ICE 10.490
CHEMICAL PROCESS SAFETY
Inherently Safe Design and Life Cycle Risk Management

E.M. Drake
MIT Energy Initiative
October 12, 2007

Topics Outline

- **Learning by accident!**
- **Hazard Identification**
- **Tools for Safer Design**
- **Risk Assessment and Management**
- **Some References**

LEARNING BY ACCIDENT

Year	Location	Chemical	Fatalities
1769	Frescia, Italy	Gunpowder	>3000
1856	Rhodes, Greece	Gunpowder	>4000
1889	Johnstown, PA	Water (dam failure)	>2000
1921	Oppau, Germany	Ammonium sulfonitrate	>500
1944	Cleveland, OH	Liquefied methane	>100
1947	Texas City, TX	Ammonium nitrate	>400
1971	Iraq	Mercury salts (on wheat seed)	>1000
1984	Brazil	Gasoline (pipeline)	>500
1984	Bhopal, India	Methyl isocyanate	>2000

Environmental Crises: Love Canal, Seveso, Rhine River, Acid Rain…
Health Hazards: Asbestos, Thalidomide, Carcinogens, Toxic Shock….

WHY DO ACCIDENTS HAPPEN??

- **Physical facilities that are inadequately designed, poorly maintained, changed without analysis, etc.**
- **Staff who are unqualified, poorly trained, incapacitated, complacent, disgruntled, etc.**
- **Procedures that are inadequate, inappropriate, or out-of-date, etc.**
- **Management systems that are limited in scope, inflexible, not supportive of open and honest communication, etc.**
- **Focus on short term profitability and denial of risk potential.**
- **External forces: earthquakes, air crashes, storms, terrorism, industrial sabotage, etc.**
- ***Most major accidents have occurred when a facility was not in normal operation (e.g. while being maintained, changed, or when shortcutting normal procedures).***

