Root Causes of Accidents

By.
Madeline Martinez

Howard University
College of Electrical Engineering
Spring - 2012

Root Causes of Accidents

The root causes of accidents can be divided in:

1. Deficiencies in the safety culture of the industry or organization

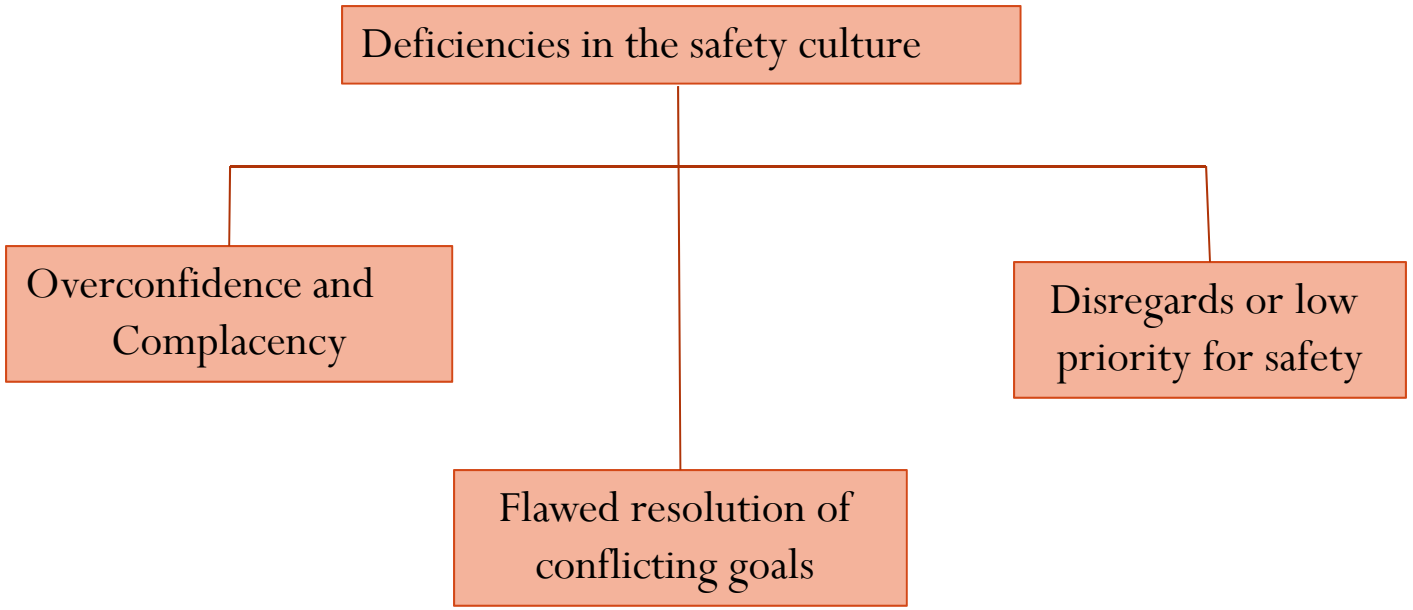
2. Flawed Organizational Structures

3. Superficial or ineffective technical activities

1. Flaws in the Safety Culture

Safety Culture:

General attitude and approach for safety reflected by those who participate in that industry .



A. Overconfidence and Complacency

Kemeny commission identified a mayor contributor to the Three Mile Island (TMI) accident:

Failure by the Nuclear Regulatory commission (NRC) to believe that a serious accident could happen.

Problem: Mindset about the infallibility of the equipment.

Lesson Learned from TMI accident:

The mindset regarding serious accidents is "probably the most important human factor with which this industry and the NRC has to contend".

Overconfidence and Complacency

Sometimes, lessons learned from accidents do not cross national borders

After TMI accident, top Soviet government and scientific leader expressed that Nuclear Power was a "Solved Problem" and that they would not have a similar accident (TMI accident).

Eight months after:

The Chernobyl disaster occurred:

Effects:

Four hundred times more radioactive material was released than had been by the atomic Bombing of Hiroshima.

