OSH 452

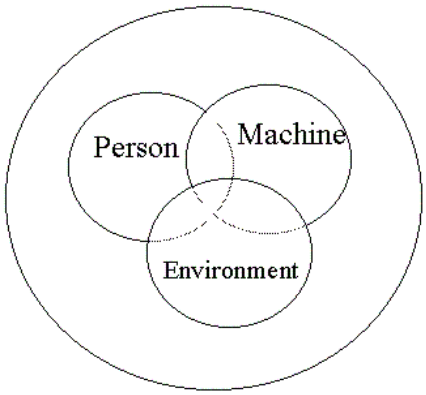
Topic: **Introduction to System Safety/Product Safety**

1. Introduction

   Definition of System Safety:
   Process of applying management and technical principles to achieve the optimum degree of safety throughout the life cycle of a system, consistent with operational requirements, time and cost.

2. Overview of System Safety:
   A. System Concept
      System—Group of interrelated elements working together to produce a desired output.

System Factors



   B. Objectives of System Safety:

C. Overall approach of System Safety:

D. Relationship to traditional approaches.

3. Historical:

4. Factors which have driven System Safety other than Aerospace, Weapons & Nuclear.

OSH 452

Topic: **System Life Cycle**

1. Introduction:

2. Life Cycle Definitions:

Concept Definition	Defining and evaluating
Development & Test	Full-scale research & development
Production	Manufacturing
Operation	Operation & maintenance
Disposal	Termination

A. **Concept Definition Phase**

a) Defining & evaluating a potential system concept.

b) Identify the potential hazards in the design .

Areas Examined:

- Critical issues related to the product
- System safety concerns regarding the types of hazards are identified and their impacts evaluated
- Preliminary Hazard Analysis performed along with risk analysis
- Similar systems evaluated

B. **Development & Test Phase**

1) Involves designing, developing & testing the system.

2) Clear definitions of subsystems, assemblies and subassemblies are made.

3) Areas to be looked at: technological risk, costs, human engineering, operational and maintenance suitability, and safety.

4) Perform FHA and FTA for specific known hazards.

5) Lab and prototype testing results are used.

6) More complete testing is performed to verify acceptability of the design. Any failures analyzed for their safety impact.

7) OHA (Operating Hazard Analysis) and FMEA (Failure Modes and Effects Analysis) is done.

8) Preliminary Publications/Training Requirements.

9) Completion of this phase leads to a go/no-go decision prior to production.

10) If any issue is missed the cost of the product will be higher.

C. **Production Phase**.

1) Quality control serves as a major focal point for inspection and testing of the product.

2) Training begins during this phase - both internal and customer.

3) Updating of previous analyses will be done as information is collected.

4) Paper work is brought up-to-date and compiled

D. **Operation Phase**.

1) System is now operational.

2) Feedback from field.

3) Accidents/incidents are investigated.

4) As design changes are proposed they are reviewed.

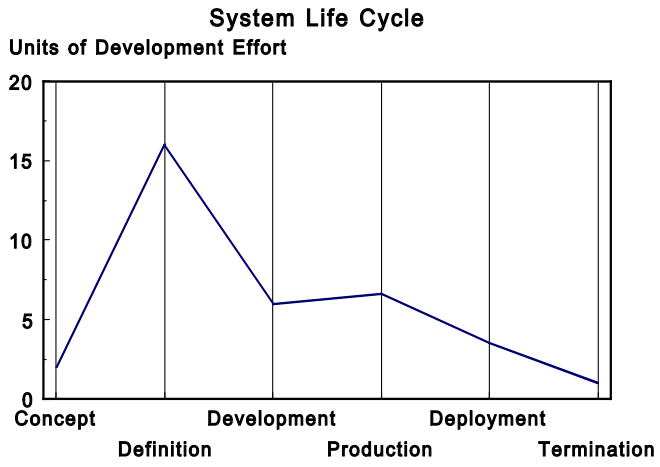
5) Mission changes.

6) Lessons learned documentation.

F. **Disposition or Termination Phase**

Termination either intentionally or accidentally

3. Amount of System Safety Work
   Text page 42.



Topic: **System Safety Implementation/Tasks**

1. System Safety Tasks:

   A. Categories of Tasks.

      1) Input to SS program planning.

      2) Evaluation of System.

3) Control of Hazards
   a) Order of precedence.- Page 43

   b) Evaluation of hazard controls.

   c) Develop recommendations for risk acceptance decisions.

4) Documentation and Related Activities.

B. Types of Data.

1) System specifications, drawings and mockups.

2) Previous incident data, lessons learned.