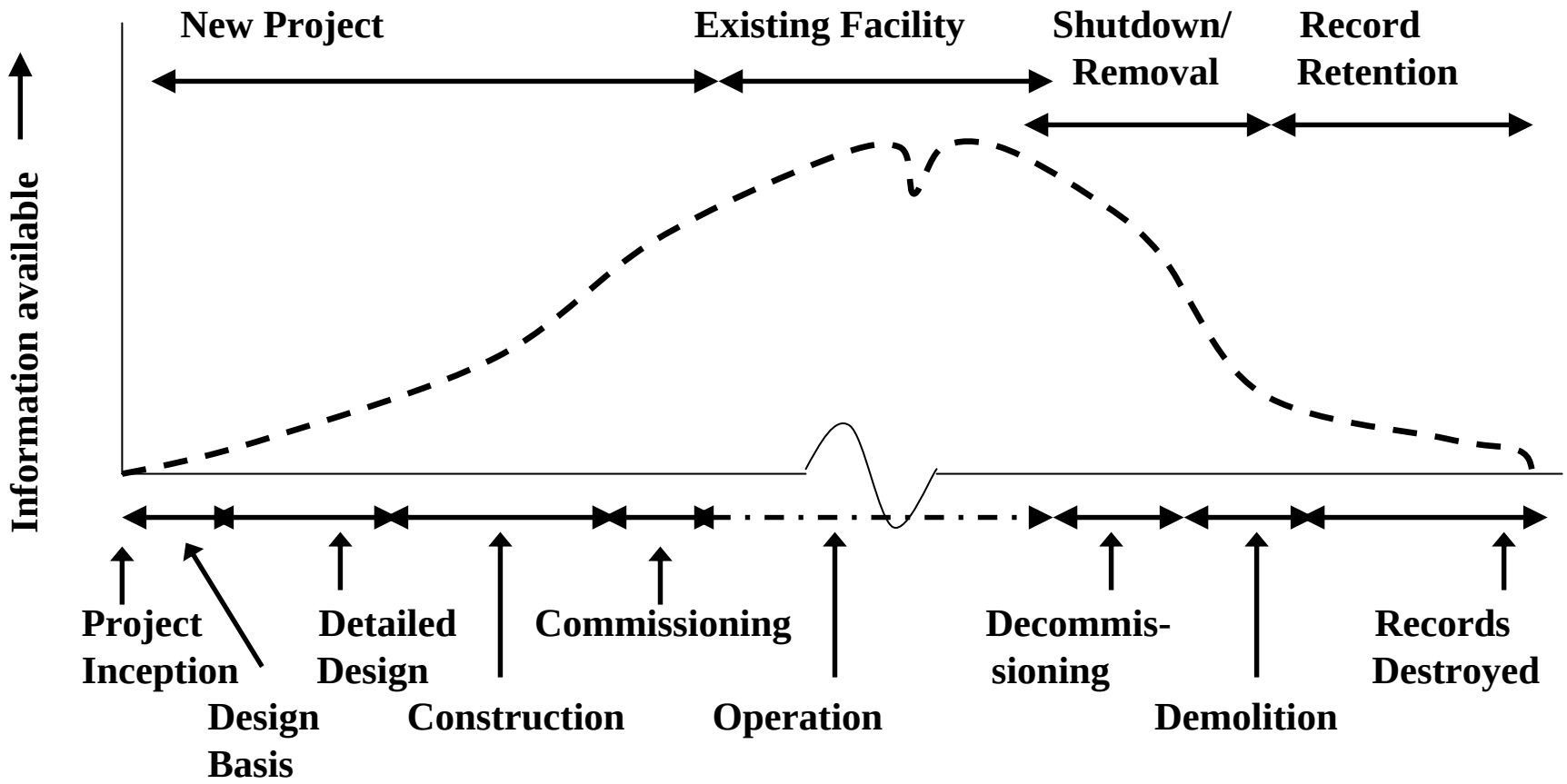
Types of Accidents

- **Fires and explosions**
- **Toxic gas releases**
- **Steam and other hot material releases**
- **Chronic exposure to toxics, radioactivity, carcinogens, mutagens, etc.**
- **Worker accidents during construction, maintenance and operation…**