Overconfidence and Complacency

Chernobyl Disaster :

- A year before it occurred, Soviet authorities at this plant described the risk of a serous accident as "Slight".
- A month before it occurred, the British Secretary of State for Energy repeated "Nuclear energy is the safest form of energy yet known to man"

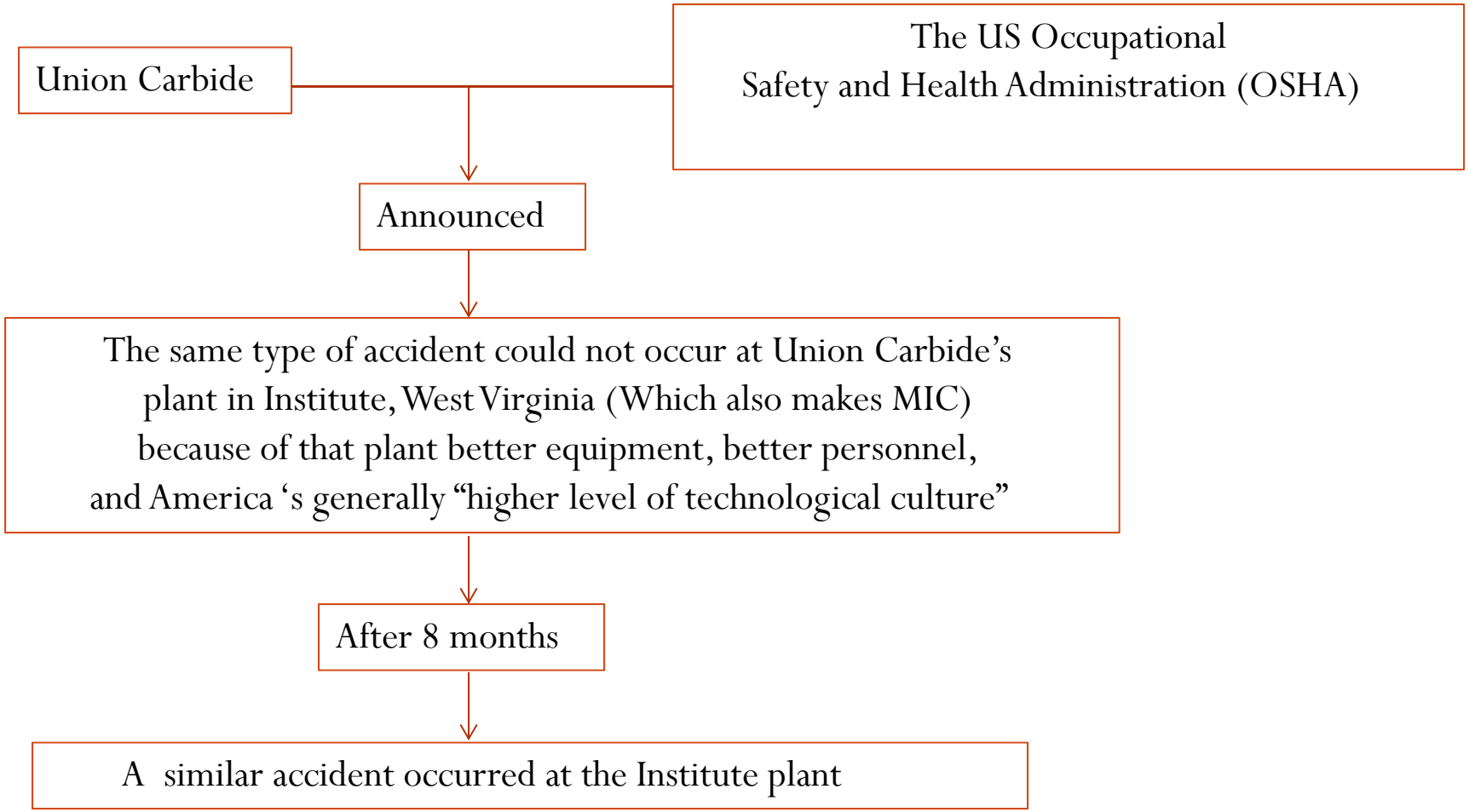
Bhopal Disaster:

- The Union Carbide Bhopal plant manager, when informed of the accident said:

"The gas leak just can't be from my plant. The plant is shut down. Our technology just can't go wrong, we just can't have leaks"

Overconfidence and Complacency

After Bhopal Disaster



Discounting Risks

Most accidents in well design systems involve two or more low-probability events occurring in the worst possible combination. The events are assumed to be independent, when in fact, they are dependent.

