Controlling Risks
System Safety Process

System Safety History

- System safety (SS) movement began in 1940s
  - Amos L. Wood, 14th Annual Meeting of the Institute of Aeronautical Sciences in January 1946
- USAF an early leader
- Air Force-Industry partnership began as early as 1954
- Early 60s, small group of managers, scientists, & engineers implemented SS in aerospace program
- In 1962, the System Safety Society was organized; professional organization in 1972

What is System Safety?

- System safety is the practice of proactive hazard management. It is based on the principle that, armed with sufficient knowledge, one can predict hazards associated with a process and can identify effective methods to lessen the risks associated with the hazards. System safety applies to the entire lifecycle of the process or thing that generates the hazard – from concept to decommissioning.

USAF System Safety Definition

Air Force System Safety Handbook:

"The application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system lifecycle."

FAA System Safety Definition

FAA System Safety Handbook:

"The application of special technical and managerial skills to the systematic, *forward-looking* identification and control of hazards throughout the life cycle of a project, program, or activity."

System Safety Principles

- Safety must be designed in.
- Inherent safety requires both engineering and management techniques to control the hazards.
- Safety requirements must be consistent with other program or design requirements.

System Safety Goal

The goal of System Safety is to optimize safety by the identification of safety-related risks, eliminating or controlling them via design and/or procedures.

Question- Where do you find the DOE system safety program defined?

Federal Law

- Code of Federal Regulation
  - 10 CFR 20, Standards For Protection Against Radiation
  - 10 CFR 820, Procedural Rules for DOE Nuclear Activities
  - 10 CFR 830, Nuclear Safety Management
  - 10 CFR 835, Occupational Radiation Protection

DOE Orders and Guidance

- Department of Energy Orders
  - DOE o 414.1d, Quality Assurance
  - DOE o 420.2c, Safety of Accelerator Facilities
- Department of Energy Guides
  - DOE G 420.2-1, Accelerator Facility Safety Implementation Guide for DOE o 420.2B, Safety of Accelerator Facilities
  - DOE G 441.1-1C, Radiation Protection Programs Guide for use with Title 10 Code of Federal Regulations, Part 835, Occupational Radiation Protection

Industry

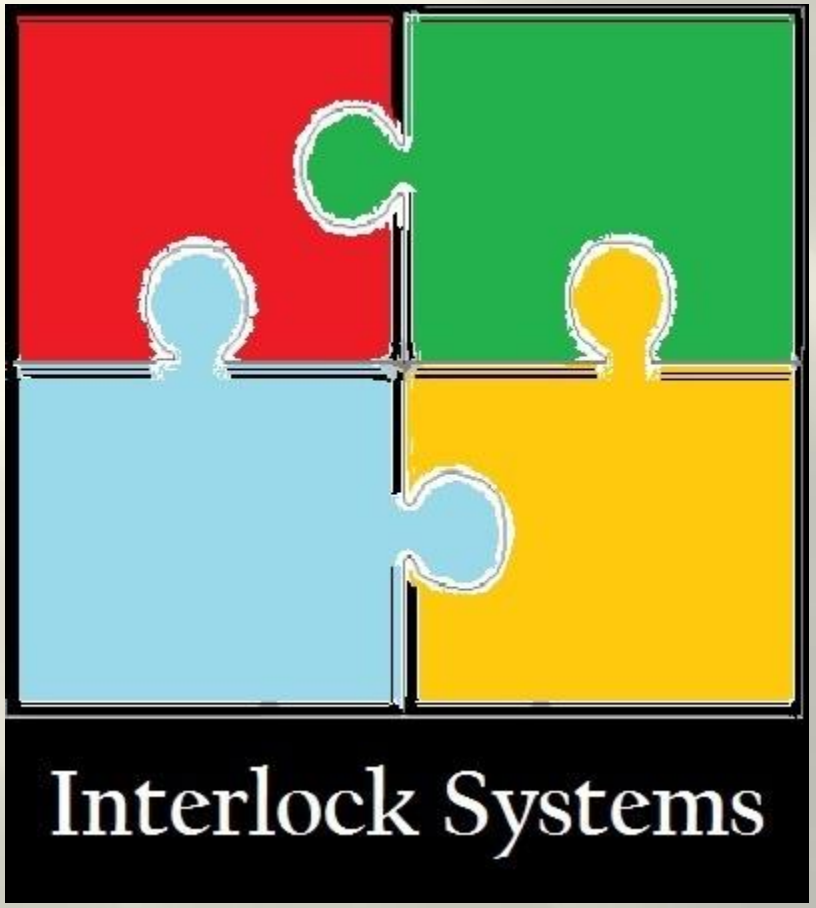
- Industrial Standards
  - ANSI/HPS N43.2-2001, Radiation Safety for X-ray Diffraction and Fluorescence Analysis Equipment
  - ANSI/HPS N43.3-2008, Installations Using Non-Medical X-ray and Sealed Gamma-Ray Sources, Energies Up To 10 MeV
  - NFPA 101, Life Safety Code, Chapter 7

Are your programs…

Simplemented?

