CHAPTER 12

The System and Software Safety Process

Alix Martin

Introduction

- General Tasks
  - Conceptual Development
  - System Design
  - Full Scale Development
  - System Production and Deployment
  - System Operation
- Examples
  - An Underground Rail Station
  - A Combat Weapon System
  - The NASA Space Shuttle Project

The General Tasks

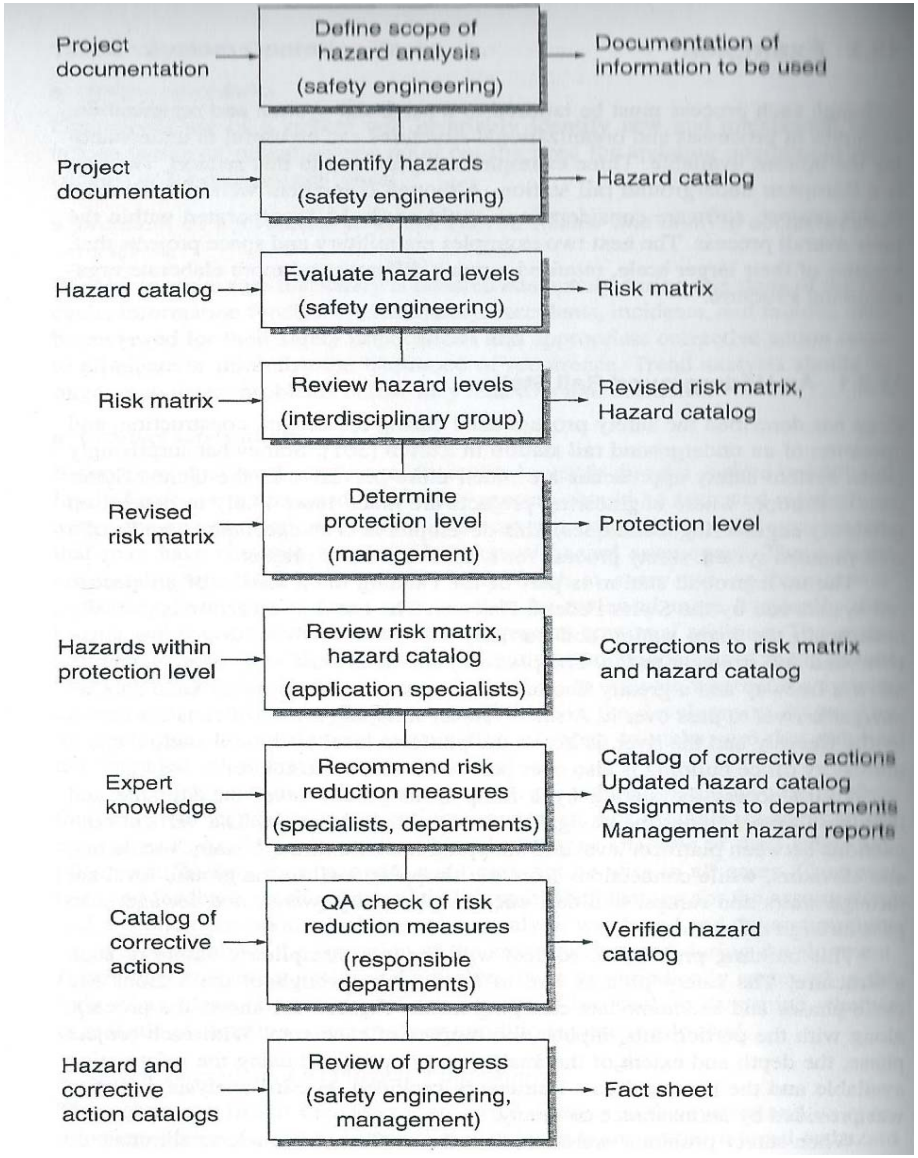
- System safety has its own task and plays a safety coordinating role with respect to the entire program
- Tasks involved in system safety differ in the various phases of a project
  - Engineering project can be divided into 5 stages
    - Conceptual Development
    - System Design
    - Full Scale Development
    - System Production and Deployment
    - System Operation
- There are primary system safety activities during each of the phases.

An Underground Rail Station

- Zogg has developed an example of a well-planned system safety process for a relatively small project.
- Underground station of an electric rail system run by the Swiss Federal Railway. (Tunnel under river)
- Shows a process that displays inputs/outputs of each step.
- Hazard analysis expertise was provided by an insurance company.
- In depth analyses requires specialized knowledge and are performed by teams of experts on various aspects of the project.

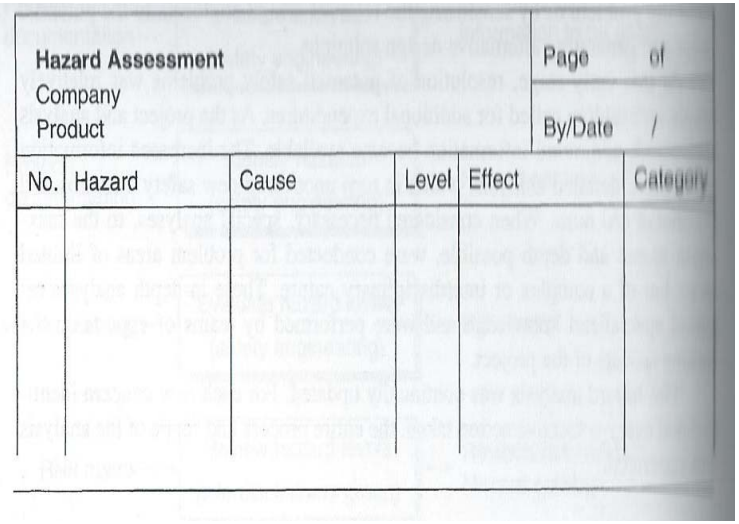
An Underground Rail Station

- Definition of Scope
  - Safety personal define the hazards scope before the analysis.
  - When analyzed, in terms of track length and width, and the lowest and highest level of the structure.
  - 3D frame drawn out, providing various levels of information of different project components.
  - Also helps define what type of structure and construction methods are required.



An Underground Rail Station

- Hazard Identification and Assessment
  - Hazardous characteristics of the system (malfunctions or environmental).
  - A list of questions, called a *ticker list*, was used to help uncover hazards.
  - Hazard identification includes:
    - The hazards
    - The causes
    - The levels – six levels representing relative probability of occurrence of cause: Frequent, Moderate, Occasional, Remote, Unlikely, Impossible
    - The effects – four categories representing severity of effect: Catastrophic, Critical, Marginal, Negligible
    - The categories – establishes priorities for identified hazards.
  - The number in the boxes represent the criticality.
  - An arbitrary breakpoint called the protection level helps define how in depth risk reduction efforts will be for concentrated hazards.