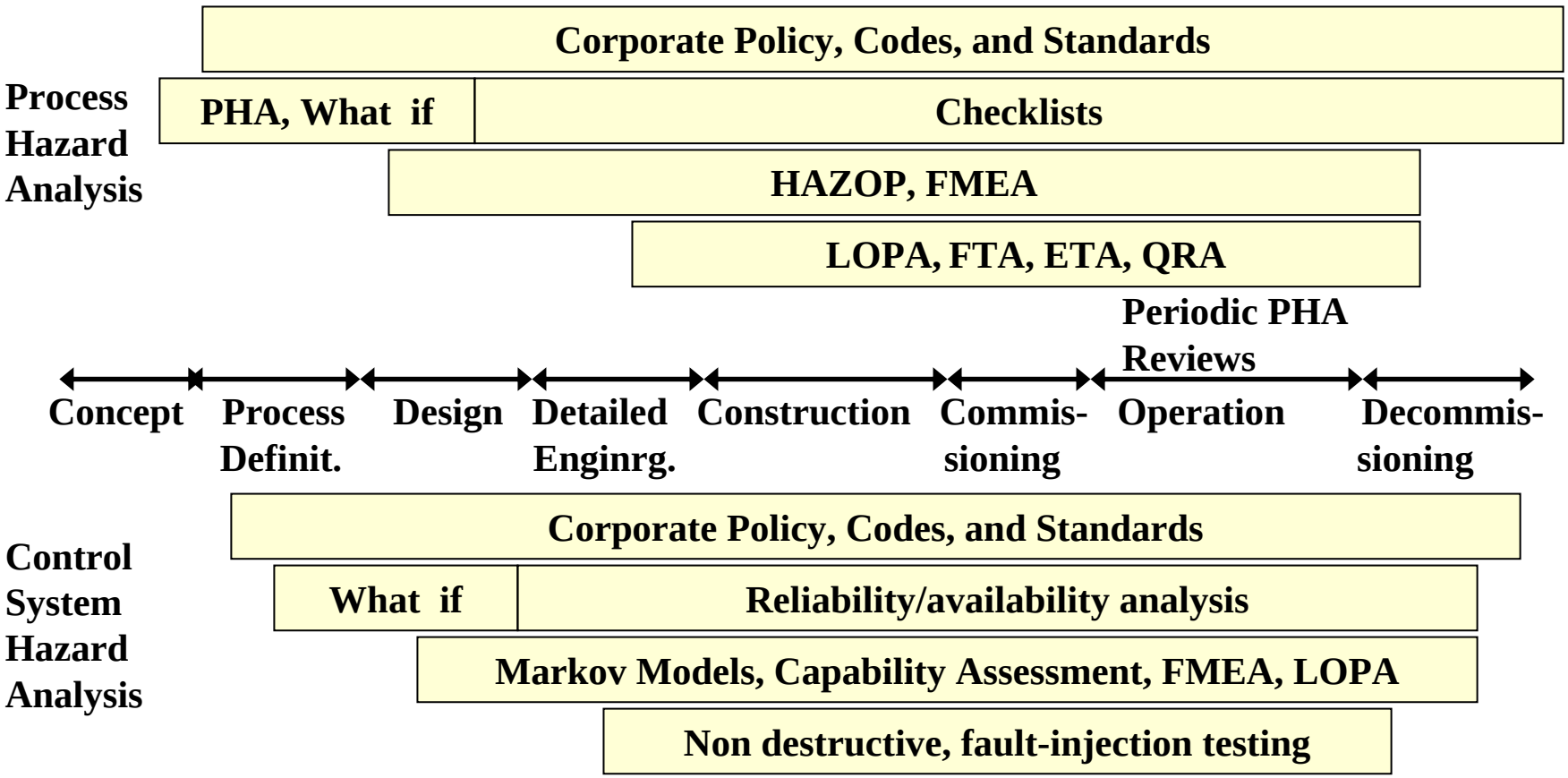
The Fear of Liability

- **Human Life:** Accidents with non-worker loss of life may involve liability > 1 $ million per life
- **Worker injuries:** OSHA imposes fines for worker injuries depending on circumstances - typically around $ 1K+ per incident
- **Environmental incidents:** Typical costs $50K to > $1 million
- **Negligent management is a felony – 5 years jail time in some cases**
- **US Dept. of Justice collected almost $200 million in civil and criminal penalties in 2000**

Process Life Cycle



Tools for Safer Design



Hazard Identification

- **During conceptual/early design stages:**
  - **Past experience**
  - **Analysis of potentially hazardous properties of all chemicals and equipment involved**
  - **Checklists**
  - **General design guidelines**
  - **Codes and standards**
  - **“What – if” Analysis**

Hazard Identification

- **What potentially hazardous chemicals are used?**
- **What quantities might potentially be released?**
- **What might be the consequences?**

  Fire? Explosion? Toxic gas?
- **What are potential impacts? Areas? Deaths? Injuries? Environmental damage? Financial losses?**

"Consequence models" have been developed to estimate impacts – various software packages are available

Safety Philosophies

- **Regulations, codes, and standards**
- **Inherently safe design**
- **Systematic design assessment (HazOp, FMEA)**
- **Protection layers**
- **Risk assessment and acceptability criteria**
- **Life Cycle Risk Management**

Examples of Codes and Standards

- **Industrial**
  - **ASME, API, IEEE, ISA, etc. –codes and standards**
  - **NFPA codes (National Fire Protection Assn.)**
  - **Insurance company requirements**
  - **AIChE/CCPS Guidelines**
  - **Corporate design practices**
  - **Corporate commitment to ISO standards**
- **Government Regulations**
  - **EPA regulations (SARA, RCRA, TSCA, Clean Air/RMP, ….)**
  - **DOT regulations (transportation)**
  - **OSHA regulations (occupational, 29CFR1910 process safety mgmt.)**
- **Local Regulations**
  - **Zoning, Building codes, Permit requirements, Emergency response coordination, …**