- Partially implemented simple program
- Do not contain sufficient DOE policies
- Contain prescriptive elements
  - Sanctioned or authorized by long-standing custom or usage
  - Passed down by Indian sweat lodge ritual

Robust Programs

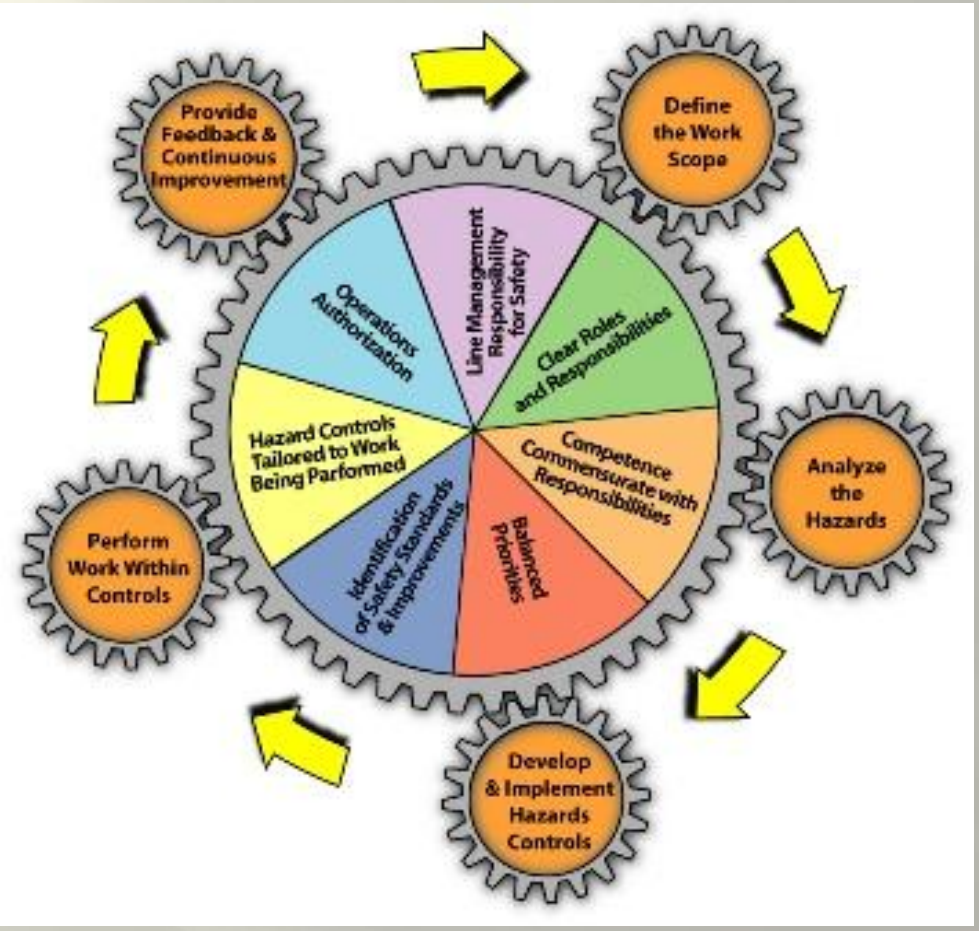


- Review every two or three years
- Compare with CFR, DOE and Industry
- Analyze existing systems for gaps

DOE Safety Management System Policy 450.4

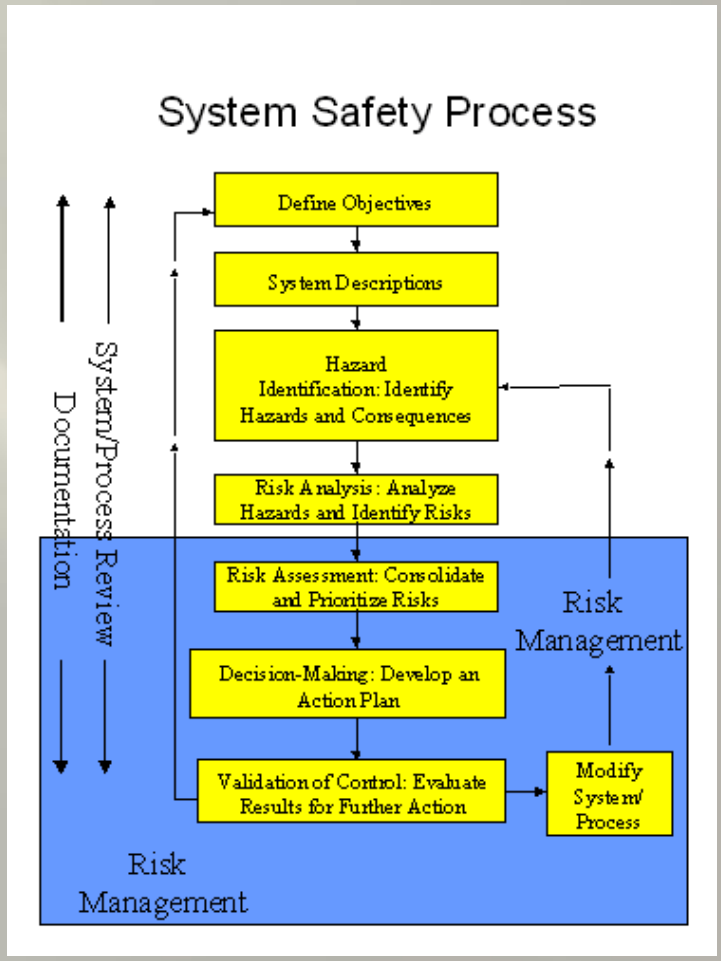
- The Department and Contractors must systematically integrate safety into management and work practices at all levels so that missions are accomplished while protecting the public, the workers, and the environment.”