3) Test data.

a) Lab tests

b) Usage (Field) tests.

4) Operator and maintenance procedures.

5) Usage profiles.

6) Personnel selection criteria.

C. Differences for systems not following ‘typical’ cycle.

1) Non-developmental Items (off-the-shelf)

2) Facilities.

Topic: **System Safety Program Plan (SSPP)**

1. System Safety Program Plan (SSPP)

It outlines responsibilities, methods of accomplishment, milestones, depth of effort, integration with other engineering and management activities.

The most important element in implementing a system safety program.

2. Parts of SSPP

a) Hazard Analyses.

b) Risk Assessment - A decision making process consisting of evaluation and control of the probability of occurrence and the consequences of a hazardous event.

c) Data

d) Testing and demonstration.

e) Training

---

3. Placement of System Safety Personnel

a) Principles - System Safety Personnel:

Must be free to inquire into all areas of design, operation and maintenance.

Must have direct access to information and appropriate people without filtering.—Including: Access to decision-making management.

b) Placement of function.

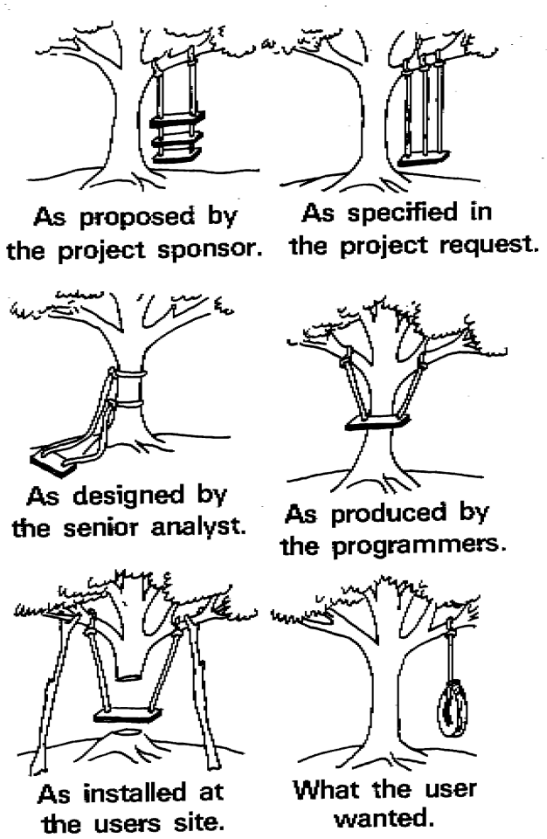
---

4. Project Development

- Projects frequently turn out different than how they are initially envisioned.

- There are many people involved in a project and it is the job of the project manager to clearly understand what is desired and to ensure everyone on the project team has the same understanding.

The illustration demonstrates what frequently happens in project development.



Topic: **Risk Assessment**

Introduction to Hazard Analysis

A. Risk: An expression of the possibility of a mishap in terms of hazard severity and hazard probability.

B. Risk assessment A decision making process consisting of evaluation and control of the probability of occurrence and the consequences of a hazardous event.

C. Risk Assessment.

2) Information needed to evaluate:
Severity—Worst credible result of accident due to hazard.

Hazard Severity—page 16

CATEGORY	NAME	CHARACTERISTICS
I	Catastrophic	Death Loss of System
II	Critical	Severe injury or morbidity Major damage to system
III	Marginal	Minor injury or morbidity Minor damage to system
IV	Negligible	No injury or morbidity No damage to system

Traditional risk management choices.

A. Terminate.

1. Engineering the risk out.

2. Remove the operation or process with which the risk is associated.

B. Treat

C. Transfer

D. Tolerate

Definitions.

A. Risk Acceptance: The process of identifying, quantifying (to the maximum practical degree), and accepting risk by the appropriate level of management.

C. Controlled Risk: The level of risk after controls are applied.

D. Residual Risks: An expression of probable loss from hazards that have not been eliminated.

E. Risk Management: The overall process of identifying, evaluating, controlling/reducing, and accepting risks.

F. Gambling: Making nonsystematic risk decisions.

Risk assessment steps.

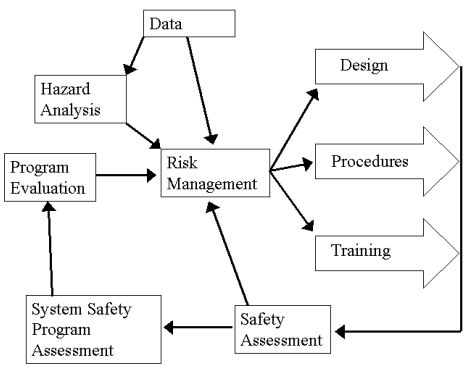
A. Hazard identification.