Elements of Inherently Safe Design

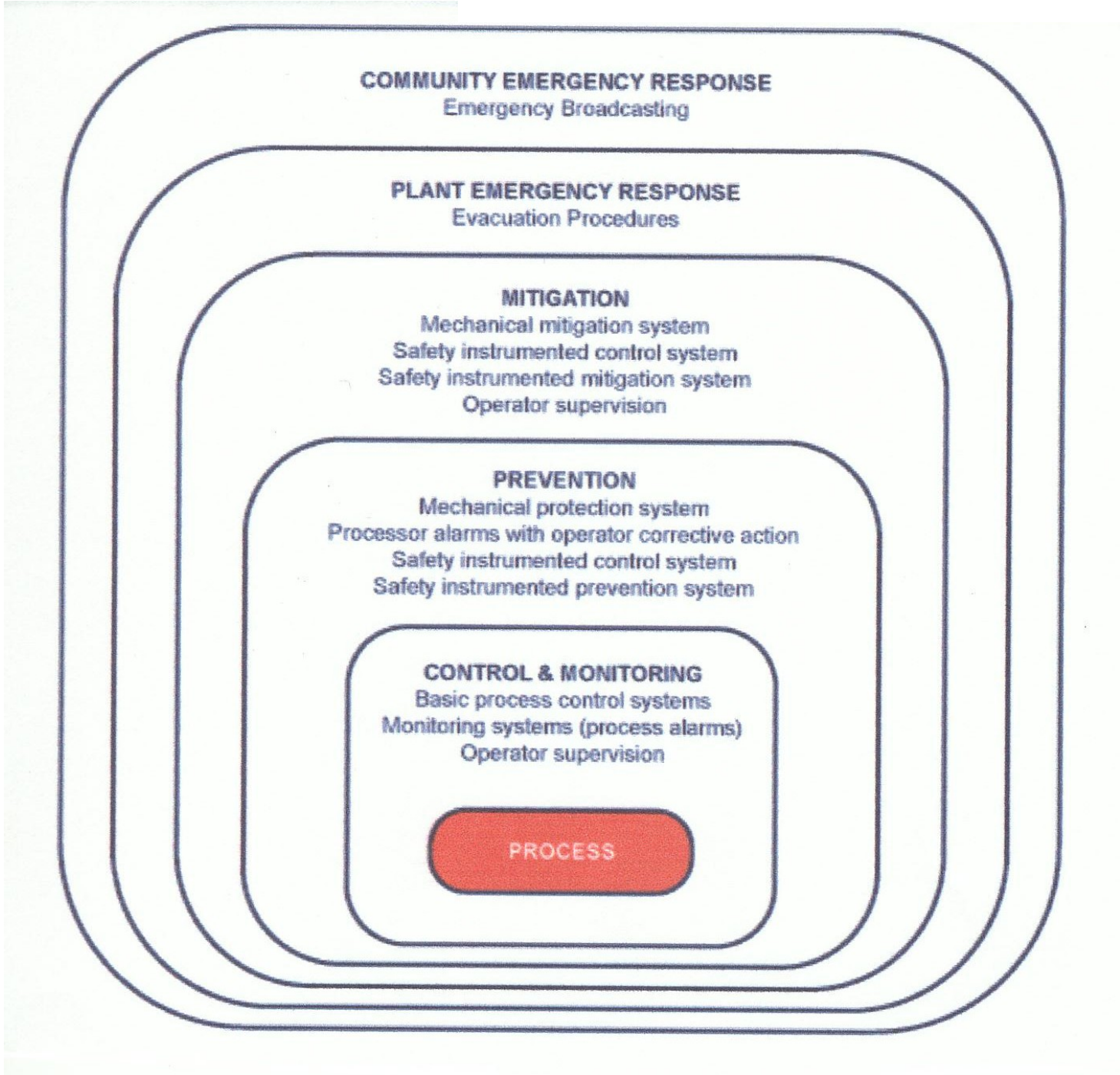
- **Less hazardous materials?**
- **Smaller inventories?**
- **Less severe process conditions?**
- **Use of “fail-safe” or “fault-tolerant” (redundant) safety systems**
- **Preference for passive protection systems over active ones (separation of storage tanks, rather than water deluge protection)**
- **Choice of more durable materials of construction**
- **Design for external perils (wind, seismic, traffic, sabotage, etc.)**
- **Provide for periodic safety reviews through lifetime of facility**
- **Critical evaluation of any “near misses” during commissioning or operation**
- **Critical and comprehensive analysis of any modifications**