Phenomenon called: The Titanic Coincidence

When Titanic was launched in 1912, it was the largest and safest ship the world had never known. Up to four compartments could be ruptured without the ship sinking, never seen in history.

One of the ship officers assured a female passenger that "Not even God himself could sink this vessel"

While the owners were trying to break the current speed record, the Titanic ran into an iceberg that cut a 300-foot gash in one side of the ship, flooding 5 adjacent compartments.

Discounting Risks

Coincidences that contributed to the Titanic accident:

1. The captain was going far too fast for existing conditions.
2. A proper watch was not kept.
3. The ship was not carrying enough lifeboats.
4. Lifeboats drills were not held
5. The radio operator on a nearby trip was asleep and so did not hear the distress call.

The Titanic Effect says that the magnitude of disasters decreases to the extent that people believe that disasters are possible and plant to prevent them

Overrelying on Redundancy

- Challenger Disaster: There was a substantial safety margin in the O-rings. Even if the primary O-ring did not seal, it was assumed that the secondary one would. During the accident, the failure of the primary O-ring caused conditions that led to the failure of the secondary O-ring.

- Bhopal Disaster: A number of independent safety devices "failed" at the same time.

Warning: Poorly design safety device is worse than safety device at all, since its presence creates a sense of security

Ignoring High – Consequence, Low Probability Events

A common discovery in that the events were recognized before the accident, but was dismissed as incredible.

Therac-25 accidents

The Therac-25 was a radiation machine. It involved at least 6 accidents between 1985 and 1987, in which patients were given massive overdoses of radiation, approximately 100 times the intended dose.

A Therac-25 operator, who was involved in two of the overdoses, testified that she had been told the system had so many devices that an accident was impossible on this machine (10,000,000%)

Underestimating Software-Related Risks

- A believe that software cannot "fail" and that all errors will be removed by testing

Therac-25 Accident

Software was not even included in the original hazard analysis of the machine. When accidents started, software was not investigated. Overdoses were blamed on transient hardware failures. Additional hardware was added creating more complacency about the safety of the machine.

Safety devices are currently being replaced by software in commercial aircrafts, nuclear power plants, weapon systems, etc

B. Low Priority Assigned to safety

The entire organization must have a high level of commitment to safety in order to prevent accidents. The informal rules (Social processes) as well as the formal rules must support the overall safety policy.

Many managers recognize that safety is good business over the long term; others, put short term goals ahead of safety.

Bhopal Accident

Staff, training , and maintenance had been severely reduced prior to the accident. Top management justified these measures as merely reducing avoidable and wasteful expenditures without affecting overall safety.

