OSH 452

Topic: **Probability**

Concept of probability

Probability—ratio of occurrences of specified types to total number of occurrences.

Probability Examples

Be careful about the amount of data you have, you must have enough data.

The last 10 years Acme taxi had the following experience:

Acme Taxi Accident Experience:

YEAR	ACCIDENTS	TRIPS
2001	8	1000
2002	10	1250
2003	6	1100
2004	9	1150
2005	12	1300
2006	3	1350
2007	4	1400
2008	2	1500
2008	3	1475
2010	2	1600
TOTAL	**59**	**13125**

You must be careful not to bias the probability when you choose which data to use. Try to use as much data as possible. Generally 3-5 years of data are sufficient.

PROBABILITY LIMITATIONS

Probability is always bound by 0 and 1.

ADDITION LAW

P(A or B) = P(A) + P(B)

MULTIPLICATION LAW
P(A and B) = P(A) * P(B)

COMPLEMENTARY LAW
P(Not A) = 1-P(A).

Given Information:
Accidents 0 or 1 or 2 or 3 or ... or 400
P(0, 1, 2, 3,...,400) = .349 + .387 + .172 + .081 + ... + .000 = 1
The numbers represent the probability that a company would experience that exact number of accidents in 400 trips.

In this example we assume that once an accident occurs, the trip is over. Therefore, in 400 trips there can be only 400 accidents. The total of all the probabilities of accidents the company might experience must equal 1.

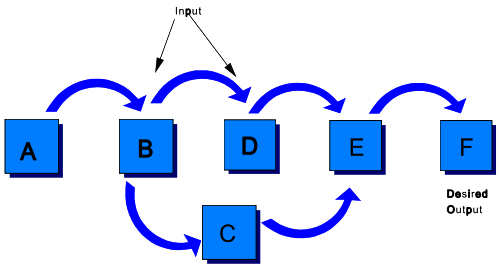
DEPENDENCE VS INDEPENDENCE
Dependence—What happens on one trial affects the probability of the next trial.

Independence—What happens on one trial does not affect the probability of the next trial.

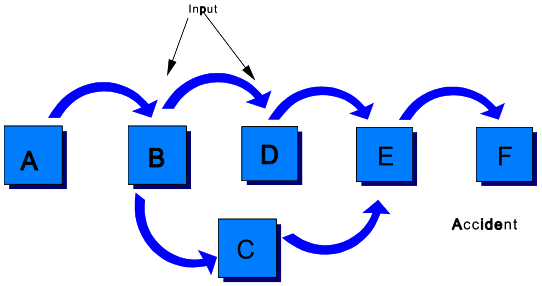
Topic: **Network Theory**

1. **Definitions:**

Reliability Network—To get desired output you must have certain inputs.

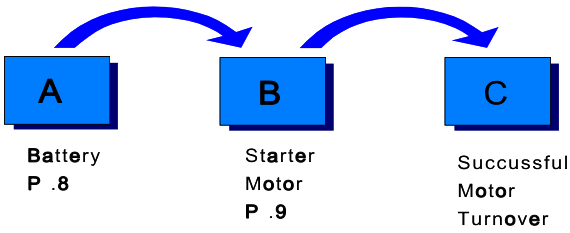


Accident Network—To get undesired output (accident) certain inputs must exist.



2. Series System.

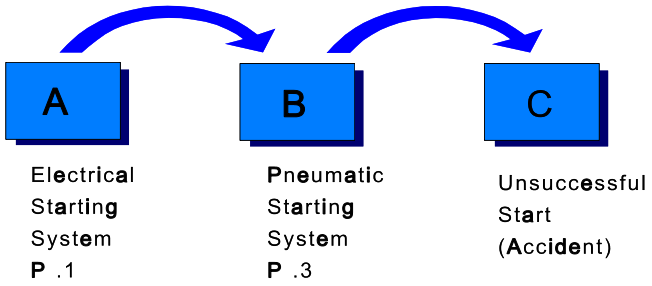
Reliability Example:



P(Success) = P(A and B) the only way C can happen is if A and B happens.

Series system is not desirable because system reliability is lower than component reliabilities.

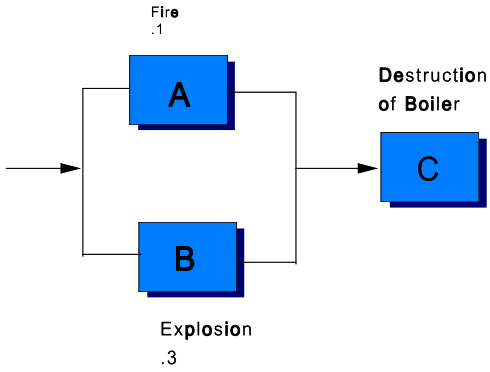
Accident Example: Accident (C) can only happen if A happens and then B happens. Both events must occur or A must fail to work and B must fail to work before C (accident) occurs.



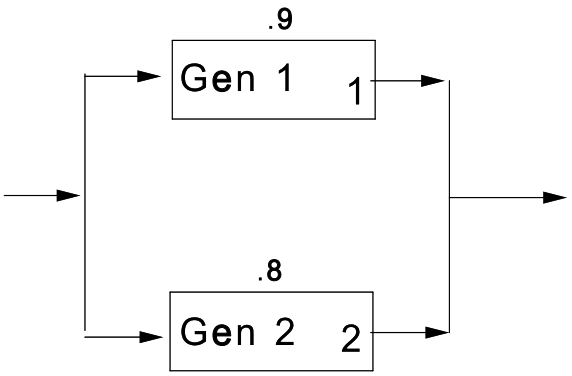
A series relationship is good because the probability of an accident decreases.