Systematic design assessment

- **Hazard and Operability Studies**
  - **Systematic analysis – P&ID based**
  - **Guidewords to search for upset conditions**
  - **Identifies and documents need for additional risk reduction and recommends solutions**
- **Failure Mode and Effects Analysis**
  - **Systematic search of component equipment failure modes**
  - **Identifies need for and documents additional risk reduction requirements**

Level of Protection Analysis

- **Concept:**
  - **Normal process variations are managed by the basic process control system – abnormal excursions occur about 1-10% of the time (90 – 99% reliability)**
  - **Independent alarm and control systems are designed to bring the plant back to a safe condition with about a 90 - 99% reliability**
  - **For critical potential hazards, additional independent protection layers can be added – each with about a 90 – 99% reliability**
- **Accident frequencies can be reduced to desired levels (e.g., frequencies of 10^{-6} per year for major impacts) by addition of independent protection layers**
- **Accident impacts can be reduced by limiting inventories or adding protection systems (e.g., adding a "stopper" to a runaway reaction)**


COMMUNITY EMERGENCY RESPONSE
Emergency Broadcasting
PLANT EMERGENCY RESPONSE
Evacuation Procedures
MITIGATION
Mechanical mitigation system
Safety instrumented control system
Safety instrumented mitigation system
Operator supervision
PREVENTION
Mechanical protection system
Processor alarms with operator corrective action
Safety instrumented control system
Safety instrumented prevention system
CONTROL & MONITORING
Basic process control systems
Monitoring systems (process alarms)
Operator supervision
PROCESS

What is Risk?

The potential for undesired impacts as the result of some event or activity.

Components:	**Frequency (occurrences per year)** **Severity (magnitude of impact)**
Types of impacts:	**Death, injury,** **environmental damage,** **direct financial losses,** **liability, penalties,** **loss of reputation, etc.**

Some risk issues

- **How safe is it? (to workers and neighbors)**
- **Does it meet requirements of relevant codes and insurers?**
- **Is it safe enough?**
- **Will there be opposition? Why?**
- **Do the benefits outweigh the risks? (to whom?)**
- **Should we invest in making it safer?**