B. Hazard assessment.

C. Risk control options & decisions.

D. Risk control implementation.

E. Monitoring.



Risk management diagram

Risk management guidelines:

A. Integrate into planning - saves money, improves efficiency.

B. Accept no unnecessary risks.

C. Make risk decisions at proper level.

D. Accept risk if benefits outweigh the cost.

Society acceptance of risk.

A. If the public or interest group perceives a risk to be unacceptable it is unacceptable.

B. Perceived risks are very real to the perceivers.

C. Voluntary risks are more acceptable than involuntary.

D. Natural risks more acceptable than man-made.

E. Delayed effect more acceptable than immediate.

F. On-the-job less acceptable than off-the-job.

Society perception of risk.

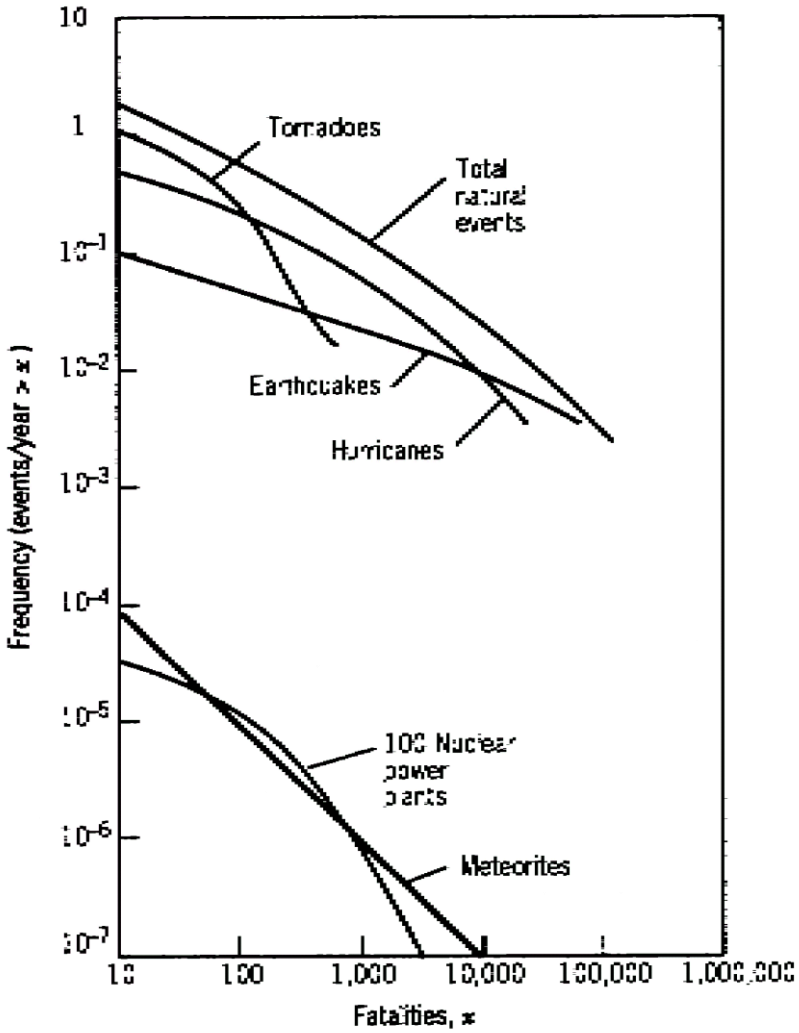
A. Tend to underestimate the level of risk for systems with which we are well acquainted.

B. Overestimate for the unknown.

C. Underestimate risks for activities that are believed to be controlled or are fun.

D. Overestimate risks for activities that are not understood or are dreary.

Risk of actual events. (Figure 32.3, page 309 (Roland))



Topic: **Risk Assessment (continued)—Facility Risk Assessment**

1. Introduction.—U.S. Army Corps of Engineers

2. **Step one**—initial risk categorization.

   A. Made early in the concept phase of the project.

   B. Purpose is to serve as an indicator for the level of effort and scope of the system safety program.

   C. Evaluating factors.

   D. Categorized.

      Low risk = requires a minimal SS effort and little user involvement.

      Medium = requires at least a PHA and some user involvement.

      High risk = requires a comprehensive SS effort and high user involvement.

3. **Step two**—systematic identification of hazards associated with the project.

4. **Step three**--Hazard information is converted to risk information by evaluating severity of potential accidents and the probability that the hazard could produce an incident.