3. Parallel System.

Accident Example:



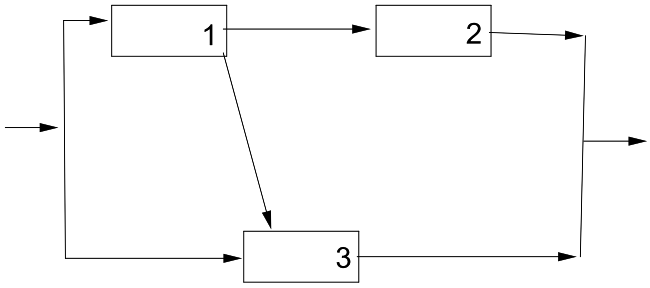
Overall probability of destruction is higher than individual probability of failure. A parallel relationship in accident systems is BAD because the probability of an accident increases.



(a)	Gen 1 works	*	Gen 2 works	=	.9	*	.8	=	.72
(b)	Gen 1 works	*	Gen 2 fails	=	.9	*	.2	=	.18
(c)	Gen 1 fails	*	Gen 2 works	=	.1	*	.8	=	.08

Topic: **Cut Sets**

Reliability system.

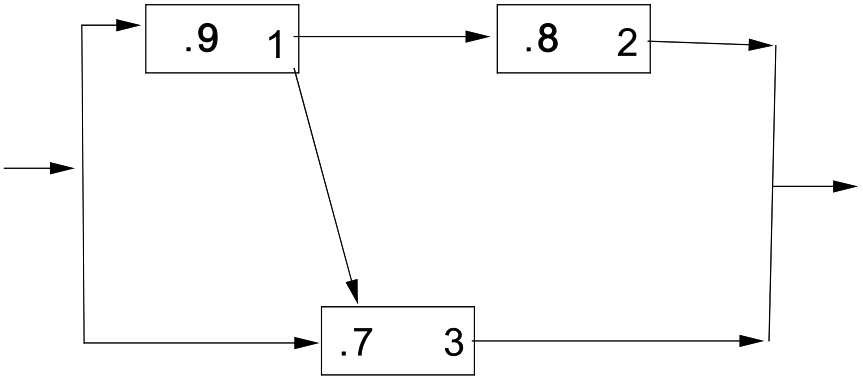


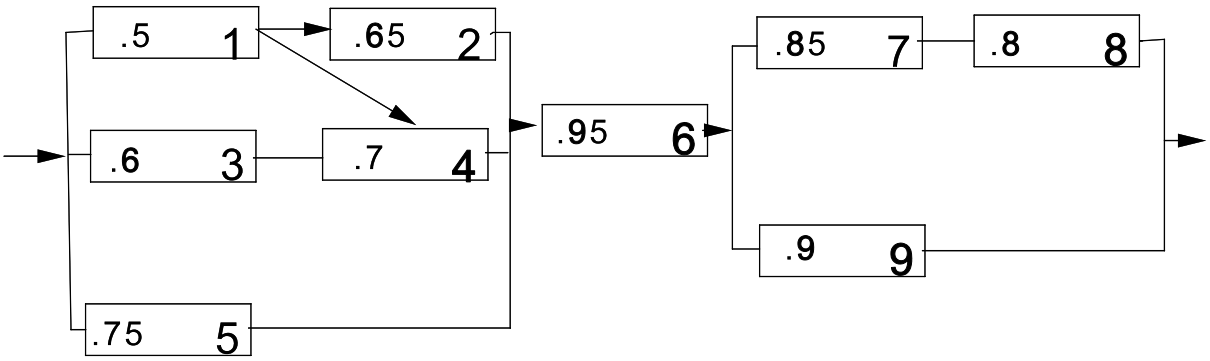
Cutting the system—What blocks must fail at the same time in order to make the system fail?

Minimum Cut Sets—All blocks in a set are necessary for failure.

Provides the upper bound on the probability of system failure.

Calculation




.5
1
.65
2
.6
3
.7
4
.75
5
.95
6
.85
7
.8
8
.9
9

Topic: **Fault Tree Analysis** - Construction

1. Developed by:

2. Uses of Fault Tree Analysis.

3. Timing.

4. Scope of Fault Tree Analysis.

Construction Approach.

5. Overall construction sequence.

    A. Identify undesired event.

    B. Determine all events leading to undesired event.

    C. Determine critical paths (cut sets).

    D. Quantify end events.

    E. Determine the importance/significance of various paths

6. Types of Fault Events.
    A. Fault - the failure of a component of a system.

B. Primary fault -
Failure of component due to internal characteristics in normal operating conditions.

C. Secondary fault-
Failure due to external stresses or environment

D. Commanded fault -
Failure due to incorrect input to the component.

"No Miracle Rule"

7. Symbols.

A. Fault Event-which must be further analyzed. (primary/command fault). (rectangle)

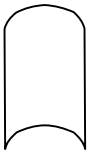
B. Basic Event-no further analysis necessary. (secondary fault) (circle)

C. Undeveloped Event -not analyzed further due to lack of information or is insignificant.) (diamond)

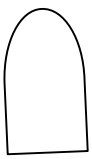
D. Normal event- Event that is expected to occur normally.