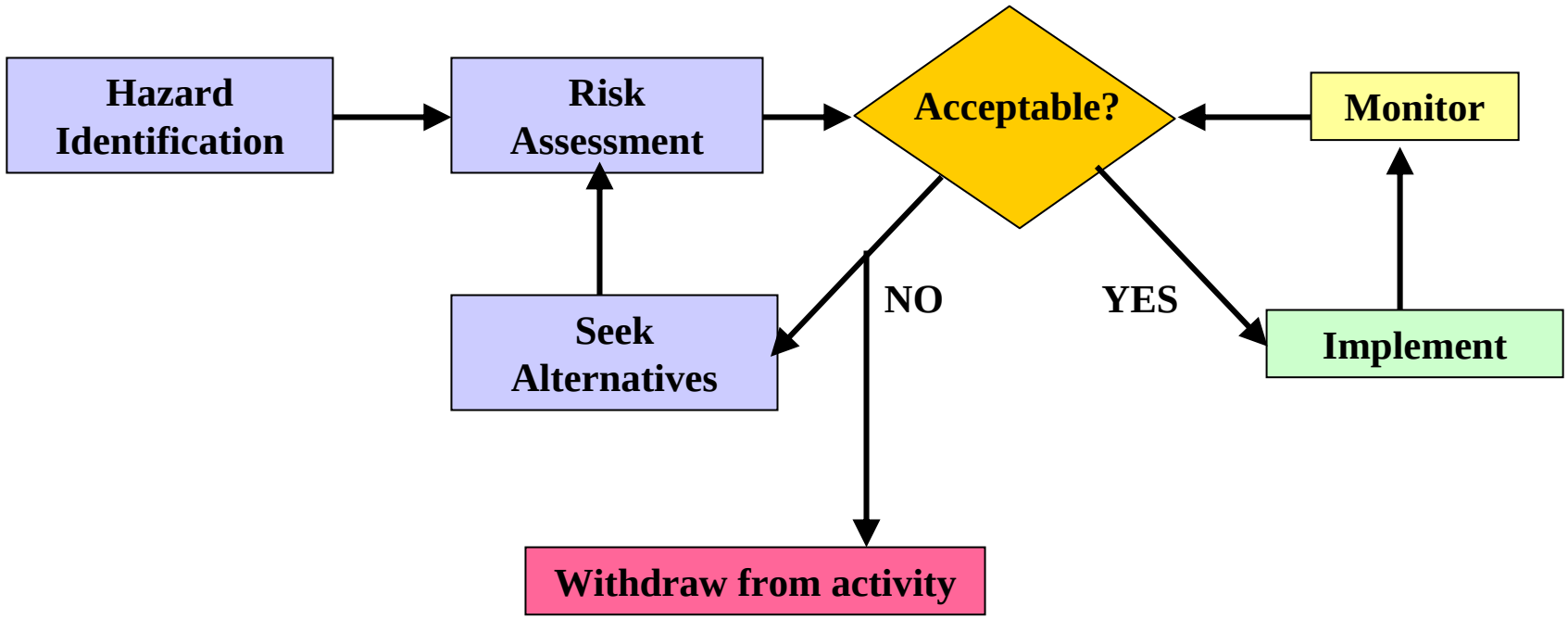
Risk Assessment and Management

- **For facilities where significant hazards are identified, quantification of the likelihood and consequences of such hazards provides a basis for better understanding and ranking risks, as well as providing insights for risk mitigation and management**
- **Quantification is subject to inherent uncertainties – and knowledgeable risk management includes careful recognition of uncertainties and assumptions**

Steps in a Risk Assessment

- **What are the potential hazards?**
- **How severe and how likely is each?**
- **How can they be avoided or controlled?**
- **Is the residual risk acceptable?**
- **How can they be managed through facility lifetime?**
- **What risks are associated with demolition?**
- **Are any legacy risks left after demolition?**

Life Cycle Risk Management



A Framework for Hazard Assessment and Risk Management

- **Project Kick-off meeting**
  - **Attendees: Plant Mgr, Project Mgr, HSE Specialist**
  - **Aim: Establish site specific legal and corporate requirements**
  - **Set management criteria for project and appoint Process Hazards Assessment Team Leader**
- **PHA Team Selection Criteria**
  - **Diverse skills (process design, equipment, controls and instrumentation, operations and maintenance, risk assessment, construction, etc.)**
  - **Independence (between designers and assessors)**

A Framework for Hazard Assessment and Risk Management, cont'd.

- **Stage I: Process Hazards Assessment**
  - **Uses process flowsheets and plant layout for preliminary identification and resolution of any major safety or other issues**
- **Stage II: Preliminary Hazards Assessment**
  - **Uses systematic design tools to evaluate the soundness of the P&IDs and choices of major equipment**

A Framework for Hazard Assessment and Risk Management, cont'd.

- **Stage III: Risk Assessment or LOPA**
  - **Uses final detailed design and equipment specifications, along with operating and maintenance procedures, training programs, emergency response plans, management structures…**
- **Stage IV: Risk Audits and Adjustments**
  - **on an on-going basis throughout the operating life of the plant – and whenever any significant changes are made – through demolition and management of residual risks**

Quantitative Risk Assessment Methods

- **Reliability analysis**
- **Availability analysis**
- **Fault tree analysis**
- **Event tree analysis**
- **Risk profiles**
- **Benchmarking**

System Functioning Analysis

- **Reliability analysis**
  - **Uses failure rate information on each component to estimate subsystem and system reliability and to plan maintenance programs – considers pdfs of failure behavior**
- **Availability analysis**
  - **Used frequently in control and safety system assessment to identify the fraction of the time that the subsystem will be able to perform its design function, considering redundancies, etc.**

Risk Evaluation

- **Fault tree analysis**
  - **Defines a "top event" which is a single source of risk (e.g., a leak of a certain magnitude) and then uses Boolean techniques to map all the potential failure paths that could lead to the top event. Repeated for all identified independent "top events." Likelihoods are assessed for each path using failure or other frequency data**
- **Event tree analysis**
  - **Starts with individual component failures and looks at how failures might propagate to a resulting set of "top events." Similar to fault tree analysis, but useful for identifying common mode failures**

Risk Evaluation, cont'd.

