PROCESS SAFETY ENGINEERING (0905477)
02 – ACCIDENT CAUSATION

ALI KH. AL-MATAR (aalmatar@ju.edu.jo)

The superior man, when resting in safety, does not forget that danger may come…. When all is orderly, he does not forget that disorder may come. Confucius (551 BC – 479 BC)

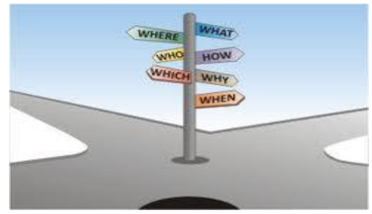
Chemical Engineering Department, University of Jordan
Amman 11942, Jordan

Outline

- Key Questions
- Why do Accidents Occur?
- The Accident Pyramid
- What is an Acceptable Risk?
- Accident Causation Theory
- Heinrich Domino Theory
- Marcum's 7 Domino Sequence of "Misactsidents"

Key Questions

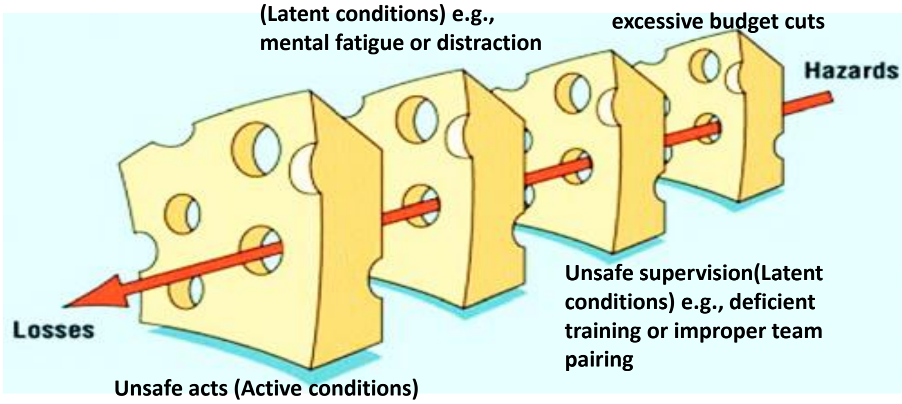
- Why do Accidents occur?
- How do Accidents occur (the nature of accidents)?
- What must we do to keep them from happening?
- When?



Why do Accidents Occur?

- We choose to handle dangerous process **materials**, **conditions** and **energies**
  - To make a living
  - To provide society with desirable products subject to
    - Extreme processing conditions
    - Increased process plant complexity
- As long as we choose to handle them, a potential for loss events exists
  - Things can be done to reduce their **likelihood** and **severity** to negligible or **tolerable** levels.