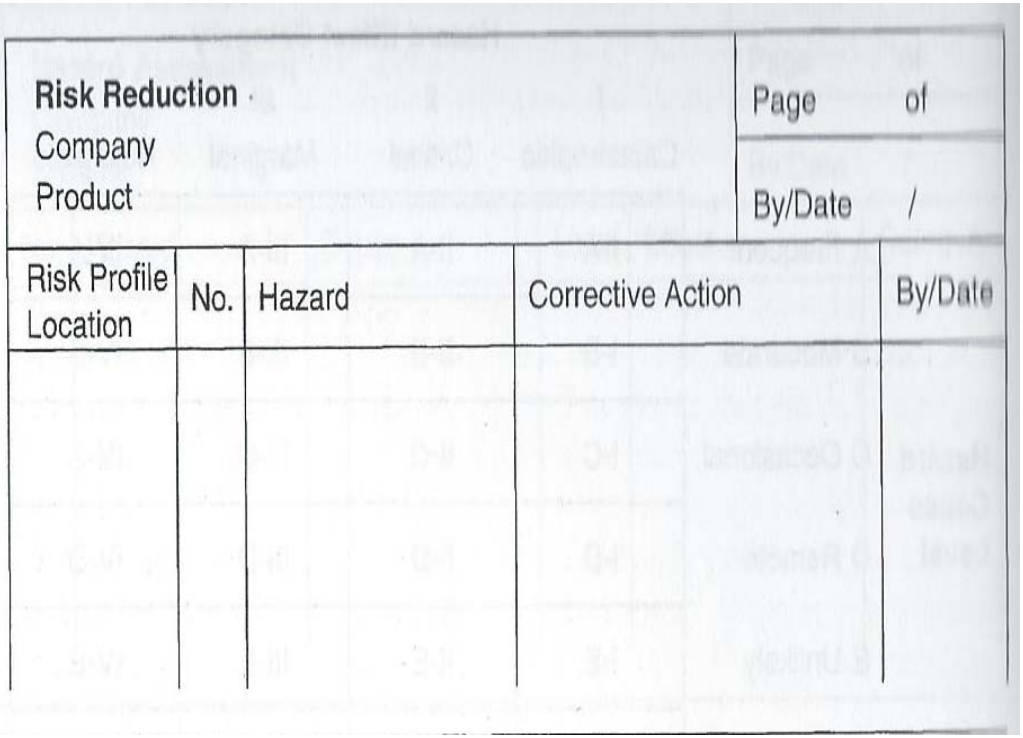


Hazard Assessment				Page of
Company				
Product				By/Date /
No.	Hazard	Cause	Level	Effect	Category

Hazard Cause Level	Hazard Effect Category I Catastrophic	II Critical	III Marginal	IV Negligible
A Frequent	I-A	II-A	III-A	IV-A
B Moderate	I-B	II-B	III-B	IV-B
C Occasional	I-C	II-C	III-C	IV-C
D Remote	I-D	II-D	III-D	IV-D
E Unlikely	I-E	II-E	III-E	IV-E
F Impossible	I-F	II-F	III-F	IV-F

An Underground Rail Station

- Risk Reduction
  - Efforts are made to protect against the possible hazardous conditions or events.
  - Each hazard is documented and assigned to specialists or departments that can help risk reduction.
  - Recommended risk reduction measures are cataloged with corrective actions.
  - Zoggs claims that this is important because the progress became visible in periodically updating risk profile and risk reduction catalogs.



Risk Reduction Company Product			Page of By/Date /	
Risk Profile Location	No.	Hazard	Corrective Action	By/Date

A Combat Weapon System

- Defense systems are developed using safety standard, MIL-STD-882 (set of task that may be required in any particular contract)
- System here is a U.S Navy cruiser with destroyer combat system equipped with nuclear weapons.
- Nuclear weapon systems are subject to different and more stringent standards.
- Very large project, required safety efforts from a prime contractor, associate contractors, and subcontractors.

A Combat Weapon System

- Tasks
  - Safety efforts consisted of three major functions
    - Establishment of a safety baseline (from Navy data files)
      - System Safety Engineering (SSE) prepares the Preliminary Hazard Analysis (PHA)
      - SSE prepares evaluated hazard reports
      - SSE defines the safety requirements for the specifications
      - SSE starts the system hazard analysis
    - Identification and elimination of control of hazards
      - With the baseline established, the system safety program is modified to prescribe a plan of action.
      - Update the PHA (sub functions in this grouping below)
      - Continuing the system hazard analysis
      - Participating in System Safety Working Groups (SSWG) and Nuclear Safety Advisory Group (NSAG) activities.
      - Perform various other types of required hazard analyses
      - Complete the Safety Summary Report (SSR), which is the reporting mechanism for all safety activities in Navy programs.
    - Safety verification
      - Inspections, demonstrations, and data analysis to determine the risk reduction.

A Combat Weapon System

- **Types of Hazard Analyses**
  - *A large number of hazard analyses were performed on this project.*
  - **Preliminary Hazard Analysis (PHA)-** Addresses each element and hazard related to radiation, acoustic noise, electrical energy, pressure, temperature…
  - **System Hazard Analysis (SHA)-** Includes detailed studies of possible hazards created by interfaces between system components. (for corrective actions to take)
  - **Operating Hazard Analysis (OHA)-** Specifies training requirements, input to technical manuals, warning signs, emergency procedures.
  - **Maintenance Hazard Analysis (MHA)-** Provides warning notices, special tools, handling equipment.
  - **Computer Program Safety Analysis (CPSA)-** Identifies computer software safety requirements and traces these requirements through Combat, Prime Item Development, Program Performance, Program Design, and Interface Design specifications.
  - **Subsystem Hazard Analysis (SSHA)-** Uses fault trees failure mode and effect analyses for each subsystem to examine.
  - **Radiation Hazard Analysis (RHA)-** Deals with areas involving electromagnetic and ionizing radiation.
  - **Nuclear Safety Analysis (NSA)-** Assures that the combat system satisfies four DoD nuclear safety standards: There shall be positive measure to prevent nuclear weapon accident, There shall be positive measure to prevent deliberate prearming, There shall be positive measure to prevent inadvertent prearming, There shall be positive measure to ensure adequate security.
  - **Inadvertent Launch Analysis (ILA)-** Use qualitative fault tree analysis for engagement orders of target.
  - **Weapon Control Interface Analysis (WCIA)-** Use qualitative fault tree analysis to address isolation, launch priority.

A Combat Weapon System

- Safety Criteria
- The prime contractor's safety engineering group is responsible for establishing qualitative probability rankings of hazard occurrences, hazard consequences, and frequency of exposure.