- **Risk profiles**
  - **Individual "top events" are quantified in terms of frequency and risk (e.g., fatalities) and then are combined to produce a cumulative distribution function that plots the frequency of accidents with "n or more" fatalities as a function of "n." Main risk contributors can be ranked by frequency**
- **Benchmarking**
  - **Compares risk profiles with those associated with other activities to gain an idea of relative risk.**

Risk Acceptability?

- **Society (and individuals) accepts a wide range of risks – depending on awareness and on distribution of costs and benefits**
- **Oversight by regulatory authorities – either implicitly or explicitly**
- **Usually up to owner and operator and their insurors, based on experience and judgment**
- **Depends on location, surrounding populations, and nature of risk – along with a wide variety of associated issues (jobs, fear, economic impacts, etc.)**

Sources of Public Fear about Risk

- **Is it necessary?**
- **Is it voluntary?**
- **Have I any control?**
- **Is it fair?**
- **Do I believe in (trust) the decision-makers?**
- **Is it familiar?**
- **Are consequences dread?**
- **Is it complex?**
- **Is it moral?**
- **Is it uncertain?**

Risk Communication

- **Good management commitment to safety**
- **Attitude of continual improvement**
- **Public briefings with discussions**
- **Open participation in public hearings**
- **Cooperation in community emergency planning**
- **Plant visits and emergency drill practices**
- **Honesty about accidents – no CYA!**
- **Encourage employees to be community ambassadors**
- **Funded (expenses paid) community representative in management oversight group**

Philosophy of Life Cycle Risk Management

- **Integrate knowledge of potential future problems into initial design**
- **Treat safety, control systems, process waste minimization, and waste and product disposal as integral parts of design – not as "afterthoughts"**
- **Choose inherently safe or more fault tolerant designs whenever practical**
- **Pay attention to the potential for human error in design, construction, testing, operations, maintenance and management**

Philosophy of Life Cycle Risk Management, cont'd.

- **Take a multidisciplinary team approach to design and design evaluation (process experts, control system experts, experienced operators and maintenance personnel, safety and human factors specialists, management experts, etc.). Have the evaluators reasonable independent of the designers to avoid blind spots.**
- **Invest in quality and proven performance whenever practical (not the cheapest solution!)**

Anticipate and adjust –
avoid learning from disaster!

Some Reading

- **Lees, Frank, *Loss Prevention in the Chemical Industries*, (Vol 1 & 2), Second Edition, Butterworth Architecture, London (1996).**
- **AIChE/CCPS, New York, NY:**
  - ***Inherently Safer Chemical Processes: A Life Cycle Approach***
  - ***Guidelines for Hazard Evaluation Procedures***
  - ***Guidelines for Technical Management of Chemical Process Safety***
  - ***Guidelines for Auditing Process Safety Management Systems***
  - ***Guidelines for Engineering Design for Process Safety***
  - ***Guidelines for Safe Automation of Chemical Processes***
  - ***Guidelines for Safe Storage and Handling of High Toxic Hazard Materials***
  - ***Guidelines for Chemical Process Quantitative Risk Analysis***
  - ***Guidelines for Use of Vapor Cloud Dispersion Models***
  - ***Guidelines for Vapor Release Mitigation***
  - ***Guidelines for Investigating Chemical Process Incidents***
  - ***Guidelines for Process Equipment Reliability Data***
- **Henley, E.J. and H. Kumamoto, *Reliability Engineering and Risk Assessment*, Prentice-Hall, Englewood Cliffs, NJ (1981).**

Some Reading, continued

- **Crowl, D.A. and J.F. Louvar,*Chemical Process Safety: Fundamentals with Applications*, Prentice-Hall, Englewood Cliffs, NJ (1990).**
- **NUREG, *Probabilistic Safety Analysis Procedures Guide*, NUREG/CR-2815, Nuclear Regulatory Commission, Washington, DC (1985).**
- **Sax, N.I. and M.C. Bracken, *Dangerous Properties of Industrial Materials*, 5th Edit., Van Nostrand-Reinhold, New York, NY (1979).**
- **Patty, F.A., *Patty's Industrial Hygiene and Toxicology*, 3rd Edit., Wiley, New York, NY (1985).**
- **Bretherick, L., *Handbook of Reactive Chemical Hazards*, 2nd Edit., Butterworths, Stoneham, MA (1983).**