Reason's Swiss Cheese Model for Accident Causation

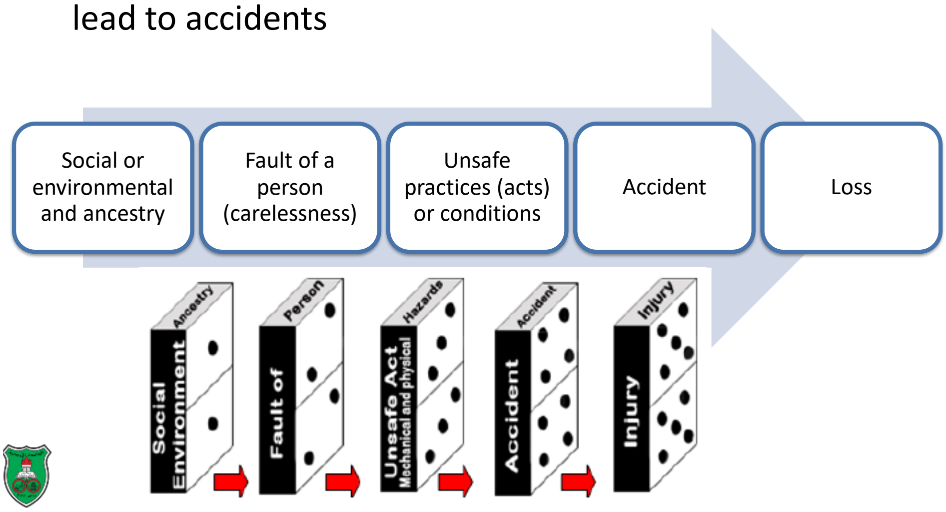


Accident Causation Theory

- "Acts of God"
  - An instance of uncontrollable natural forces in operation.
- "Pilot Error" – beginning of industrial revolution
  - The action or decision of the pilot that, if not caught or corrected, could contribute to the occurrence of an accident or incident, including inaction or indecision.
- "Mismanagement" – current legal leanings
  - The process of managing something badly or wrongly.

Heinrich Domino Theory

- Developed by H.W. Heinrich in 1932.
- Predictable chronological sequence of causal factors lead to accidents



Marcum's 7 Domino Sequence of "Misactsidents"

- Supposes that all accidents can be avoided and that the liability resides with management

1. Inadequate preparation
2. Substandard performance
3. Miscompensated risks
4. Harmful contact incident
5. Adverse reaction
6. Sustained losses
7. Incurred costs

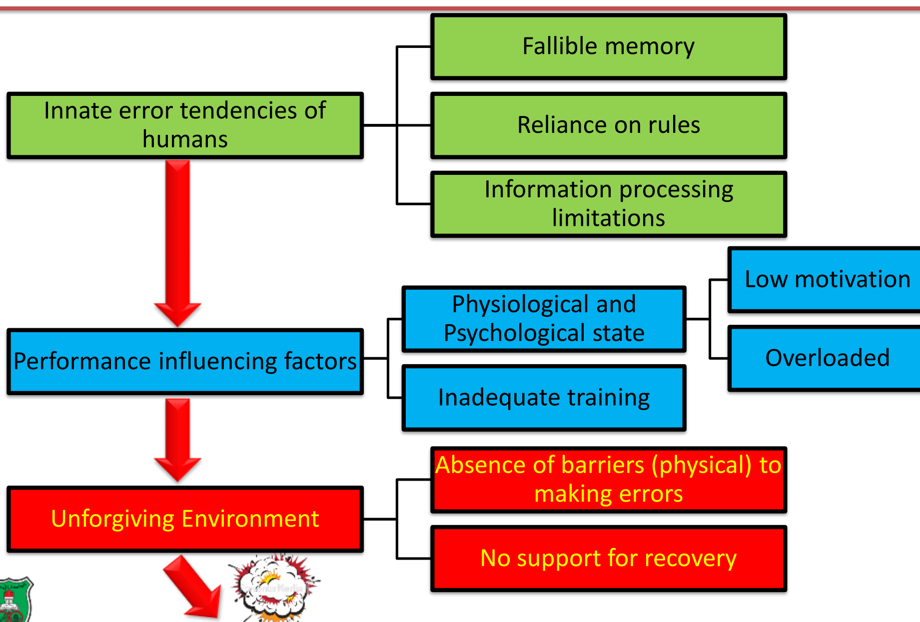
System-Induced Error

- An accident occurs if a **triggering event** occurs at a time when the **innate error tendencies of humans** as determined by **performance influencing factor** lead to an error in an **unforgiving environment.**

Developed during the 1980’s

originating in or arising from the intellect or the constitution of the mind, rather than learned through experience: an innate knowledge of good and evil

Triggering Events



Main Causes of Accidents

Ignorance

- Incompetent design, construction or inspection occurs.
- Supervision or maintenance occurs by personnel without the necessary understanding.
- Assumption of responsibility by management without an adequate understanding of risks.
- There is a lack of precedent.
- There is a lack of sufficient preliminary information.
- Failure to employ competent Loss Prevention professionals