E. Gates.

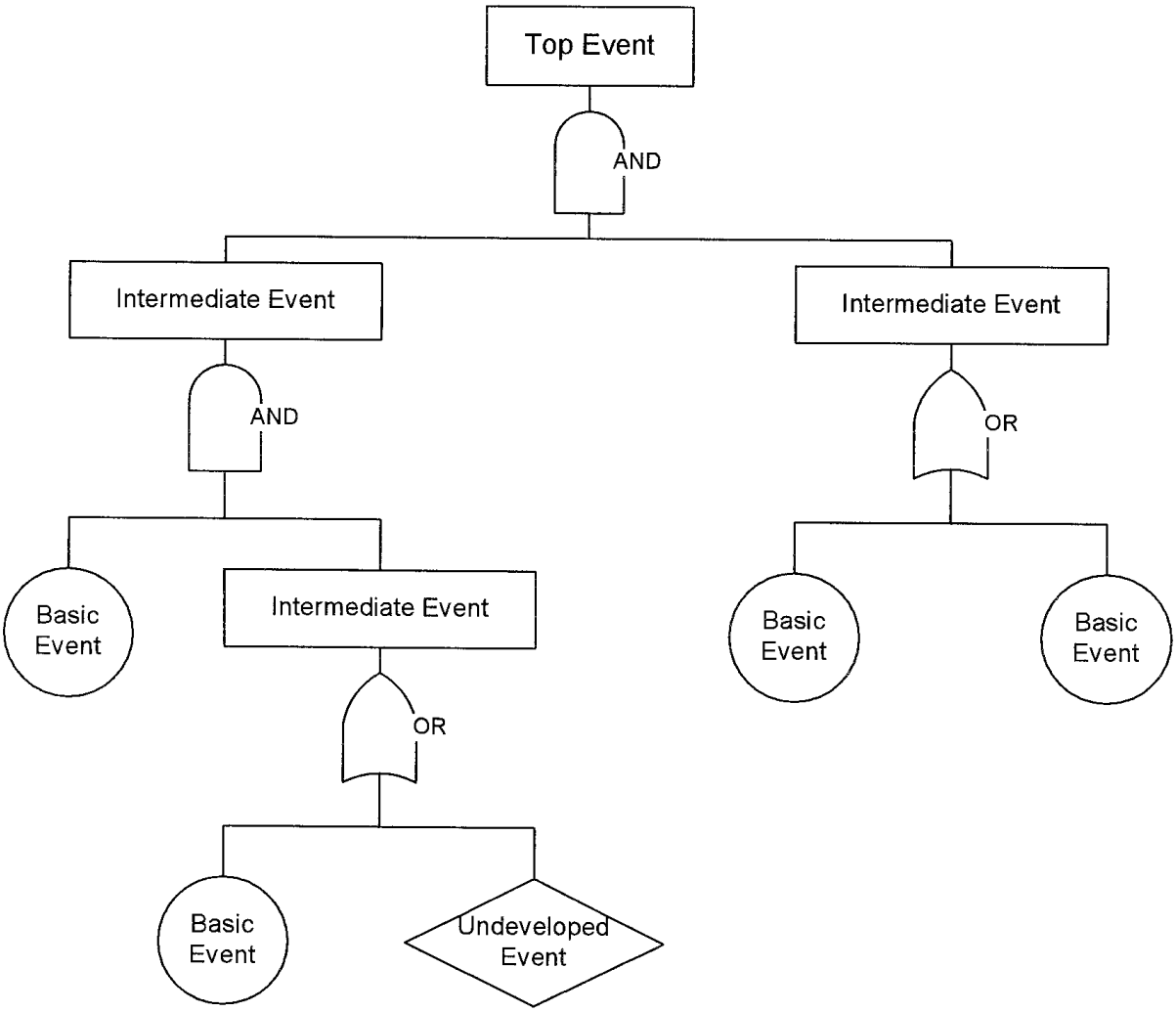
1) "or" gate - one or more events apply.