- Shows hazard criticality index matrix for hazard severity and probability

- Reports used for them system
  - Safety test reports
  - System hazard alert reports
  - General safety analysis summary report
  - Combat system safety statement
  - Nuclear safety analysis report
  - Other various reports

Hazard probability ranking.

Rank	Level	Description
Frequent	A	Likely to occur frequently
Probable	B	Will occur several times in unit life
Occasional	C	Likely to occur sometime in unit life
Remote	D	Unlikely to occur in unit life, but possible
Improbable	E	Extremely unlikely to occur
Impossible	F	Equal to a probability of zero

	A Frequent	B Probable	C Occasional	D Remote	E Improbable	F Impossi
Catastrophic I	Design action required to eliminate or control hazard 1	Design action required to eliminate or control hazard 2	Design action required to eliminate or control hazard 3	Hazard must be controlled or hazard probability reduced 4	9	
Critical II	Design action required to eliminate or control hazard 3	Design action required to eliminate or control hazard 4	Hazard must be controlled or hazard probability reduced 6	Hazard control desirable if cost effective 7	Assume will not occur 12	Impossi occurre
Marginal III	Design action required to eliminate or control hazard 5	Hazard must be controlled or hazard probability reduced 6	Hazard control desirable if cost effective 8	Normally not cost effective 10	12	
Negligible IV	10	11	Negligible hazard 12	12	12	

The NASA Space Shuttle Project

- The Challenger accident involved failure in carrying out the process rather than flaws in the process itself.
- The Space Shuttle is one of the most complex engineering projects ever attempted.
- The operational phase of the Space Shuttle project is called the National Space Transportation System.
- Basic NASA safety policy is issued at the Administrator level and implemented by contractors involved in the Space Transportation System (STS) development.
- The Basic NASA safety policy is to:
  - Avoid loss of life, injury of personal, damage, and property loss
  - Instill a safety awareness in all NASA employees and contractors
  - Assure hazards are fully considered
  - Review and evaluate plans so that that meet safety requirements

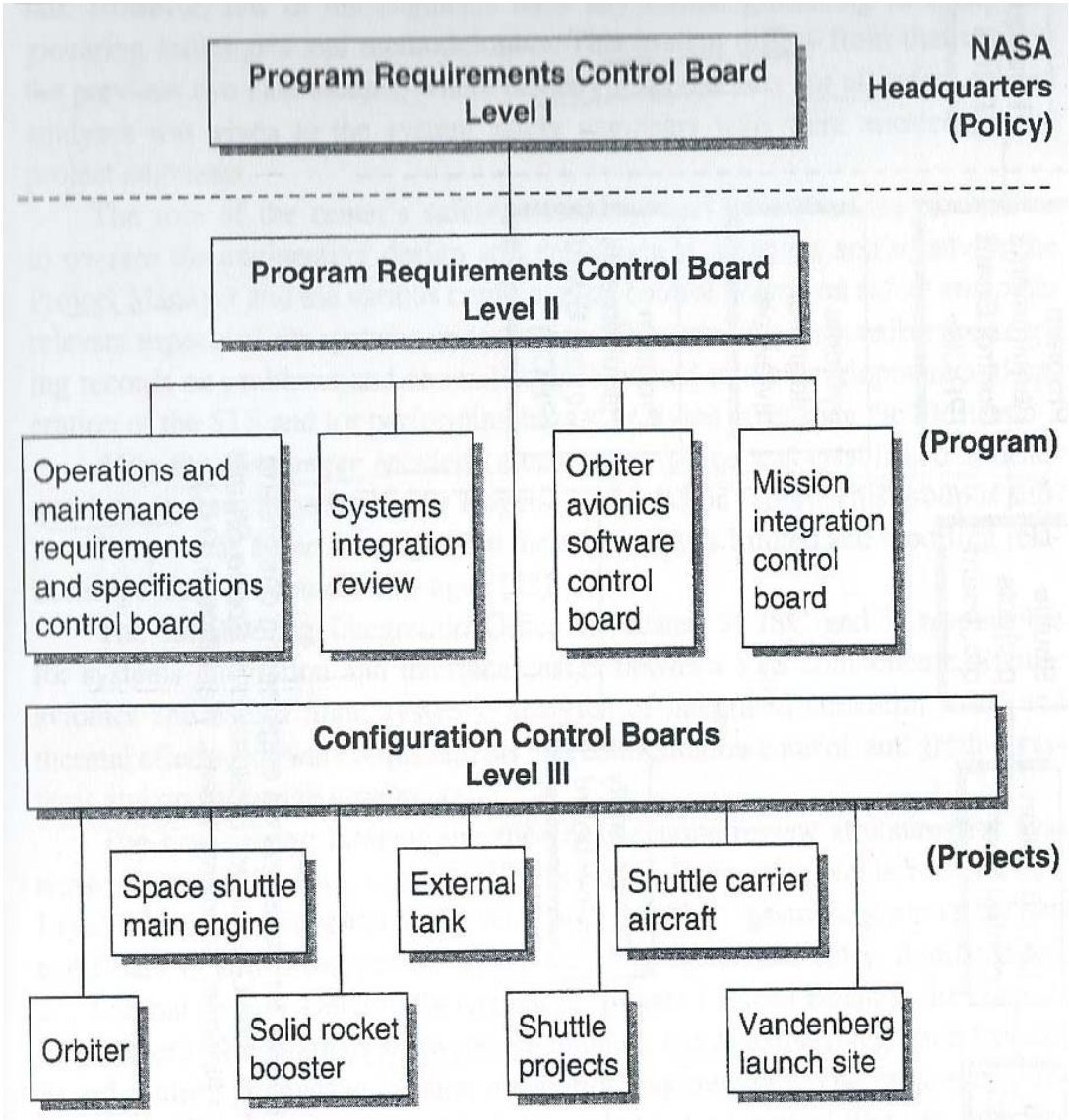
The NASA Space Shuttle Project

Management Structure

- The program draws on resources from three field centers.
  - Johnson Space Center (JSC) responsible for orbiter component of the STS
  - Marshall Space Flight Center (MSFC) responsible for propulsion components of the STS
  - Kennedy Space Center (KSC) responsible for major ground support for launch and landing operations.
- Project manager at each NASA center are responsible for particular components and subsystems.
- The hierarchy of management levels within the NSTS program
  - Level I- headquarters: concerned with policy
  - Level II- major program management (JSC) (KSC) program
  - Level III- project management (all centers) projects
- Each management level has associated boards that review and approve or disapprove actions proposed.
- The two Program Requirements Control Boards (Level I, Level II)- review results of failure modes and effects analysis.
  - Have authority to decide upon changes to documentation, hardware, and software