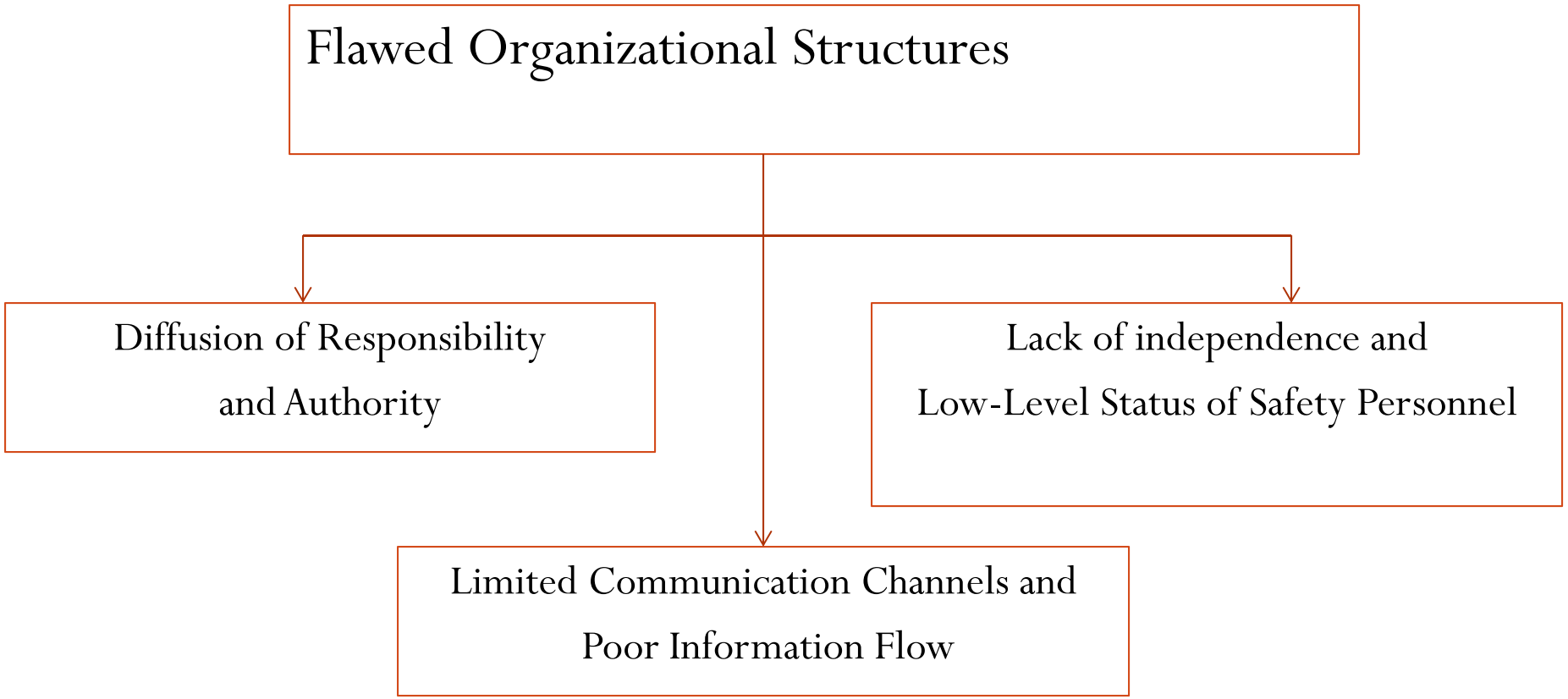
C. Flawed Resolution of Conflicting Goals

Safety not only needs to be recognized as a high priority goal, but procedures for resolving goal conflicts need to be established.

Challenger Accident

It is a classic case of poorly handled conflicts between safety and schedule.

2. Ineffective Organizational Structure



Diffusion of Responsibility and Authority

- Problems arise when responsibility is divided across organizational boundaries: *There should be at least one person in the organization with overall responsibility for safety.*

- A large organizational distance between decision maker and those with technical awareness is, of course, a common problem in engineering organizations

Poor decision making can have disastrous results when safety is involve

Lack of independence and Low-Level Status of Safety Personnel

The safety organization must be independence from the project or program management for which it provides oversight or input.

Challenger Disaster:

- Safety, reliability, and quality assurance offices where under the supervision of the organizations and activities whose efforts they were to check.
- Lack of involvement in critical discussions and decision making.

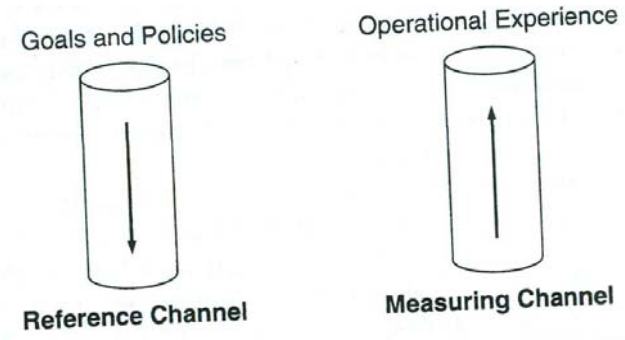
Limited Communication Channels and Poor Information Flow

Communication paths and information need to be explicitly defined.