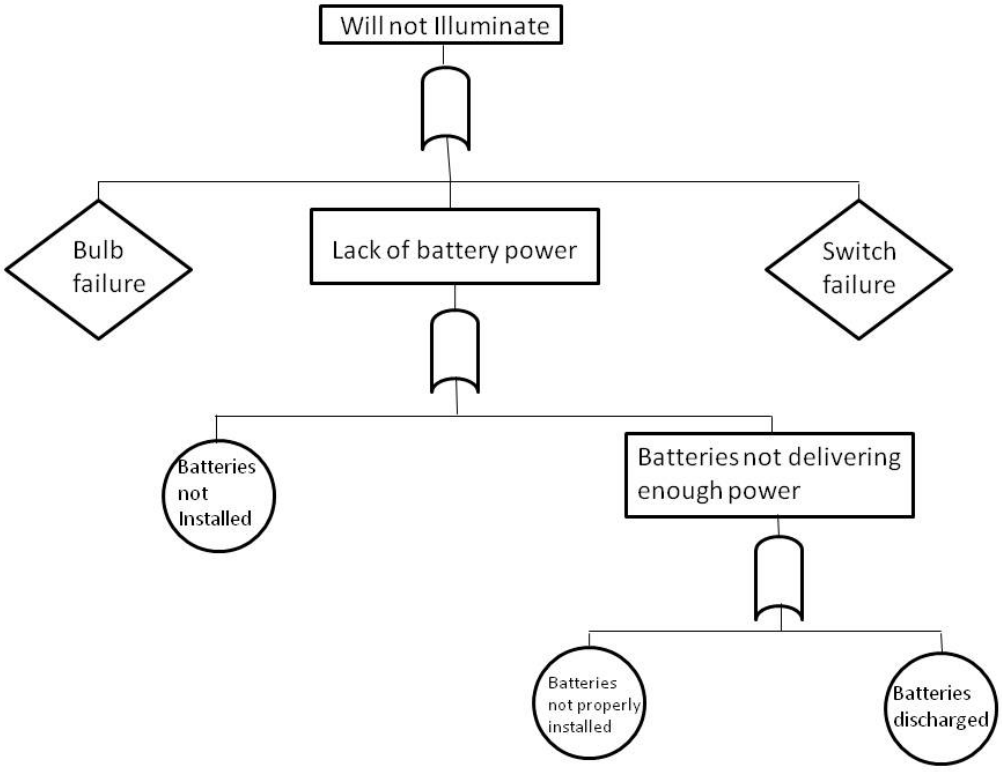
2) "and" gate - all events apply.



How Fault Trees are drawn



Examples.
Battery Operated Flashlight.



Drawing Rules:

A. If you have a rectangle (means must analyze further) you must have a gate and at least two events under it.

B. All branches must end with circles (basic event) or triangles (event not developed further).

C. Must have an event between gates

9. Characteristics of Fault Tree Analysis.

   A. Deductive approach.

   B. Focuses on the undesired event

   C. Not restricted to series & parallel networks.

   D. Allows for either quantitative and qualitative analysis.

   E. Forces "system insight."

   F. (Negative) Very tedious and a costly approach.

OSH 452

Topic: **Fault Tree Analysis - Quantification**

1. Quantification of Fault Trees.

Fault trees are equations. We solve them using Boolean algebra and cut set theory.

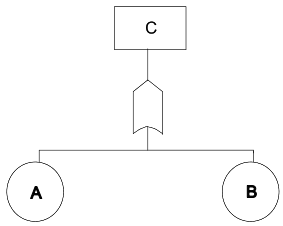
Boolean algebra—Don't duplicate events.

Cut Sets—Focused on critical paths (minimum cut sets)

Logical gates.

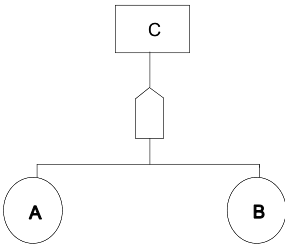
a) "or" any of the events could have caused the undesired event. Boolean "union" or +.

P(*C*) = P(*A* + *B*)



b) "and" intersection or *.

P(*C*) = P(*A* * *B*)



A. Steps. (Do in listed order).

1) Start at top of tree & develop equations 1 level at a time.

2) Substitute events into the overall equation.

3) Reduce the equation using Boolean algebra.

4) Determine most critical paths.

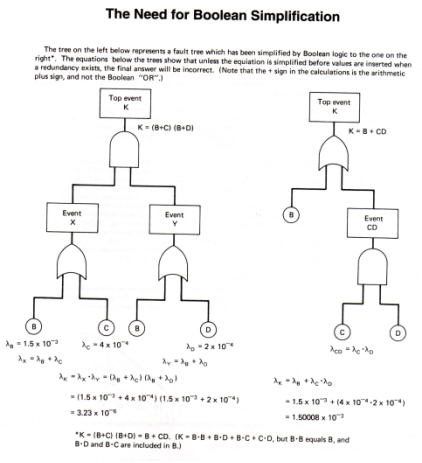
5) Determine equivalent fault tree.

6) Relative determination of safety.

7) Quantify the fault tree.

Handout

Calculate probability:



1. Figure out equation.
   K = (B + C) (B + D)

2. Simplify equation. *[Multiply B by B+D and C by B+D]*
   K = BB + BD + BC + CD

3. Factor. (BB is same as B)
   K = B + BD + BC + CD

4. Continue to Factor. (B is in BD and BC, remove them)
   K = B + CD

5. Solve Probability (substitute numbers)

   K = .0015 + (.0004 * .0002) (converted powers to decimals)
   K = .0015 + (.00000008)
   K = .00150008 or 1.50008×10^{-3}

OSH 452

Topic: **Fault Tree Analysis - Wrap-up**

1. Other quantitative measures:

   A. Fault Rate . Probability of failure over a specified time interval.

   λ

   B. Unreliability. Probability of one failure over a specified time interval.

   $\overline{R}$

   C. Mean Down Time. Mean time system is in a fault state.

   D. Expected Faults . Number of times the fault is expected in a given time interval.

2. Summary of Fault Tree.

   A. Deductive approach & analyzes inter-relationships and common faults.

   B. Requires detailed design information & is done at a later period during the system life cycle

C. Limitations.

1) Symbols confusing.