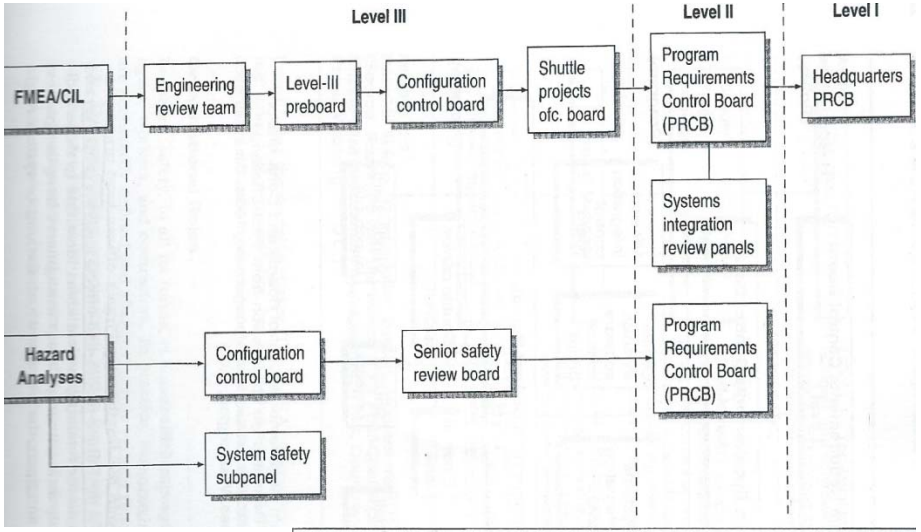
The NASA Space Shuttle Project

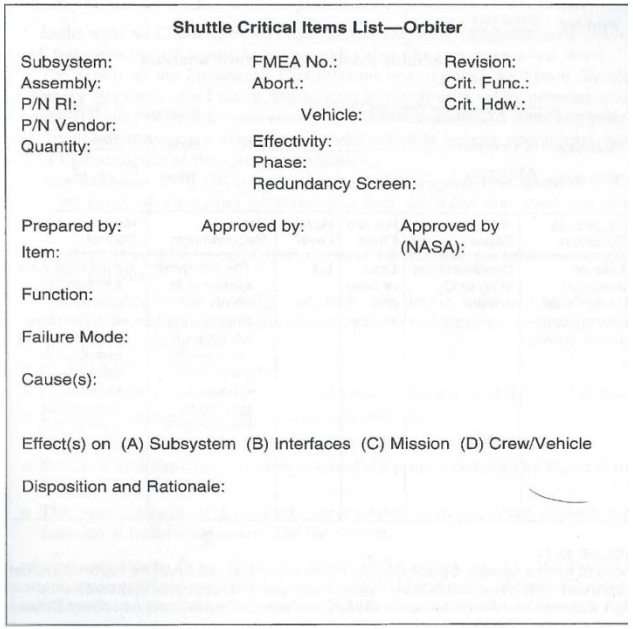
- Organizational Roles
  - Responsibilities are allocated across various functional organizations
    - The engineering organizations within the project offices
    - A Safety, Reliability, Maintainability, and Quality Assurance organization at headquarters.
    - The Engineering Integration Office
    - The operations organizations
  - After the Challenger accident, a new safety office was established: The Engineering Integration Office, included avionic software, and a separate review structure for system integration and software (Level I, Level II).
  - NASA engineers within the Engineering Project offices have primary responsibility for carrying out the failure modes and effect analyses (FMEAs).



The NASA Space Shuttle Project

- Safety Related Analyses
  - Critical Items Lists (CILs) and FMEAs help identify hardware items that are critical to the performance and safety of the vehicle and the mission.
    - Determine the potential failure modes for functional units
    - Analyzes it to determine resulting performance
    - Worst case effect of a failure in that mode
  - Items on the CIL must have design improvements to meet fail safe and redundancy requirements before Shuttle take off.
  - The Problem Reporting and Corrective Action (PRACA) system is a large database containing data from reports and information on corrective actions taken.
  - In wake of the Challenger FMEA/CIL's were reevaluated for deficiencies.
  - NRC audit report: Look at multiple event failure instead of single event failures.





Shuttle Critical Items List—Orbiter

Subsystem:
Assembly:
P/N RI:
P/N Vendor:
Quantity:

FMEA No.:
Abort.:
Vehicle:
Effectivity:
Phase:
Redundancy Screen:

Revision:
Crit. Func.:
Crit. Hdw.:

Prepared by:
Approved by:
Approved by (NASA):

Item:

Function:

Failure Mode:

Cause(s):

Effect(s) on (A) Subsystem (B) Interfaces (C) Mission (D) Crew/Vehicle

Disposition and Rationale:

Chapter 14
Hazard Analysis Models and Techniques

Alix Martin

Introduction

- Checklist

- Hazard Indices
- Fault Tree Analysis
- Management Oversight and Risk Analysis
- Event Tree Analysis
- Cause Consequence Analysis
- Hazards and Operability Analysis
- Interface Analysis
- Failure Modes, Effects, and Criticality Analysis
- State Machine Hazard Analysis
- Task and Human Error Analysis Techniques
- Evaluations of Hazard Analysis Techniques

- Conclusions

Checklists

- Description
  - Help provide feedback
  - Uniquely tailored to procedures and practices
  - List of a hazards or specific design features
  - Helps make sure things are not overlooked
- Life Cycle Phase
  - Provides information about known hazards or high risk conditions
  - Information gained during the hazard analysis process
- Evaluation
  - Help designers ensure good engineering design practices, and compliance with standards.