Hazard Severity page 16

CATEGORY	NAME	CHARACTERISTICS
I	Catastrophic	Death Loss of System
II	Critical	Severe injury or morbidity Major damage to system
III	Marginal	Minor injury or morbidity Minor damage to system
IV	Negligible	No injury or morbidity No damage to system

5. **Possible Hazard Likelihood**

DESCRIPTION	LEVEL	SPECIFIC INDIVIDUAL ITEM	FLEET OR INVENTORY
Frequent	A	Likely to occur frequently	Continuously experienced
Probable	B	Will occur several times in life of an item	Will occur frequently
Occasional	C	Likely to occur sometime in life of an item	Will occur several times
Remote	D	Unlikely but possible to occur in life of an item	Unlikely but can reasonably be expected to occur
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced	Unlikely to occur, but possible
Eliminated	F	Incapable of occurrence	Incapable of occurrence

6. Risk Assessment code matrix used in the facility system safety effort:

Risk assessment code (RAC)

Risk Assessment Code Matrix (RAC)				
PROBABILITY	**SEVERITY**			
	I Catastrophic	II Critical	III Marginal	IV Negligible
A Frequent	1	1	1	3
B Probable	1	1	2	3
C Occasional	1	2	3	4
D Remote	2	2	3	4
E Improbable	3	3	3	4
F Eliminated	Eliminated			

7. Facility Risk Acceptance
   RAC 1 - Unacceptable
   RAC 2 - Undesirable
   RAC 3 - Acceptable with controls

RAC 4 – Acceptable

8. **Step four**--Control rating code.

   A. Used to evaluate alternative control measures

   B. Rules for use:

      1) The CRC should never be more than 1 digit higher than the original RAC it controls.

      2) No single-point failures are allowed in severity level I or II mishaps.

      3) RAC 1 or 2 hazards cannot be controlled with cautions, warnings, or personal protective equipment only.

Design passive device—that provides protection automatically.

Active safety device—requires application or activation by the user or operator, or warning devices only.

9. Control Rating Code for CRC Matrix

		Design	Passive Safety Device	Active Safety Device	Warning Device
		I	II	III	IV
A	Eliminate Energy Source	1	1	2	3
B	Limit Energy Source	1	1	2	3
C	Prevent Release	1	2	2	3
D	Provide Barriers	2	2	3	4
E	Change Release Patterns	2	3	4	4
F	Minimize/Treat Harm	3	3	4	4

10. After the control is figured out a second RAC is determined.

    A. The CRC is evaluated to ensure the rules have been met.

    B. Controlled RAC is 3 or 4.

    C. If the CRC rules are met and the RAC is 3 or 4 the corrective action is taken and the risk has been reduced to an acceptable level.

Topic: **Risk Assessment (TREC)**

1. Introduction.

2. There are ten severity codes that represent single event losses from less than $100 to over $10 billion, with each severity code increasing by an order of magnitude.

   A. SEVERITY CODES

CODE	RANGE	AVERAGE
10	>10 Bil	5×10^{10}
9	1-10 Bil	5×10^{9}
8	100 Mil-1 Bil	5×10^{8}
7	10-100 Mil	5×10^{7}
6	1-10 Mil	5×10^{6}
5	100 K-1 Mil	5×10^{5}
4	10-100 K	5×10^{4}
3	1-10 K	5×10^{3}
2	100-1000	5×10^{2}
1	<100	5×10^{1}

   This scale provides a *more meaningful assessment of the hazards associated with systems capable of producing multiple deaths and hundreds of millions or even billions of dollars in total losses*.

3. The ten exposure codes represent estimates of the total number of accidents of the system.

A. EXPOSURE CODES

CODE	RANGE	AVERAGE
10	>1000	5×10^{3}
9	100-1000	5×10^{2}
8	10-100	5×10^{1}
7	1-10	5×10^{0}
6	0.1-1	5×10^{-1}
5	.01-0.1	5×10^{-2}
4	.001-.01	5×10^{-3}
3	.0001-.001	5×10^{-4}
2	.00001-.0001	5×10^{-5}
1	<.00001	5×10^{-6}

Standard unit of time suggested for exposure calculations is *100,000 exposure hours*.

C. The exposure for each hazard is determined by:

Probability of a single occurrence (expressed in number of occurrences per 100,000 exposure hours) **X** the total estimated exposure hours during the life of the system **X** by the number of systems to be produced.