DOE ISM Process



8 Step Process

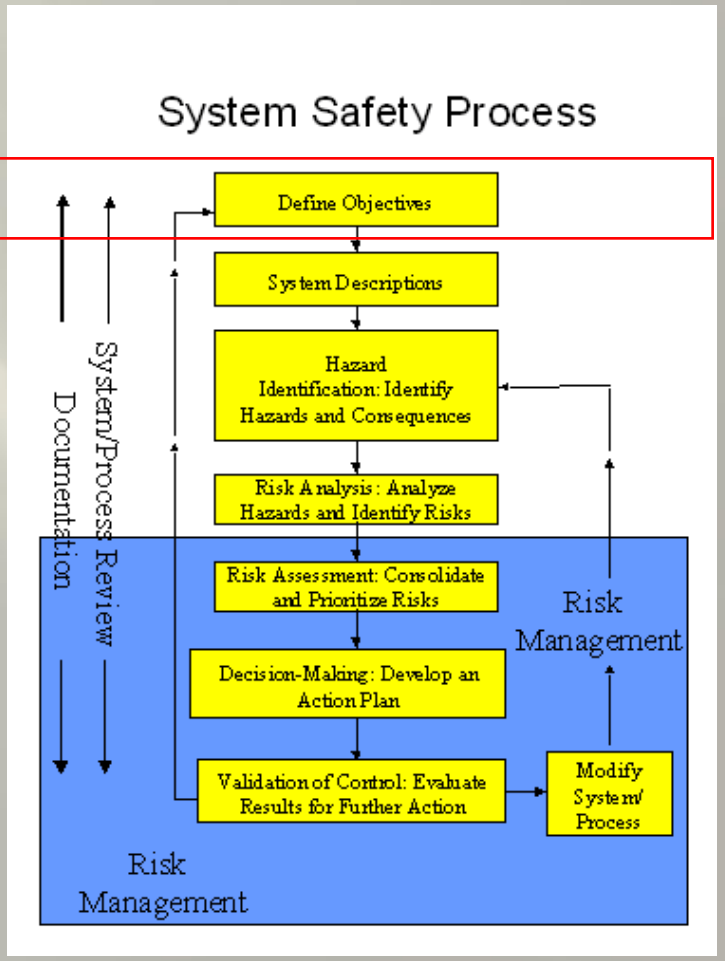
- Define Objectives
- System Description
- Hazard Identification
- Risk Analysis
- Risk Assessment
- Decision Making
- Validation & Control
- Modify System/Process



Step 1: Define Objectives

- Typically documented in
  - Business Plan
  - Operating Specifications

- In what DOE document(s) might you find this type of information?