Economic Considerations

- Initial engineering and construction costs for safety measures appear uneconomical.
- Operation and maintenance costs are unwittingly reduced to below what is necessary

Oversight and Negligence

- Otherwise competent professional engineers and designers commit errors.
- Contractual personnel or company supervisors knowingly assume high risks.
- Lack of proper coordination in the review of engineering designs.
- Failure to conduct prudent safety reviews or audits.
- Unethical behavior occurs

Unusual Occurrences

- Natural catastrophes - earthquakes, extreme weather, etc.
- Political upheaval - terrorist activities
- Labor unrest, vandalism

the real cause of most accidents is what might be classified as human errors.

How a Process Doesn't Work/Fails

- Murphy's Laws apply
  - If anything can go wrong, it will.
  - Left to themselves, things tend to go from bad to worse.
  - Nature always sides with the hidden flaw.
  - Fourth Corollary: If you perceive that there are four possible ways in which a procedure can go wrong, then a fifth way will promptly develop.
  - Eighth Corollary: **It is impossible to make anything foolproof because fools are so ingenious**.

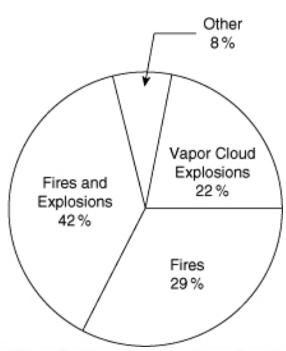
My formulation of the eighth corollary: Don't ever try to devise a fool-proof system. Because you will always find a fool who will be able to fool the fool-proof system devised.

A fundamental law of nature: Humans make mistakes. Don't forget it, don't blame it … but just plan for it!!!

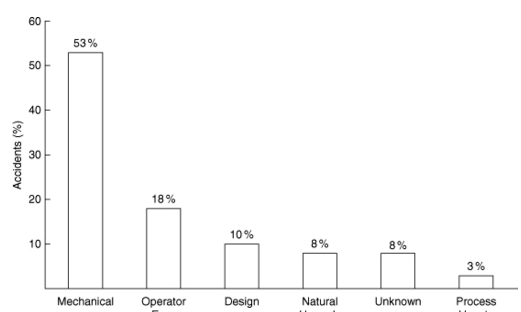
Frequency of Errors Committed by Humans

Operator/Stress/Time	Frequency of Error
Not trained, or under stress, or overloaded or short period of time	Error occurs about ½ to every time the operation is done
Trained, and not under stress, and not fatigued and not overloaded, and enough time	Error occurs about 1 in every 100 times the operation is done
Trained and not under stress and not fatigued and not overloaded and enough time AND with built in feedback	Error occurs about 1 in every 1,000 times the operation is done SOURCE: ROHM AND HAAS

Types and Causes of Loss

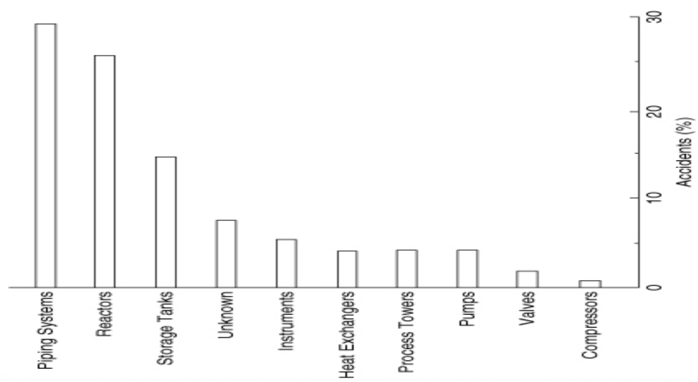


Types of loss for large hydrocarbon-chemical plant accidents. Data from The 100 Largest Losses, 1972–2001.



Causes of losses for largest hydrocarbon-chemical plant accidents. Data from The 100 Largest Losses, 1972–2001.