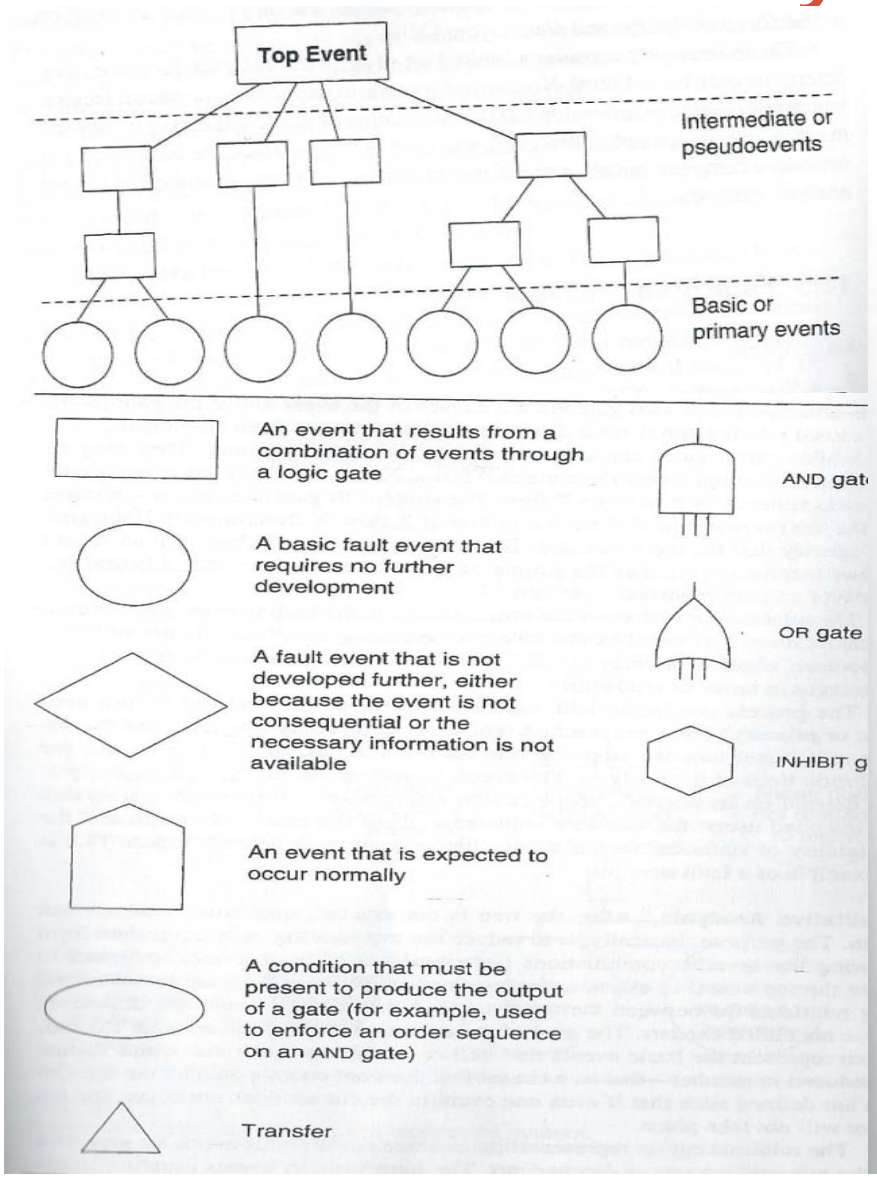
Hazard Indices

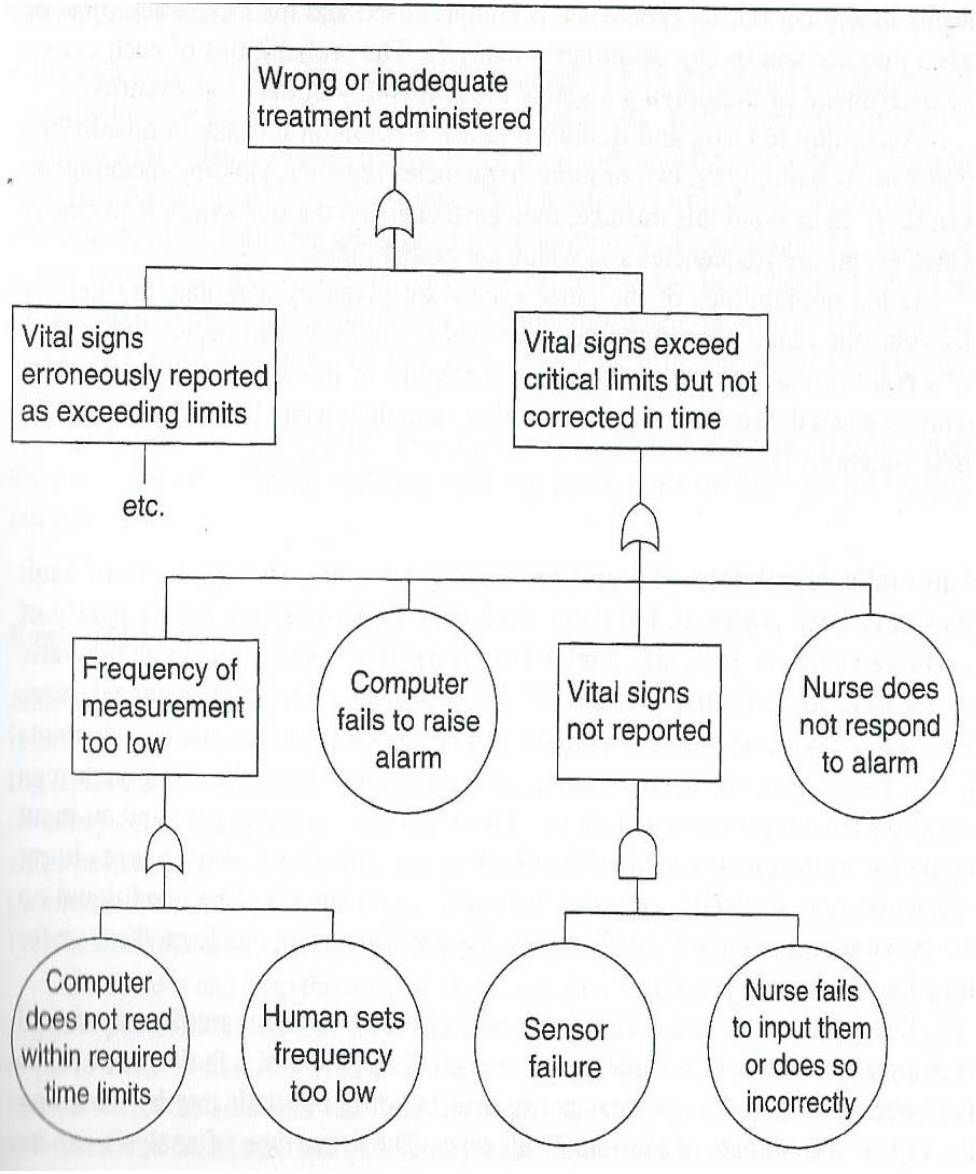
- Description
  - Measure loss potential due to fire, explosion, and chemical reactivity hazards in the process industries.
  - The Dow Chemical Company Fire and Explosion Index Hazard Classification Guide (1964)
- Evaluation
  - Provide a quantitative indication of potential hazards.

Fault Tree Analysis

- Widely used in the aerospace, electronics, and nuclear industries. (launch control system)
- Analyzes causes of hazards, not identifying hazards.
- Boolean logic methods used to describe the combinations first of individual faults
- Hardware Synthesis FTA- A model of hardware, circuit diagram, transfer statements
- Software FTA- looks for loops in the code
- Top down search method through four steps
  - System definition- initial conditions, define top event.
  - Fault tree construction- causal events related to the top event, logic symbols to describe relations.
  - Qualitative analysis- describes relations between top event and the primary events (cuts sets with respect to top event).
  - Quantitative analysis- calculate probability of the outputs of the logical gates.