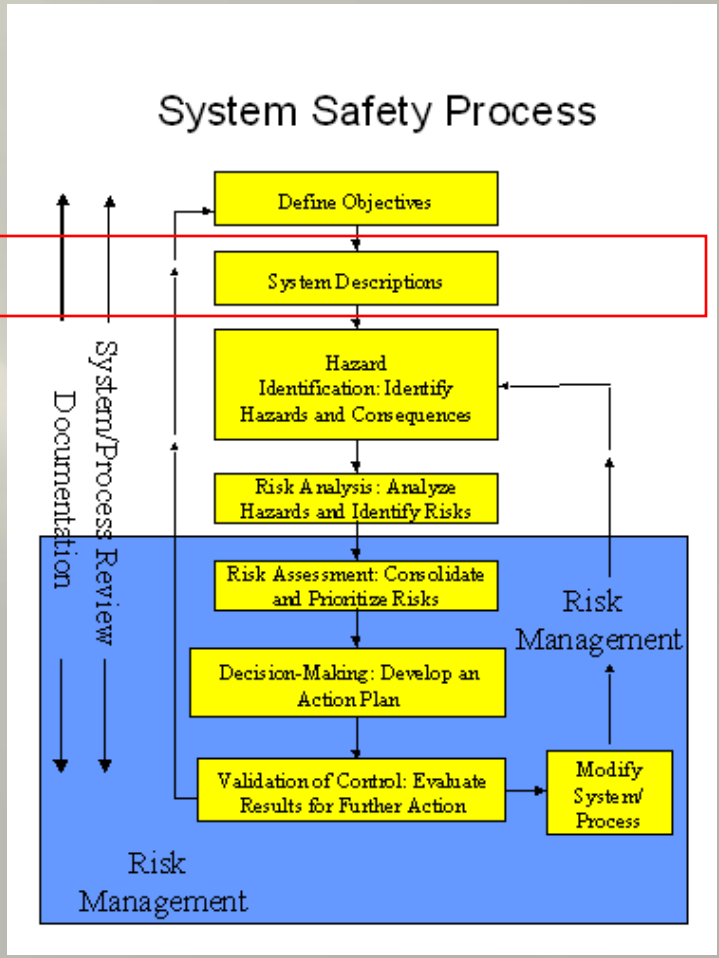


FAA System Safety Handbook

“There are no "safety problems" in system planning or design. There are only engineering and/or management problems that, if left unresolved, may lead to accidents.”

Step 2: System Description

- Provides a description of the interactions among:
  - People
  - Procedures
  - Tools
  - Materials
  - Equipment
  - Facilities
  - Software
  - Environment

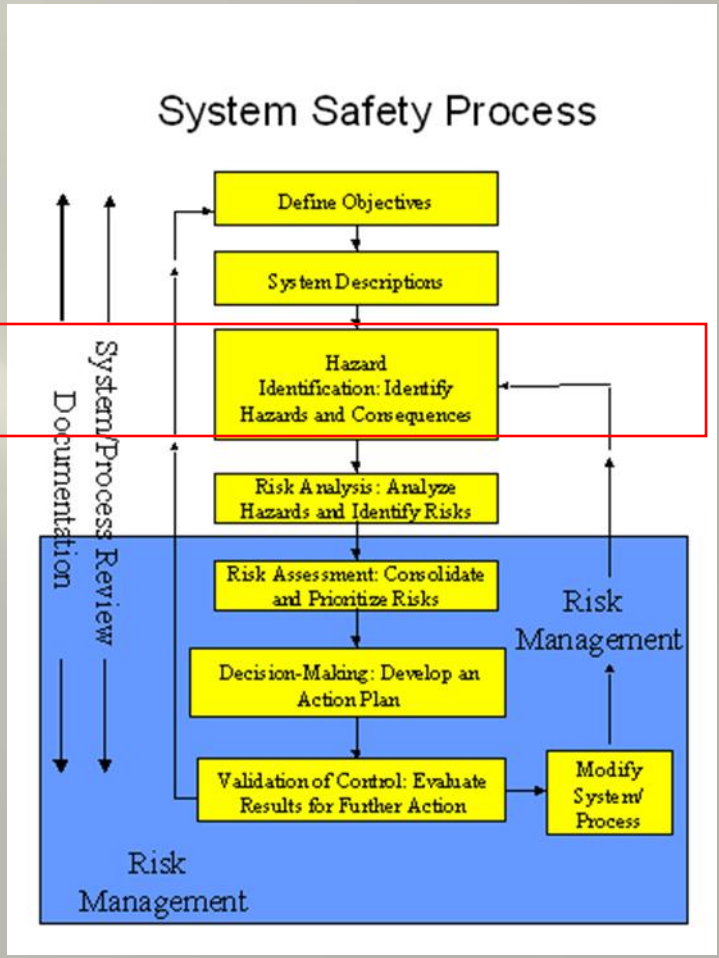


System Description (continued)