Hardware Related Loss



Hardware associated with the largest hydrocarbon- chemical plant accidents. Data from The 100 Largest Losses, 1972–2001.

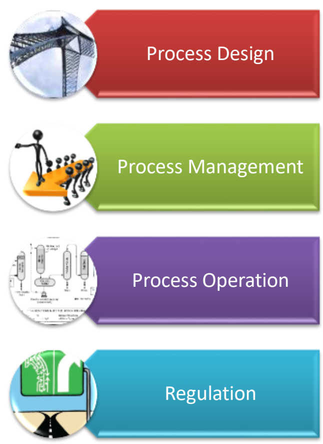
Most complicated mechanical components (pumps and compressors) are minimally responsible for large losses.

Loss Distribution with Time

Loss distribution for the largest hydrocarbon-chemical plant accidents over a 30-year period. Data from The 100 Largest Losses, 1972–2001.

The number and magnitude of the losses increase over each consecutive 10-year period for the past 30 years. This increase corresponds to the trend of building larger and more complex plants.

What Must We Do to Keep Accidents from Happening?



Stereotypes

- GREEN is on, RED is off…but not in Japan!
- H is hot water, C is cold…except in non-English countries (chaud or caliente both mean hot in French and Spanish)
- Light switch is up for on…except in the UK!

Human factors

1.Make the right way THE ONLY WAY

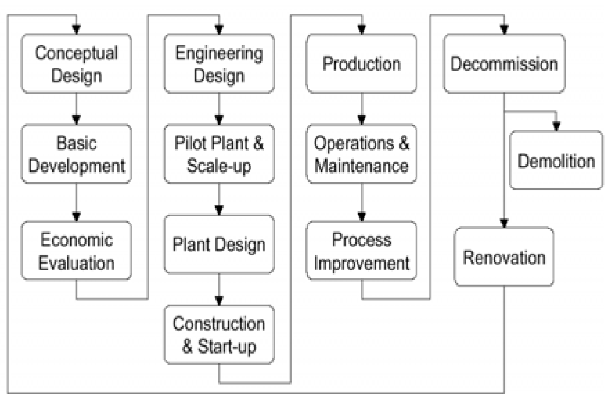
2. Make the right way THE EASIEST WAY

3. Give the operators feedback that it was done the wrong way

4. Provide safeguards for when it is done the wrong way

When

- Process safety must be inherent (integrated, built-in) into the entire life-cycle of a plant, from conceptual design to decommissioning.



Recent incidents have shown that any "fully engineered" and operational process plants can experience total destruction. Initial conceptual designs and operational philosophies have to address the possibilities of a major incident occurring and provide measures to prevent or mitigate such events.

Inherently Safer Design

ENGINEERING CONCEPT Four paths define inherently safer design.

Minimize or intensify
Use smaller quantities of hazardous chemicals. For instance, reduce inventories of in-process intermediates and raw materials or intensify production by increasing reaction efficiencies.

Substitute
Replace a hazardous chemical with a safer one, such as eliminating hazardous solvents in cleaning operations or in paints and coatings.

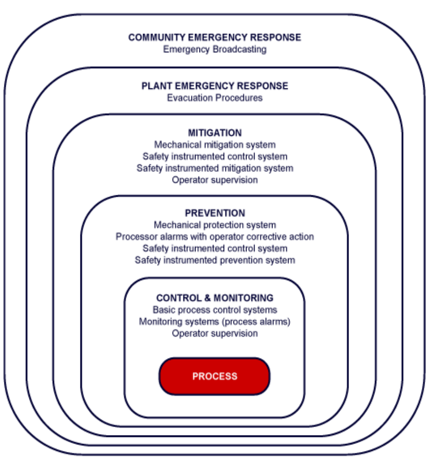
Moderate
Shift to less hazardous processes and chemicals, and modify facilities to minimize the impact of hazardous chemical releases by using, for instance, lower pressure and temperatures.