2) Gives cause and effect information only

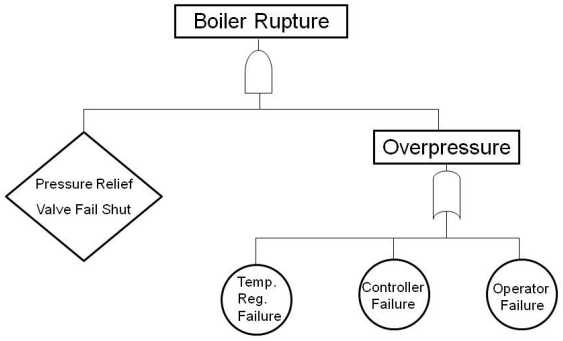
3) Boolean algebra & reductions may be tedious.

4) Relatively costly.

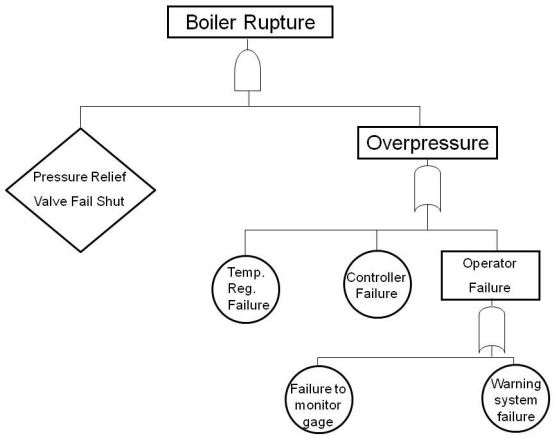
Examples of how fault tree works.

Boiler Ruptire

Original Design.



Modify design by adding a warning device.



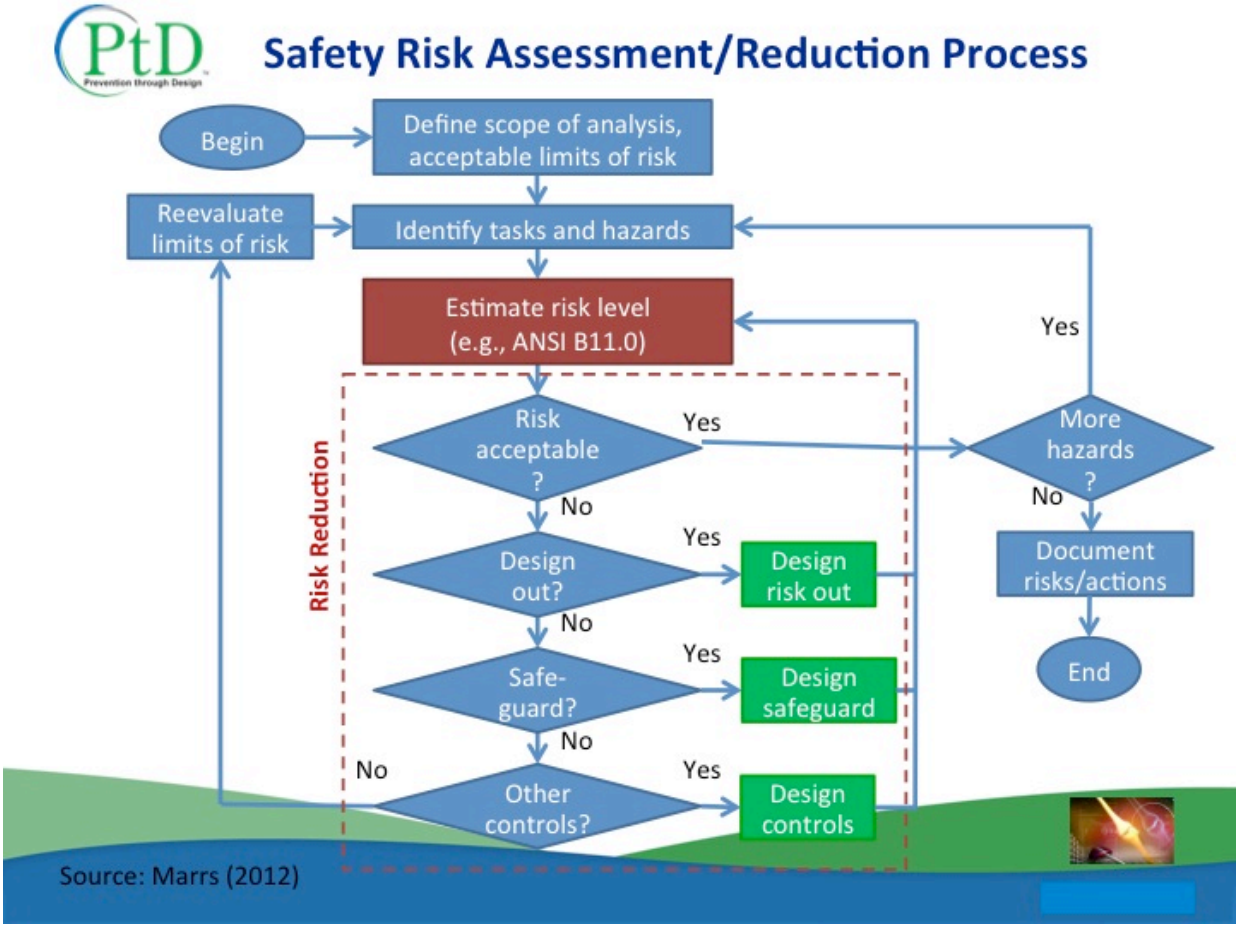
OSH 452

Topic: **Safety Through Design (Prevention Through Design)(Engineering for Safety)**

