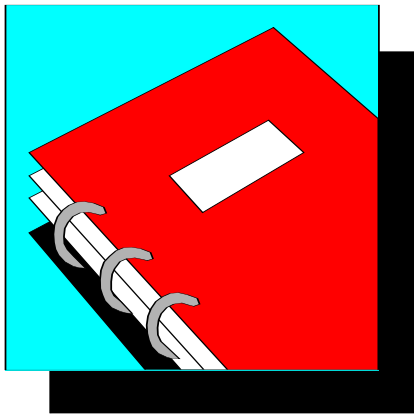
- Real life problems or conditions present to support the determination must be documented, e.g. an IST alternative:
  - Provides an extremely low yield in a reaction process
  - Introduces a more serious hazard
  - “Technology should be available at reasonable cost commensurate with the anticipated reduction or elimination of the hazard”
    - Provide costs to install and operate alternatives

QUALIFIED EXPERT

- No definition provided
- NJDEP suggests team participate in the review
- Provide expertise in:
  - Chemistry
  - Engineering
  - Process controls and instrumentation
  - Maintenance
  - Production and operations
  - Chemical process safety

IST REVIEW REPORT

- Document all the findings
- Include past IST and risk reduction measures
- Provide schedule for implementation of IST measures



IST EXAMPLES – INVENTORY REDUCTION

- Conversion of a batch to a continuous process
  - Eliminated the need for an intermediate storage tank
- Generation of hazardous materials as needed, e.g. phosgene, chlorine, sulfur dioxide, sulfur trioxide
  - Eliminated need for storage of the material

IST EXAMPLES - SUBSITUTION

- Replace chlorine in water / waste water treatment using:
  - Sodium hypochlorite
  - Ozone
  - Other disinfectant chemicals
  - UV light

IST EXAMPLES – LESS HAZARDOUS CONDITIONS / FORMS

- Using refrigerated materials under atmospheric pressure instead of under pressure
- Using diluted materials instead of the pure form
- Using hot water or steam for heating instead of flammable oil

INHERENT SECURITY PRINCIPLES

- Perception
- Information
- Layout
- Design
- Safeguards
- Computers
- Buffer zones

Inherent Security: Protecting Process Plants Against Threats, P. Baybutt, Chemical and Engineering Progress, 2003.

INHERENT SECURITY PRINCIPLES - PERCEPTION

- Plants should control how much attention they attract
  - Those visible from highways are more likely to be targeted
  - Buffer zones and setbacks can help
- Plants with prominent signage are more readily identified
- Vessels and tanks visible from outside the plant are more likely to be targeted
  - Placement in buildings or behind screens may help
- Locations close to population centers and transportation are more likely to attacked
- Avoidance of publicity may also avoid attracting the attention of adversaries

INHERENT SECURITY PRINCIPLES - INFORMATION

- Information on hazardous materials is needed by adversaries to plan an attack
  - Try to ensure they do not obtain it
- The less information available on a facility, the more secure it will be
  - Control information on chemicals handled, inventories, deliveries, capacities of tanks and vessels, and locations
- Ensure your marketing and PR departments do not inadvertently disclose sensitive information
  - Beware of the Internet!
- Be careful with in-plant signs
  - Make it easier for intruders to identify specific targets
- Balance right-to-know with need-to-know for local communities and the media

INHERENT SECURITY PRINCIPLES - LAYOUT

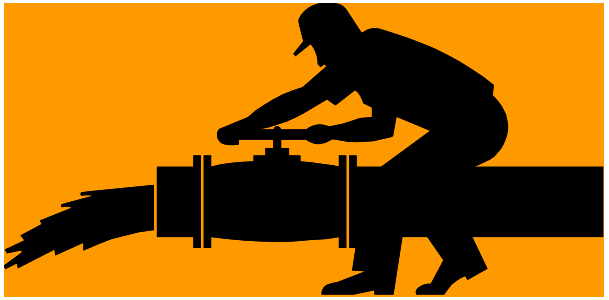
- Generally, locate sensitive areas close to the center of the plant where they will be less vulnerable
- Keep hazardous materials zones and sight lines free from obstructions to facilitate the detection of unauthorized personnel
- Disabling utilities and control systems may cause releases
  - Place them where they are difficult for intruders to locate and access

INHERENT SECURITY PRINCIPLES - DESIGN

- Where possible, avoid weak points such as sight glasses and flex hoses
- Consider whether tanks and vessels can be protected against airborne and propelled explosive devices and projectiles, e.g.
  - More robust designs
  - Increased wall thickness
  - Internal baffles
  - Double-walled construction
  - Mounding
  - Underground installation

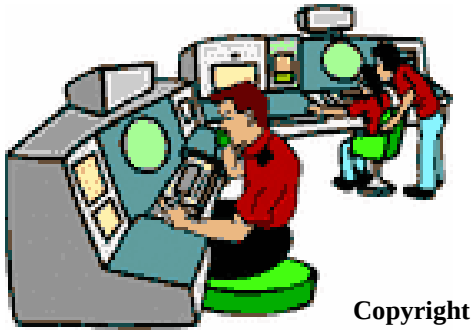
INHERENT SECURITY PRINCIPLES - SAFEGUARDS

- Attacks may involve disabling safeguards immediately prior to causing a hazardous material release
- Some safeguards are more readily disabled than others, e.g.
  - Fire water tanks are less secure than lagoons
  - Below grade dikes are more secure than dikes at grade level



INHERENT SECURITY PRINCIPLES - COMPUTERS

- Be careful of Internet connections to process control networks
  - What is not connected cannot be manipulated
- Ensure business and enterprise networks are protected from cyber attacks to obtain information for planning a physical attack
- Design process control systems to prevent misuse by insiders

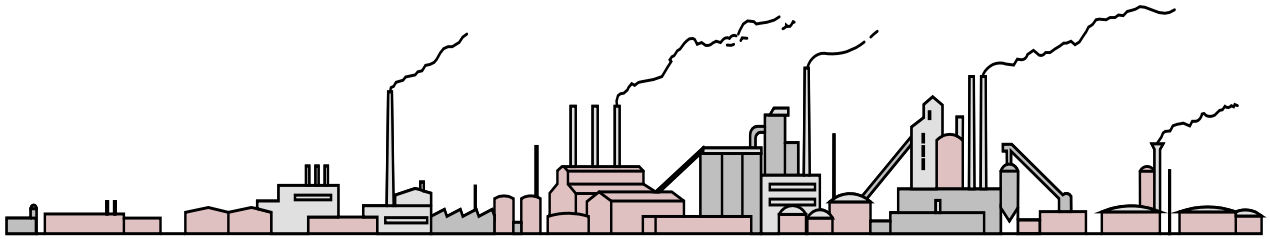


INHERENT SECURITY PRINCIPLES – BUFFER ZONES

- Provide separation for a facility from surrounding areas and sensitive populations
  - Makes it harder to locate and attack a facility
  - Also provides some protection in the event of a release
  - Ideally, follow appropriate setback guidelines

SUMMARY

- Both inherent safety and inherent security approaches should be used
  - Including for operating facilities
- Formal review is desirable
  - Required in NJ
- Consider tradeoffs between safety and security



FURTHER INFORMATION

- Technical papers on safety and security:
  - www.primatech.com
- Contact info:
  - paulb@primatech.com