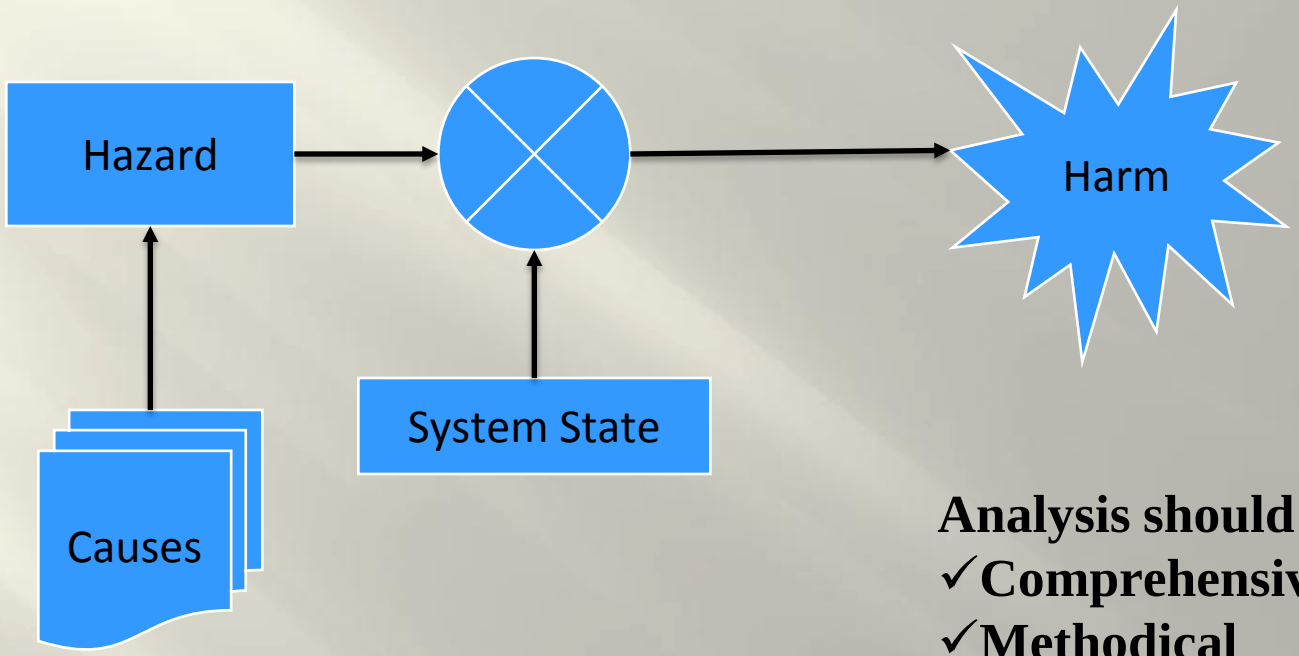
- **The object of a good system definition is to:**
  - ✓**set limits for the following steps in the process**
  - ✓**reduce complex systems into manageable parts.**

Step 3: Hazard Identification

- Sources are both internal and external
- Preliminary Hazard List
- Group hazards by function
- Develop hazard scenarios
- Develop worst case scenarios