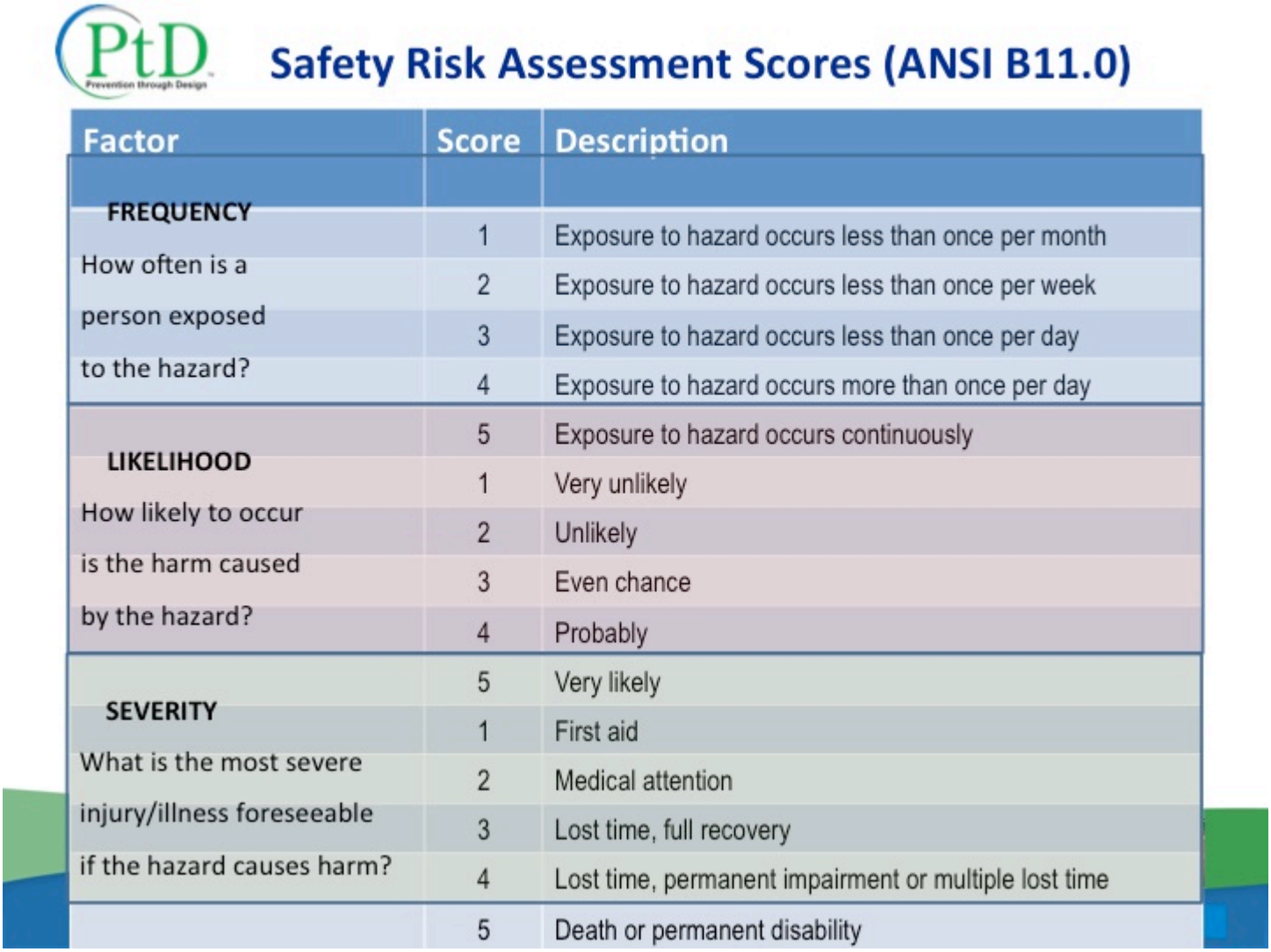
Definition

*Addressing occupational safety and health needs **in the design process** to prevent or minimize the work-related hazards and risks associated with the construction, manufacture, use, maintenance, and disposal of facilities, materials, and equipment.*

Safety Risk Assessment/Reduction Process



Safety Risk Assessment Scores



Factor	Score	Description
FREQUENCY How often is a person exposed to the hazard?	1	Exposure to hazard occurs less than once per month
	2	Exposure to hazard occurs less than once per week
	3	Exposure to hazard occurs less than once per day
	4	Exposure to hazard occurs more than once per day
	5	Exposure to hazard occurs continuously
LIKELIHOOD How likely to occur is the harm caused by the hazard?	1	Very unlikely
	2	Unlikely
	3	Even chance
	4	Probably
	5	Very likely
SEVERITY What is the most severe injury/illness foreseeable if the hazard causes harm?	1	First aid
	2	Medical attention
	3	Lost time, full recovery
	4	Lost time, permanent impairment or multiple lost time
	5	Death or permanent disability

Hierarchy of Controls

- ELIMINATION
- SUBSTITUTION
- ENGINEERING CONTROLS
- ADMINISTRATIVE CONTROLS
- PERSONAL PROTECTIVE EQUIPMENT

PTD---Prevention Through Design

Why PTD? Tangible Benefits

- Reduced site hazards
- Fewer worker injuries and fatalities
- Reduced workers' compensation premiums
- Increased productivity and quality
- Fewer delays due to accidents
- Encourages designer-constructor collaboration
- Improved operations/maint./safety

Examples

PTD Example: Anchorage Points

Design anchorage points into the design both for construction and for maintenance.