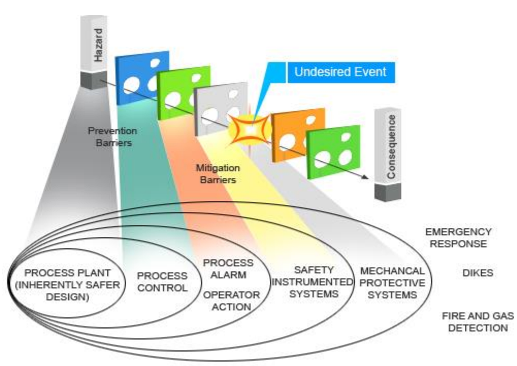
Simplify
Design facilities to eliminate unneces-sary complexity and make operating errors less likely and more forgiving. For instance, depend more on in situ creation and use for highly reactive toxic chemicals.

SOURCES: Kletz, Trevor: "Process Plants: A Handbook for Inherently Safer Design"; American Institute of Chemical Engineers: "Inherently Safer Chemical Processes"

An INHERENTLY SAFER DESIGN is one that avoids hazards instead of controlling them, particularly by removing or reducing the amount of hazardous material or the number of hazardous operations.

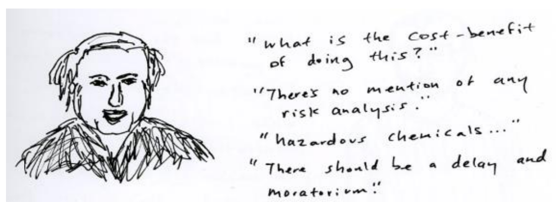
Layer of Protection Analysis (LOPA)

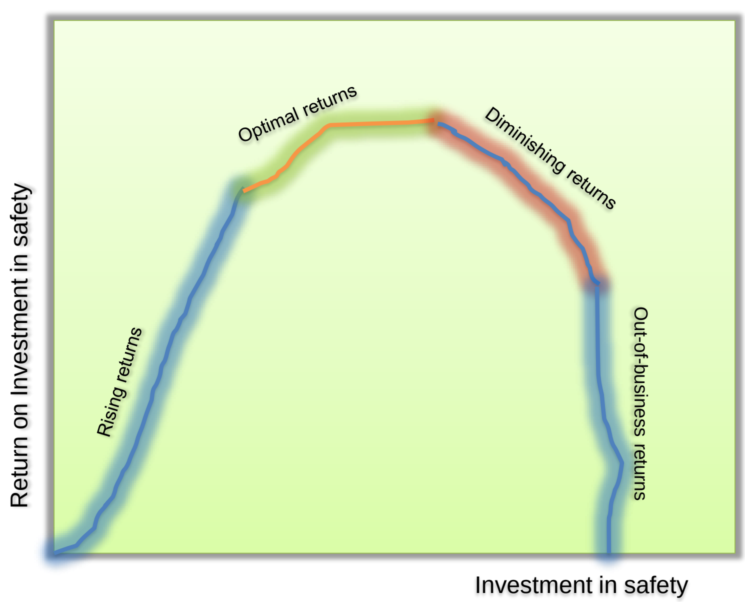




So … Is Safety a Good Business?