Hazard Analysis

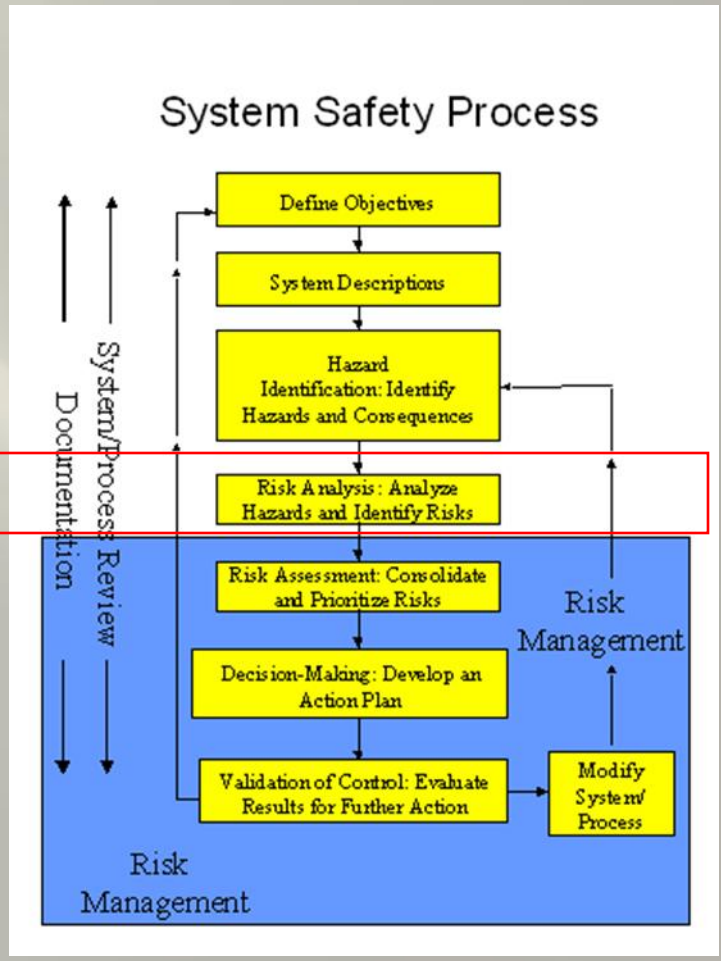


Contributory Hazards

Analysis should be:
- ✓**Comprehensive**
- ✓**Methodical**
- ✓**Disciplined**

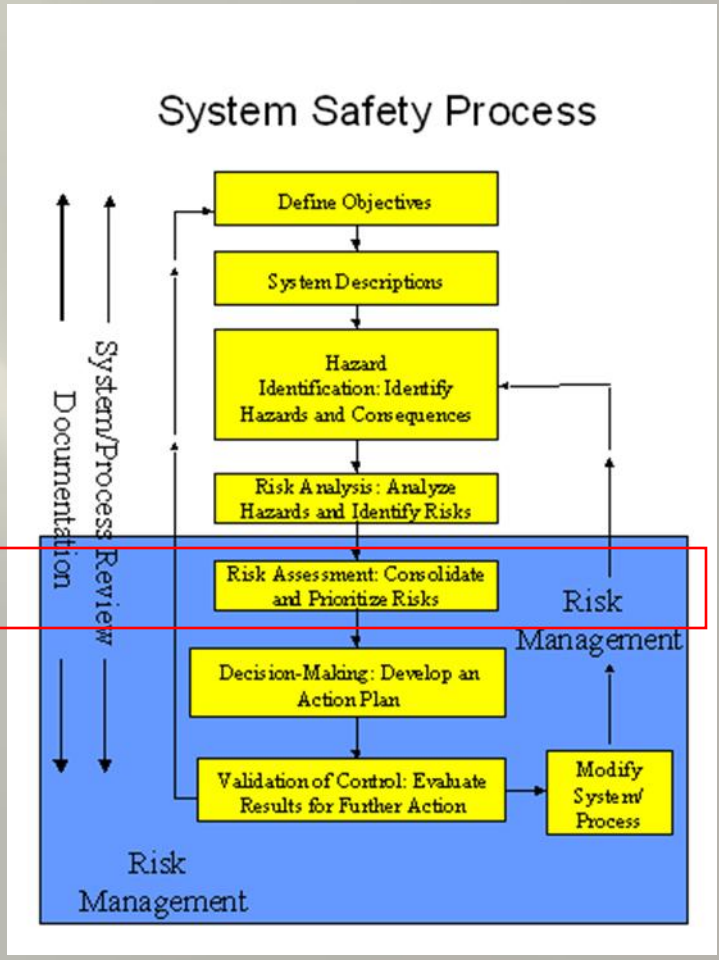
Step 4: Risk Analysis

- Characterize hazards
  - Likelihood
  - Severity
  - Exposure
- Qualitative analysis
  - Matrix
  - PHA
  - What If/Checklist
  - Lessons Learned reports
- Quantitative analysis
  - FEMA



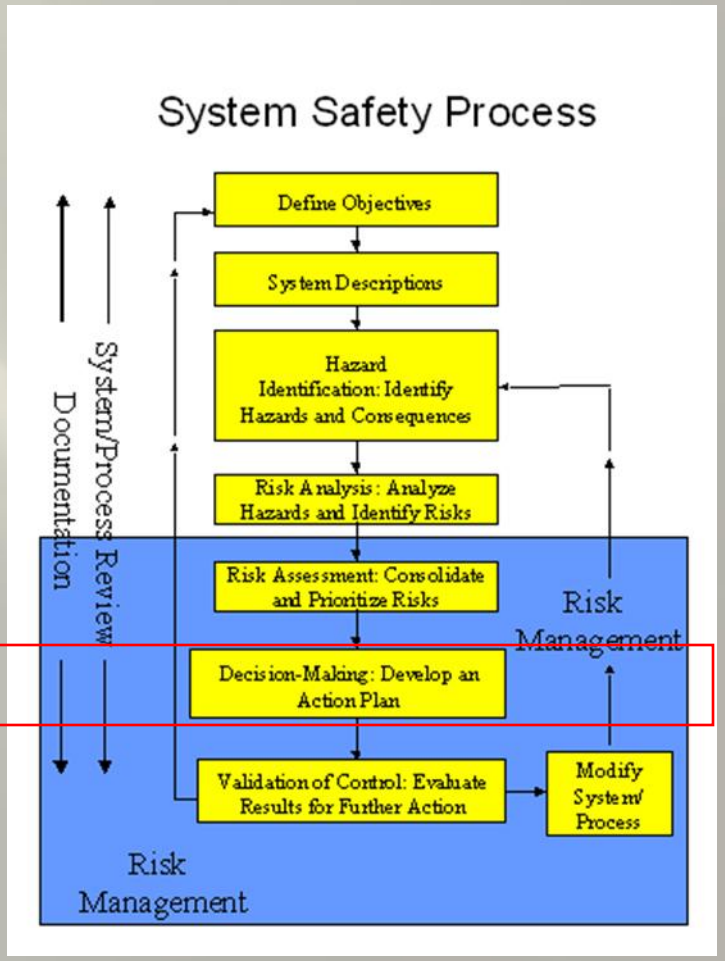
Step 5: Risk Assessment

- Combine impacts of risk elements
- Compare impacts against acceptability criteria
- May consolidate risks into sets for joint mitigation and decision making