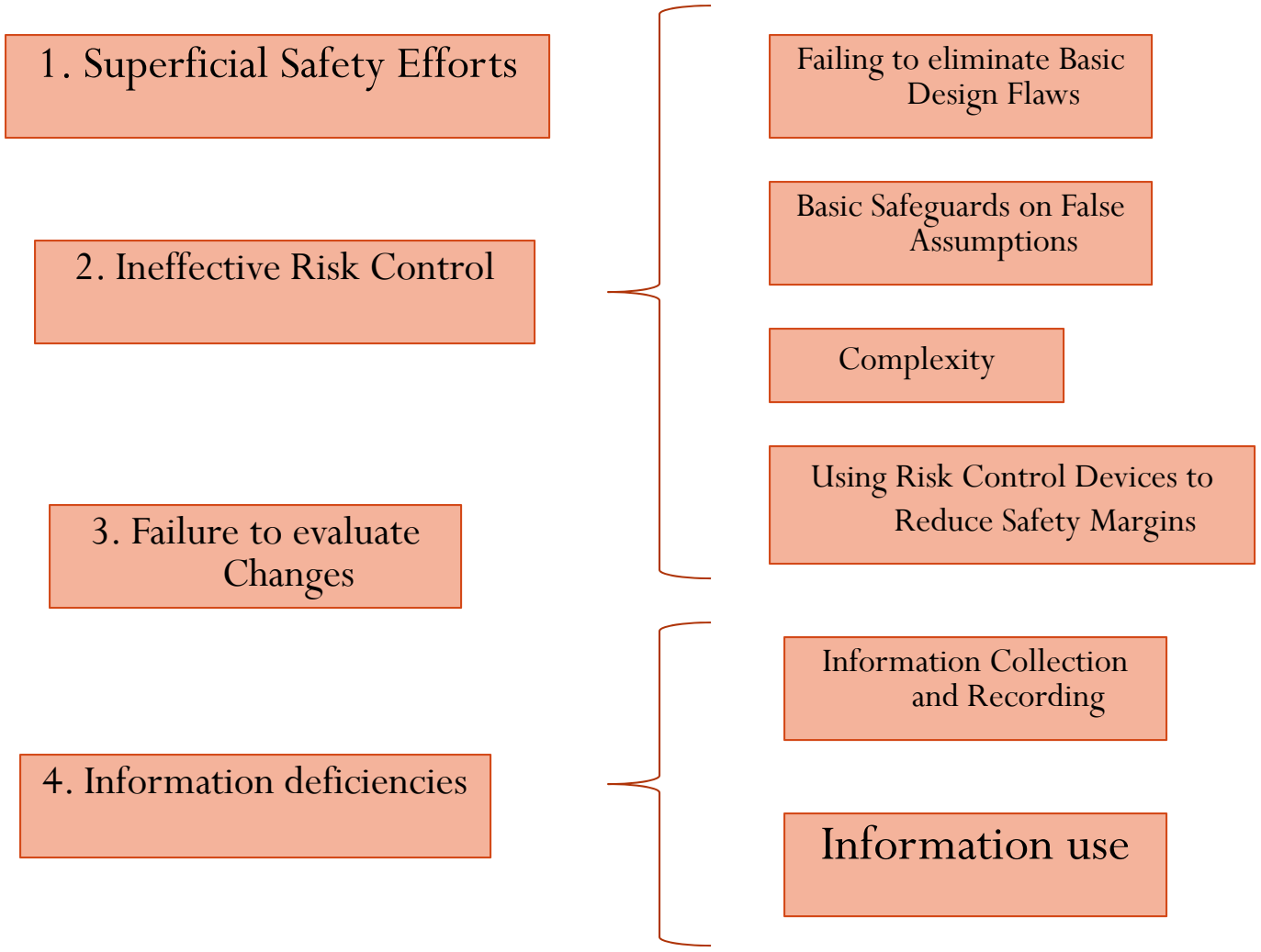
Types of Information flow:

1. Reference Channel: Communicates goals and policies downward. Decisions, Procedures and Choices need to be communicated in order to avoid undesirable modification by lower levels.

2. Measuring Channel: Communicates the actual state of affairs upward.



Ineffective Technical Activities



Ineffective Technical Activities

- **Superficial Safety Efforts**: It occurs when the system safety engineers become so involved in the project development effort that they lose their objectivity.
- **Ineffective Risk Control**: In some accidents, the hazards are identified and efforts are made to control them, but that control is inadequate.
- **Failure to evaluate Changes**: Accidents often involve a failure to reevaluate safety after changes are made.
- **Information deficiencies**: Feedback of operational experience is one of the most important sources of information in designing, maintaining, and improving safety.

THANKS !!