Fault Tree Analysis





Management Oversight and Risk Analysis

- MORT developed for the U.S Nuclear Regulatory Agency
  - Used for accident investigation, hazard analysis
  - Emphasis on management and human factors
- Assumes accidents are caused by mishandled changes to the system leading to uncontrolled energy
- MORT is a fault tree arranged by
  - Analysis of managerial functions
  - Human behavior
  - Environmental factors
- Yields useful information on planning and coordination of activities (Maintenance team, Design and plan team, Information systems)

Event Tree Analysis

- The FTA is widely used for quantification of system failures, very difficult for complex systems like nuclear power plants.

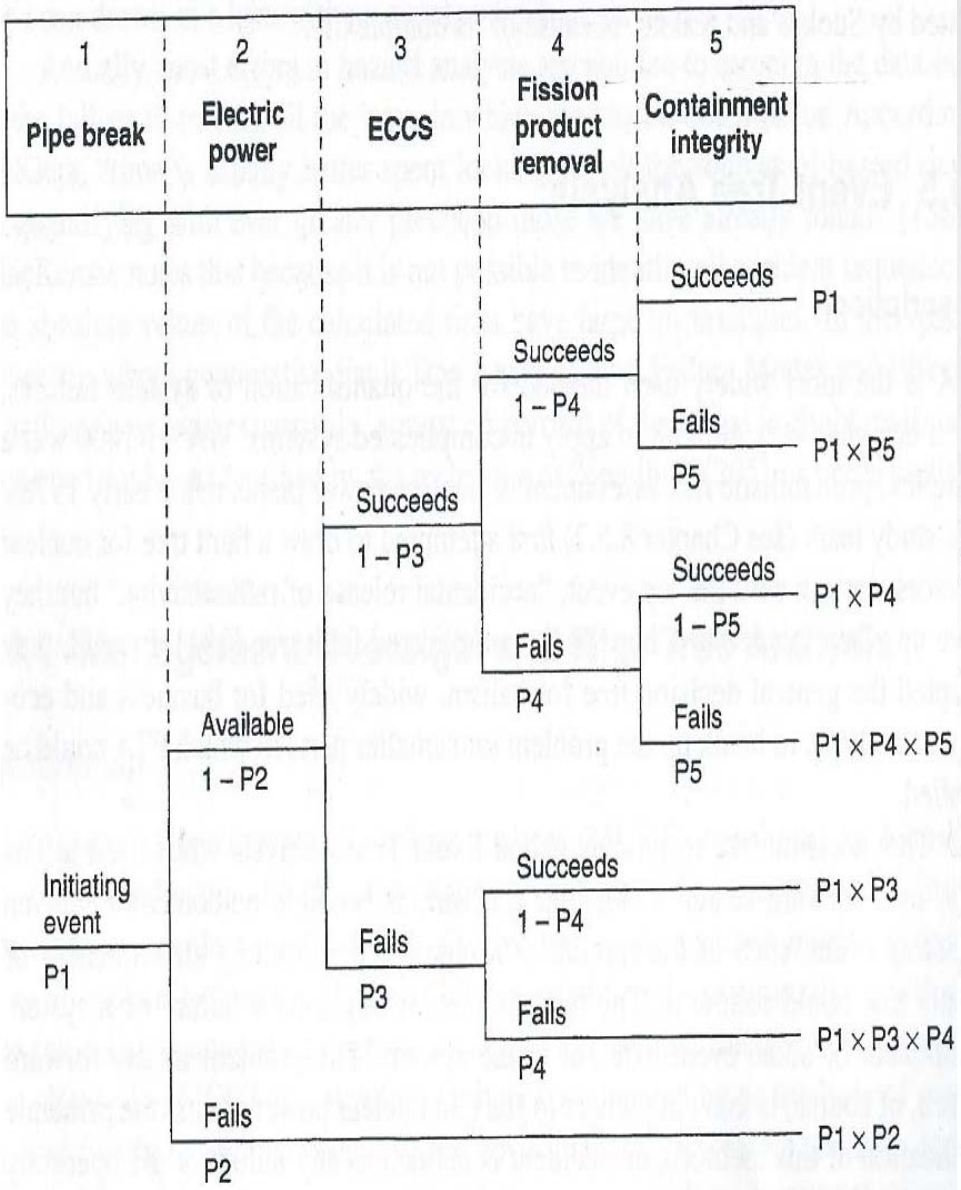
- Event Tree Analysis identify various outcomes of a given initiating event.
  - Sequences of events that follow it

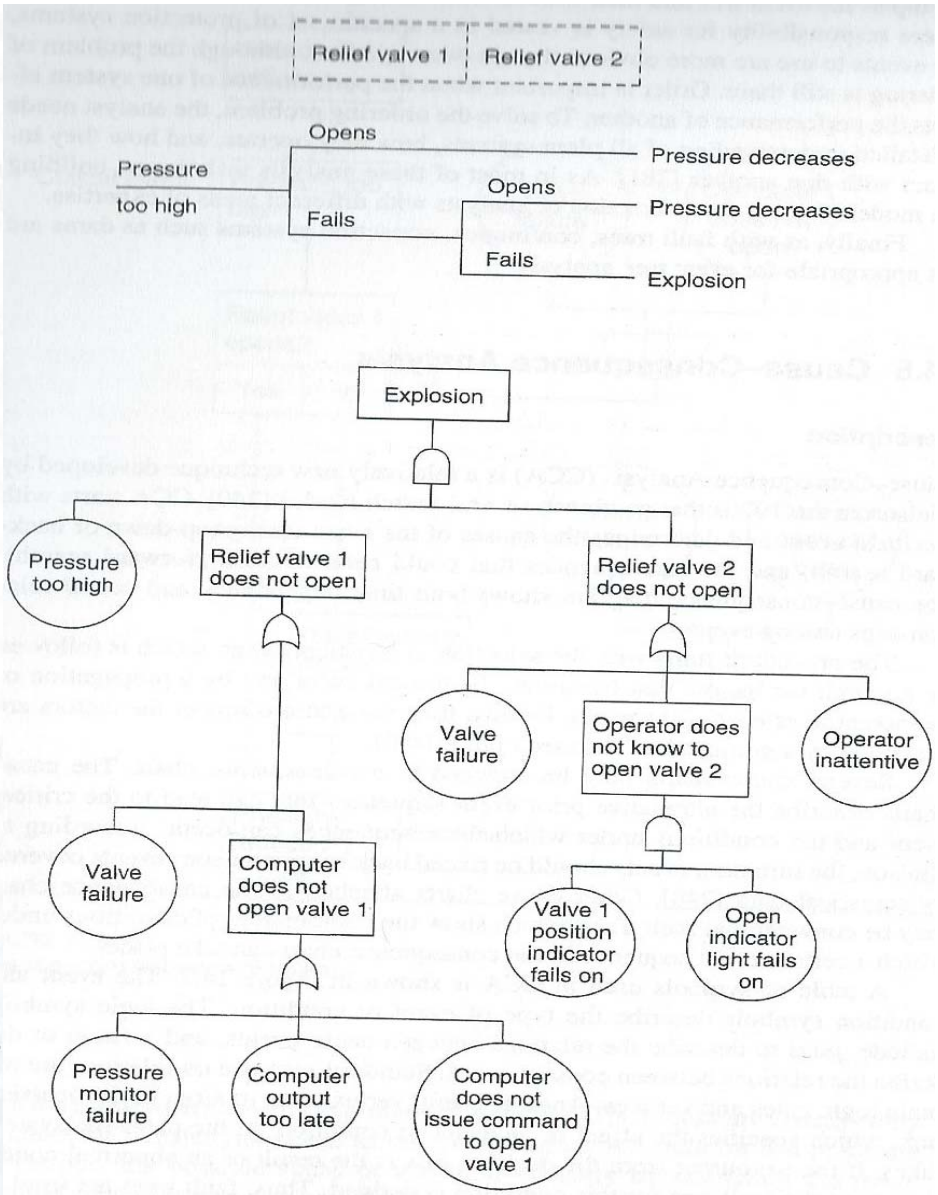
- Helpful for identifying protection system features so steps can be taken to reduce failure probability.
- Identify top event in FTA