Step 6: Decision Making

- Begins with
  - Management decision
  - Resources allocation
  - prioritized task list
- Most crucial step in process
  - Decide how to address each risk
    - Safety Order of Precedence



Safety Order of Precedence

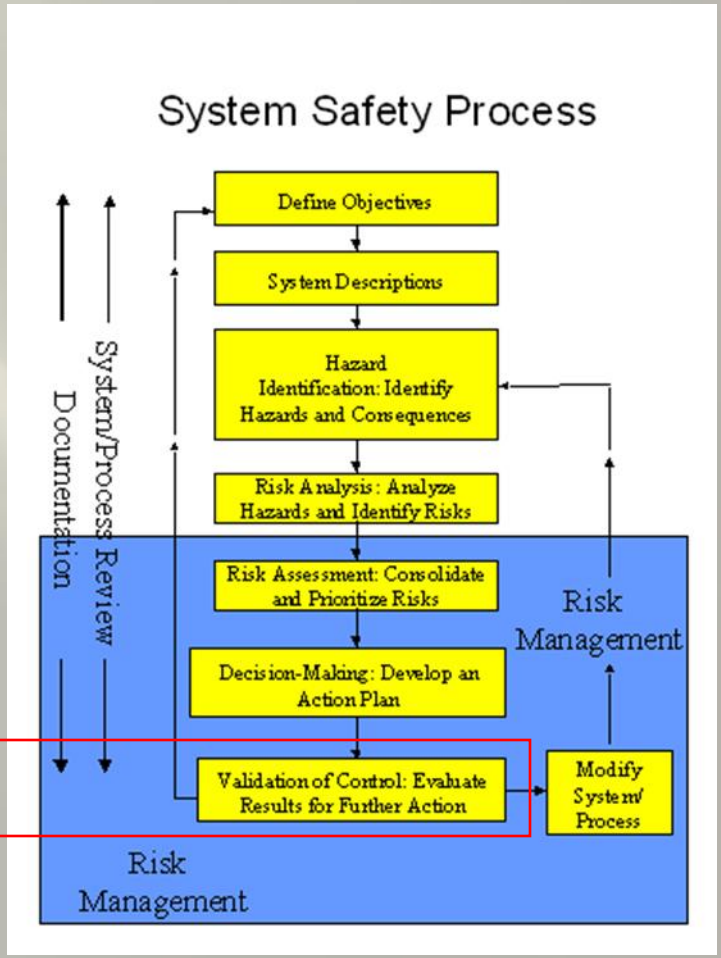
- Design engineering approach:
  - Design for minimum risk
  - Design to reduce hazards
  - Incorporate safety devices
  - Provide warning devices
  - Develop procedures and training
- Alternative action plans
- Final result -written assessment document

Effective Safety Risk Management Decisions

- Assign qualified, competent personnel
- Authority commensurate w/ responsibility
- Define, document, & track all known hazards as program policy
- Include safety risk assessment in program reviews
  - Risk acceptability
  - Risk responsibility
  - Decision milestones

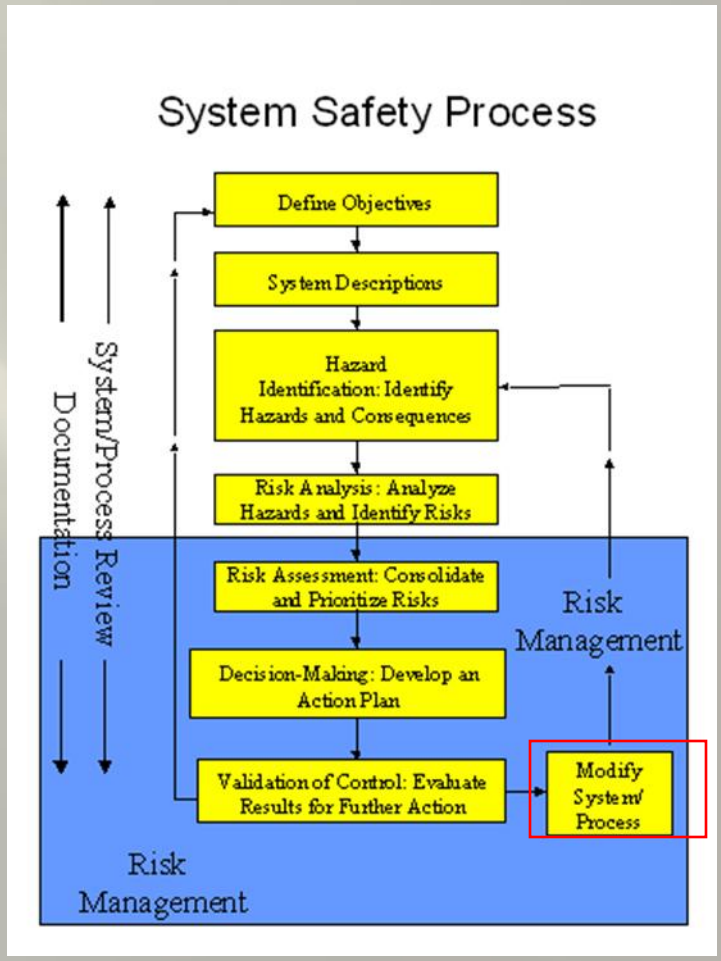
Step 7: Validation & Control

- Analyze effectiveness
  - ID data collection needs
  - ID triggering events
  - Develop plan for data review
- Document each risk status
  - Acceptable
  - Unacceptable
  - Unknown