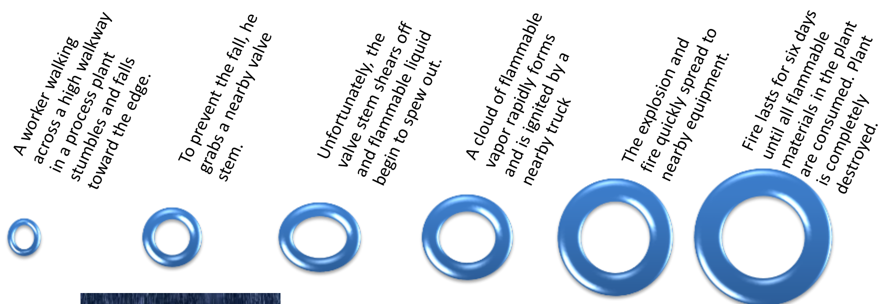
- Safety is good business and, like most business situations, has an optimal level of activity beyond which there are diminishing returns.
  - If initial expenditures are made on safety, plants are prevented from blowing up and experienced workers are spared. This results in increased return because of reduced loss expenditures.
  - If safety expenditures increase, then the return increases more, but it may not be as much as before and not as much as achieved by spending money elsewhere.
  - If safety expenditures increase further, the price of the product increases and sales diminish. Indeed, people are spared from injury (good humanity), but the cost is decreased sales.
  - Finally, even higher safety expenditures result in uncompetitive product pricing: The company will go out of business. Each company needs to determine an appropriate level for safety expenditures. This is part of risk management.
- From a technical viewpoint, excessive expenditures for safety equipment to solve single safety problems may make the system unduly complex and consequently may cause new safety problems because of this complexity. This excessive expense could have a higher safety return if assigned to a different safety problem. Engineers need to also consider other alternatives when designing safety improvements.





When it Rains it Pours

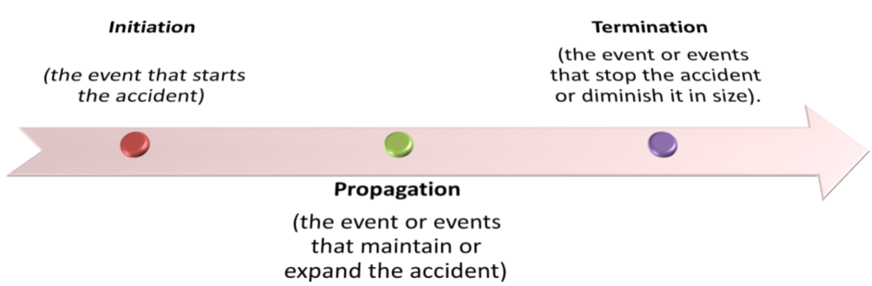
- This disaster occurred in 1969 and led to an economic loss of $4,161,000. It demonstrates an important point: Even the simplest accident can result in a major catastrophe.



المصائب لا تأتي فرادى بل زرافات ووحدانا

One Hundred Largest Losses: A Thirty-Year Review of Property Losses in the Hydrocarbon-Chemical Industries (Chicago: M & M Protection Consultants, 1986), p. 3.

Accident Sequence



Safety engineering involves eliminating the initiating step and replacing the propagation steps with termination events

Defeating the Accident Process

Step	Desired effect	Procedure
Initiation	Diminish	Grounding and bonding Inerting Explosion proof electrical Guardrails and guards Maintenance procedures Hot work permits Human factors design Process design Awareness of dangerous properties of chemicals
Propagation	Diminish	Emergency material transfer Reduce inventories of flammable materials Equipment spacing and layout Nonflammable construction materials Installation of check and emergency shutoff valves
Termination	Increase	Fire-fighting equipment and procedures Relief systems Sprinkler systems Installation of check and emergency shutoff valves

Example

The following accident report has been filed

Failure of a threaded 1½″ drain connection on a rich oil line at the base of an absorber tower in a large (1.35 MCF/D) gas producing plant allowed the release of rich oil and gas at 850 psi and –40°F. The resulting vapor cloud probably ignited from the ignition system of engine driven compressors. The 75′ high × 10′ diameter absorber tower eventually collapsed across the pipe rack and on two exchanger trains. Breaking pipelines added more fuel to the fire. Severe flame impingement on an 11,000-horsepower gas turbine–driven compressor, waste heat recovery, and super-heater train resulted in its near total destruction.

Identify the initiation, propagation, and termination steps for this accident.

Solution

Initiation : Failure of threaded 1½″ drain connection
Propagation: Release of rich oil and gas, formation of vapor cloud, ignition of vapor cloud by compressors, collapse of absorber tower across pipe rack
Termination: Consumption of combustible materials in process

شكرا لحسن ألاستماع

27