PTD Example: Roofs and Perimeters

"Detailing Guide for the Enhancement of Erection Safety"
Published by the Steel Erectors Association of America

Gives guidance on how to design.

The Erector Friendly Column
Includes holes and joints at specified points for fall protection and connections.

Avoid hanging connections
Better for connections to be on top instead of hanging.

Eliminate sharp corners

Know approximate dimension of necessary tools to make connections.

Install temporary ladders, platforms and safety lines

Southern Co.'s Design Checklists

Sutter Health's IPD Process
Integrated Project Delivery (IPD) facilitates collaboration of design and construction professionals during design

- Co-located
- Processes and norms for candid feedback
- Trust
- Sufficient time
- Life cycle costing criteria
- Common success criteria

National Initiatives and Activities

- NIOSH PtD National Initiative
- ANSI/ASSE PtD Standard (Z590.3-2011)

PTD Design Review (Prevention through Design)

- Hazard identification
- Risk assessment
-
- Design option identification and selection

1700+ ITEM PTD Checklist—has been published by NIOSH.

Obstacles to PTD

Solutions to barriers involve:

- long-term education
- institutional changes

Obstacle: Designers' Fear of Liability

- Barrier: Fear of undeserved liability for worker safety.
- Potential solutions:
  - Clearly communicate we are NOT suggesting designers should be held responsible for construction accidents.
  - Develop revised model contract language
  - Propose legislation to facilitate DfCS without inappropriately shifting liability onto designers.

Obstacle: Increased Designer Costs

Barrier: DfCS processes will increase both direct and overhead costs for designers.

Potential solution:

Educate owners that total project costs and total project life cycle costs will decrease.

Obstacle: Designers' Lack of Safety Expertise

- Barrier: Few design professionals possess sufficient expertise in construction safety.
- Potential solutions:
  - Add safety to design professionals' curricula.
  - Develop and promote OSHA courses for design professionals.
  - Utilize IPD to allow for constructor input.

Steps towards PTD

1. Establish a lifecycle safety culture
2. Establish enabling processes
3. Team with organizations who value lifecycle safety

Culture------Processes------Partners

Establish a Lifecycle Safety Culture

- Instill the right safety values
- Secure management commitment
- Confirm Life Cycle Costing criteria
- Ensure recognition that designing for construction safety is the smart thing and the right thing to do

Establish Enabling Processes

- Qualifications-based contracting
- Negotiated or Cost-Plus contracting
- IPD or enabled safety constructability input
- Collaborative decision processes
- Designer training and tools

Choose your Partners Wisely

- PtD in designer RFP
- Consider Design-Builders with industrial and international project experience

Summary

- Successful owners and design-builders have implemented PtD
- Keys to implementing PtD
    - Life cycle cost perspective and budgeting
    - Contracts facilitate collaboration between all project team members
    - Designers knowledgeable of PtD and equipped with PtD tools
- Three first steps to implementing PtD
    - Culture, Processes, Partners
- You can be a leader in implementing PtD in your organization

OSH 452

Topic: **Process Safety**

1. History of the Standard.

   A. A 30-year review of the chemical industry 100 largest loss events

   B. Catastrophic events:

      1) Union Carbide.

      2) Phillips 66.

   C. EPA Study

   D. Clean Air Act Amendments (CAAA) of 1990.

Title: Process safety management of highly hazardous chemicals.

2. Purpose—Enhance awareness of safe handling & storage of highly hazardous chemicals in industry.

3. Applicability:

   A. Performance-based approach.

   B. Applies mainly to chemical, oil, paper, food processing, fabricated metals production companies, and pyrotechnics & explosives manufacturers.

   C. Covers plants that deal with specific chemicals (330) in quantities above specified thresholds or that handle flammable liquids & gases in quantities greater than 10,000 lbs.

4. Review of Major Components:

   A. Collect & document data on process chemicals, technology, and equipment.

   B. Develop written operating procedures.

      1. Written procedures for all aspects of operation:

         1) Initial startup.
         2) Normal operations.
         3) Temporary operations.
         4) Emergency shutdown.
         5) Startup following normal shutdown.
         6) Steps for operating limits.
         7) Safety & health considerations.
         8) Safety systems & their function.

2) Operating procedures must be readily accessible.

3) Procedures must reflect up-to-date practices.

4) Must certify annually that operating procedures are current & accurate.

5) Safe work practices must be implemented to ensure hazard control during operations.