- Knowing where to start
  - Potential failures previously identified in the past years of safety analysis.
  - All protection systems that can be used after the accident are defined as heading for event trees
  - Protection functions are left to right (chronological order)
  - Two alternatives: Upper branch successful performance of protection system, Lower branch failure of the protection system

- A paths probability is found by multiplying together the probabilities at various branches of the path
- The total risk of an accident is found by combining the path probabilities for all paths leading to an accident
- Applied through a binary state system (one failure state, one succeed state)

Event Tree Analysis

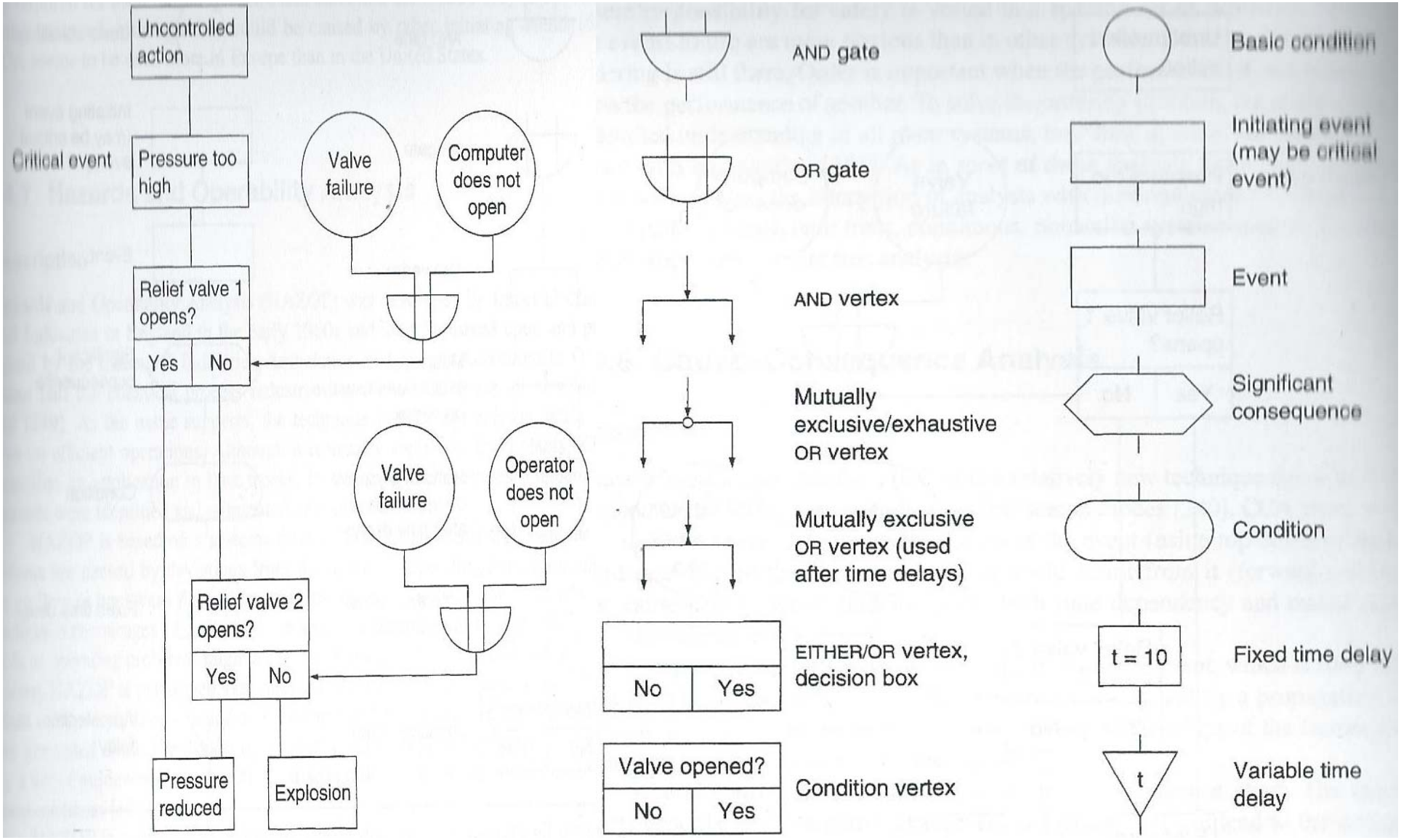




Cause Consequence Analysis

- Made in 1970, CCA starts with a critical event
  - Determines the cause of the event (top down search)
  - Determines the consequence that could result from it (forward search)
  - Allow representation on time delays
- Several cause charts may be attached to a consequence chart
  - Makes diagrams very unwieldy
- Followed by a search for factors that establish the critical events
- Represented by a block diagram (logic gates)

Cause Consequence Analysis



Hazard and Operability Analysis

- HAZOP developed by Imperial Chemical Industries in England 1960
- Based on system theory model
- Focuses on efficient operations and not just safety
  - Assumes that accidents are caused by deviations from the design or operating intentions. (flow)
- Qualitative technique based on guide-words
  - NO OR NOT
  - MORE, LESS
  - AS WELL AS
  - REVERSE
  - LATE