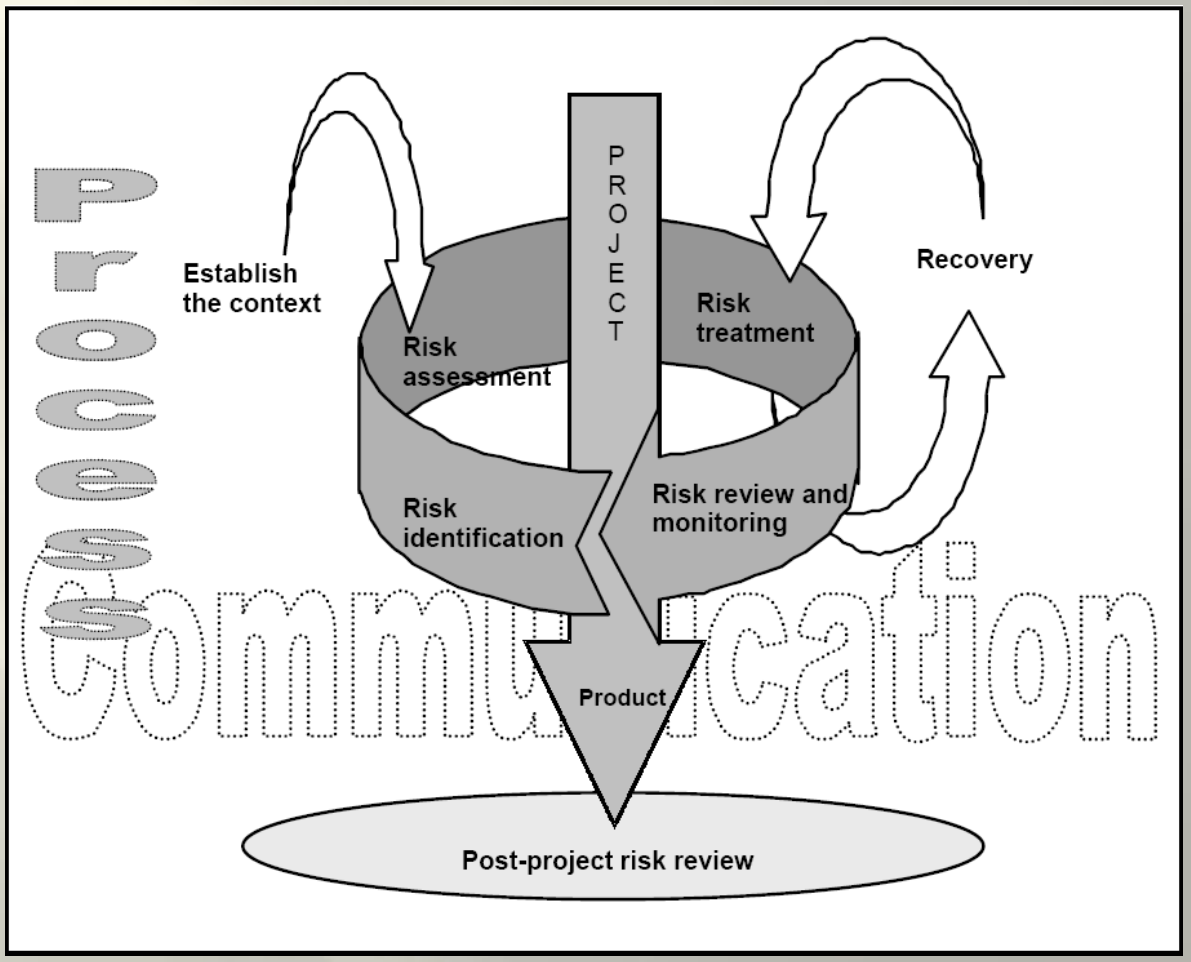


Step 8: Modify System/Process

- Modify if needed
- Why?
  - Risk status changes
  - Mitigation results are unacceptable
  - Addressed wrong hazard
  - System/process undergoes change
- Re-enter process at the hazard ID step



Risk Management standard IEC 62198



Summary

- System Safety is a process that guides you into developing a context for your safety system design.
- The System Safety process requires you to document this context.
- Once your context has been established, you can then develop your safety system within that context.