4. The total risk exposure code is determined by adding the severity and exposure code.

A. TOTAL RISK EXPOSURE CODE (TREC) MATRIX

		EXPOSURE CODE									
		10	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
SEVERITY CODE	**10**	20	19	18	17	16	15	14	13	12	11
	9	19	18	17	16	15	14	13	12	11	10
	8	18	17	16	15	14	13	12	11	10	9
	7	17	16	15	14	13	12	11	10	9	8
	6	16	15	14	13	12	11	10	9	8	7
	5	15	14	13	12	11	10	9	8	7	6
	4	14	13	12	11	10	9	8	7	6	5
	3	13	12	11	10	9	8	7	6	5	4
	2	12	11	10	9	8	7	6	5	4	3
	1	11	10	9	8	7	6	5	4	3	2

5. Formulas:

A. Total Risk Exposure (TRE)—The total number of dollars estimated to be at risk as a result of the particular hazard being evaluated.

$$TRE = 5 \times 10^{(TREC-5)}$$

B. Annual Risk Exposure (ARE)—The total risk exposure divided by the estimate project life in years.

$$ARE = \frac{TRE}{\text{Project Life}}$$

C. Unit Risk Exposure (URE)—A measure of the projected dollar loss per unit

$$URE = \frac{TRE}{\text{Number of units}}$$

OSH 452

Topic: **Human Factors**

1. Introduction.

2. Human Response.

3. Human failure modes.

   A. Human performance varies—Performance = (Aptitude + Training) X Motivation.

   B. Ability to function under stress varies.

   C. Boredom vs Vigilance

   D. Expectation and stereotypes

E. Perception

F. Coupling –

4. The variability in stress resistance and the multiple failure modes of humans tend to make human error rates relatively high.

5. Human error rates.

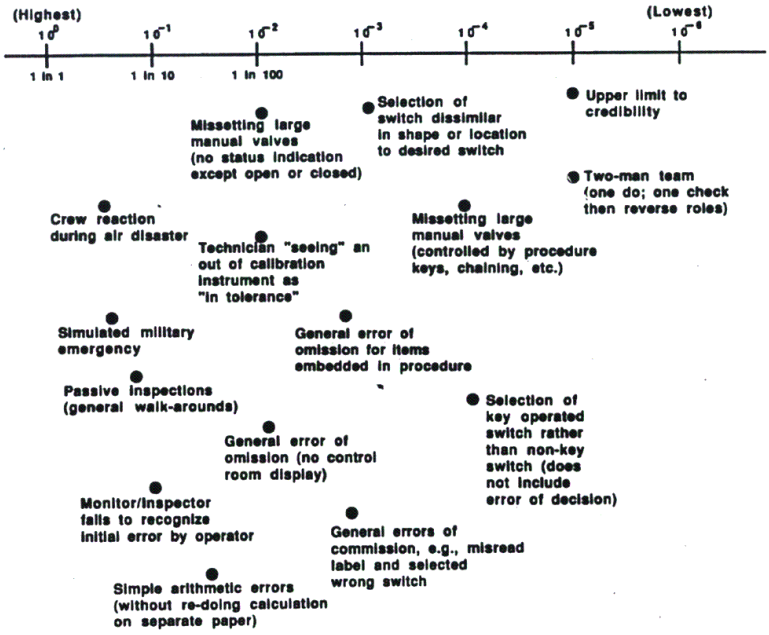


Figure 12-2 Estimates of human performance error rates. (Source: SSDC course handouts. Data points were compiled from various government studies.)

Note that a general walk-around inspection will fail to identify about 10% of workplace hazards.

Bottom line—Humans are the least reliable component in many systems.

Army Battle and Non-Battle Losses in Theater

	WWII 1942-45	Korea 1950-53	Vietnam 1965-72	DS/DS 1990-91	NTC 1988-89
	Rate per 1,000 Soldiers				
Accident*	95.57	120.33	154.66	11.14	3.52
Friendly fire	1.50**	3.03**	2.67**	.68	2.89***
Enemy action	73.61	148.56	131.02	2.90	105.56***

*Deaths and injuries (ground and aviation)
**Research-based estimate (2% of all direct- and indirect-fire losses)
***Simulated (MILES) direct fire vehicle kills.

6. Human factors is multi-disciplinary:

7. Human Factors Engineering.

   A. Designing the system so that machine, human tasks and environment are compatible with the capabilities and limitations of people.

   B. Engineering the system for the population that will use it.

8. Human factors are applicable. - Crane Levers. (Examples)

9. Examples of human factors considerations:

   A. People tend not to look where they put their hands/feet.

   B. Large or dark objects imply "heaviness", small or light-colored ones appear light in weight.

   C. Knobs on electrical equipment turn clockwise for on or to increase.

   D. Exit doors should be pushed; enter doors pulled.

   E. Seat heights are expected at a certain level.

   F. Red means Stop or Off; Green means Go or On.