6) Procedure changes must be properly authorized and updated & affected employees trained.**}**

C. Establish a management-of-change procedure.

D. Employee participation.

E. Conduct a pre-startup review for new facilities.

F. Train employees involved in the process.

G. Evaluate contractors.

H. Develop a mechanical integrity program.

I. Develop provisions for hot work permits.

J. Emergency planning & response.

K. Conduct a compliance audit at least every three years--to ensure that procedures and practices are adequate.

L. Incident investigation.

M. Conduct a process hazards analysis.

Must address:

1) Process hazards.

2) Identification of previous incidents.

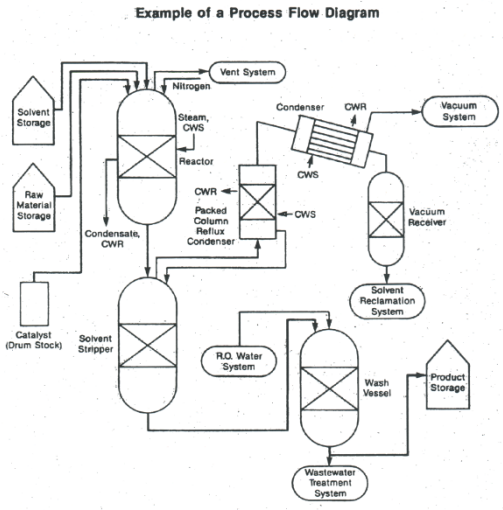
3) Engineering & administrative controls used.

4) Human factors.

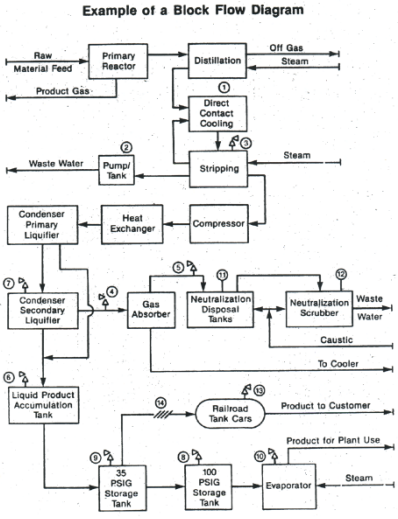
5) Consequences of failure of controls.

6) Strongly recommends block flow diagrams and process flow diagrams.

Process Flow Diagram.



Block Flow Diagram



5. Analysis Techniques.

A. **What-if**.

Summary: Provides comprehensive coverage of a broad range of hazards.

Procedure: Brain-storming method whereby the applied experience of the team is used to derive potential operating problems and determine their effects.

Advantages: Is relatively easy to use and good for relatively uncomplicated processes.

Concerns: Quality depends on the reviewer's experience & background. The right questions must be asked to perform an effective analysis.

B. **Checklists.**

Summary: Uses checklist previous developed.

Procedure: Go down the checklist checking and answering questions posed.

Advantages: Directly addresses the most important areas.

Concerns: Checklist may miss important areas.

C. **Failure mode and effects analysis (FMEA).**

Summary: Methodical approach to failure mode and consequences.

Procedure: Each system component or subsystem is postulated to fail and the failure's effect on the system and any external effects are determined.

Advantages: Works best when studying a specific item of equipment. It's semi-quantitative approach assists in ranking hazards.

Concerns: It assumes normal operation is satisfactory. An accurate model or diagram must be developed to proceed effectively.

D. **Hazard and Operability Study (HAZOP).**

Summary: Structured engineering review to determine the response of systems to deviations from design parameters .

Procedure:

Process broken down into line/vessel/equipment/control/ operating sequence (Node).

Guide words coupled to design parameters.

Deviation—combination of a guide word and a parameter.

Advantages: Determines how deviations from design intentions can occur & whether consequences of such deviations are hazardous. Promotes employee involvement.

Concerns: Its assumption that all designs are correct for normal situations. Requires a good team leader and good model diagrams. Time-consuming and expensive.

E. **Fault tree analysis (FTA).**

Summary: Defines various routes to a top event and quantifies probability of reaching that event.

Procedure: Determine undesired events and causes that contribute to the events.

Advantages: Provides objective information for decision-making.

Concerns: Focuses on events, rather than the process, & requires quantitative techniques & expertise. Often reserved for critical hazard situations.

F. **An appropriate equivalent methodology**.

6. Mandatory & non-mandatory sections.

7. Overlap with EPA rules.

Parallel Provisions of OSHA, EPA Rules	
Process Safety Management OSHA 29 CFR 1910.119	**Chemical Accidental Release Prev. EPA 40 CFR, Part 68**
Application (a)	Applicability - 68.10
Definitions (b)	Definitions - 68.3
Employee participation (c)	***Not covered***
Process safety information (d)	Process safety information - 68.26
Process hazards analysis (e)	Process hazard analysis - 68.24
Operating procedures (f)	Standard operating procedures-68.24
Training (g)	Training - 68.30
Contractors (h)	*Not covered*
Pre-startup safety review (i)	Pre-startup review - 68.34
Mechanical integrity (j)	Maintenance - 68.34
Hot work permit (k)	*Not covered*
Management of change (l)	Management of change - 68.36
Incident investigation (m)	Accident investigation - 68.40
Emergency planning & response (n)	Emergency response - 68.45
Compliance safety audit (o)	Safety audits - 68.45
Trade secrets (p)	*Not covered*

8. Positive effects.

   A. Reduce potential for a catastrophic incident.

   B. Reduce waste.

   C. Increase production and improve procedures.