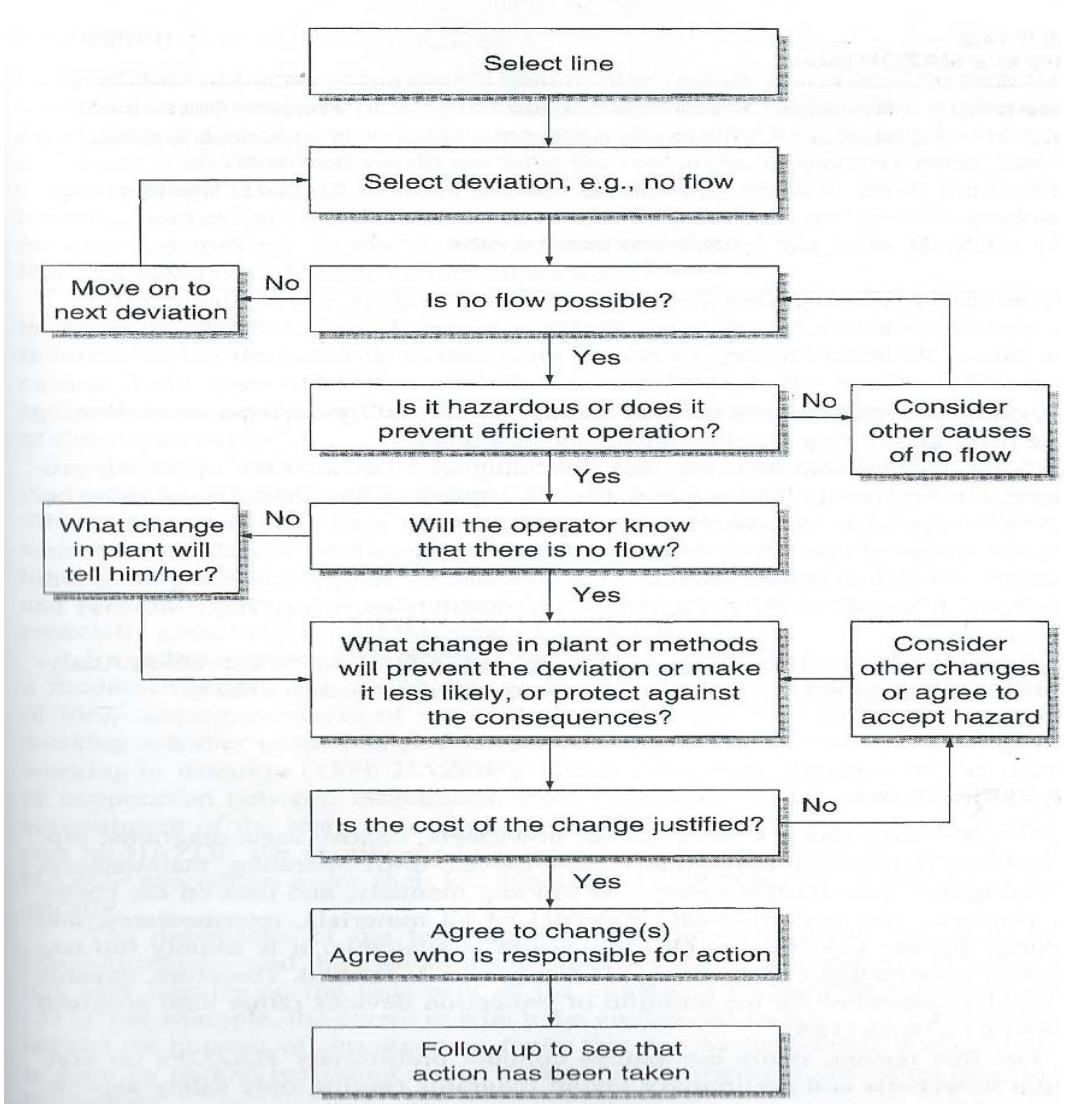
  Parameter

  Flow, pressure, temperature

  HAZOP then is carried out by a team of people, with specific roles for follow-up

Hazard and Operability Analysis

- Yes/No consideration
- Parameter: Flow



Interface Analyses

- Examines the interface between components made, and determines whether a connection provides a path for failure propagation
- Similar to HAZOP
- Include potential foe common mode failure to affect redundant hardware components.

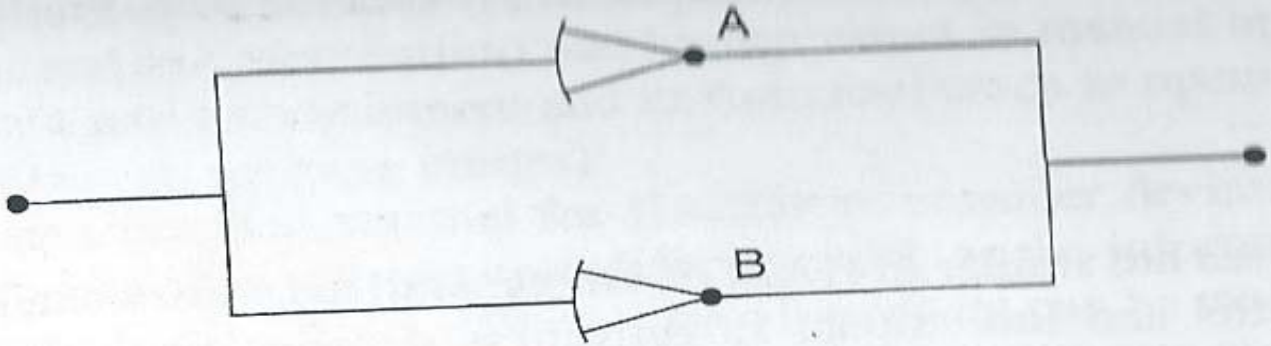
- Ex. No output from a unit or interconnection that goes through the software.

Failure Modes and Effects Analysis

- Initiating events are failures of individual components.
- List all components and their failure modes.
  - The effect on other components or whole system
- Then probabilities and seriousness of each failure mode are calculated.

- Results are documented in a table with column headings
- Great for hardware items, effective for analyzing single unit failures to enhance individual item integrity.

Failure Modes and Effects Analysis



Critical	Failure probability	Failure mode	% failures by mode	Effects	
				Critical	Noncritical
A	1×10^{-3}	Open	90		X
		Short	5	5×10^{-5}	
		Other	5	5×10^{-5}	
B	1×10^{-3}	Open	90		X
		Short	5	5×10^{-5}	
		Other	5	5×10^{-5}	

Failure Modes, Effects, and Criticality Analysis

- More detailed analysis of the criticality of the failure
- Displays description of means of control
- Sometime Critical Items List (CIL) are generated from results.

Failure Modes and Effects Criticality Analysis

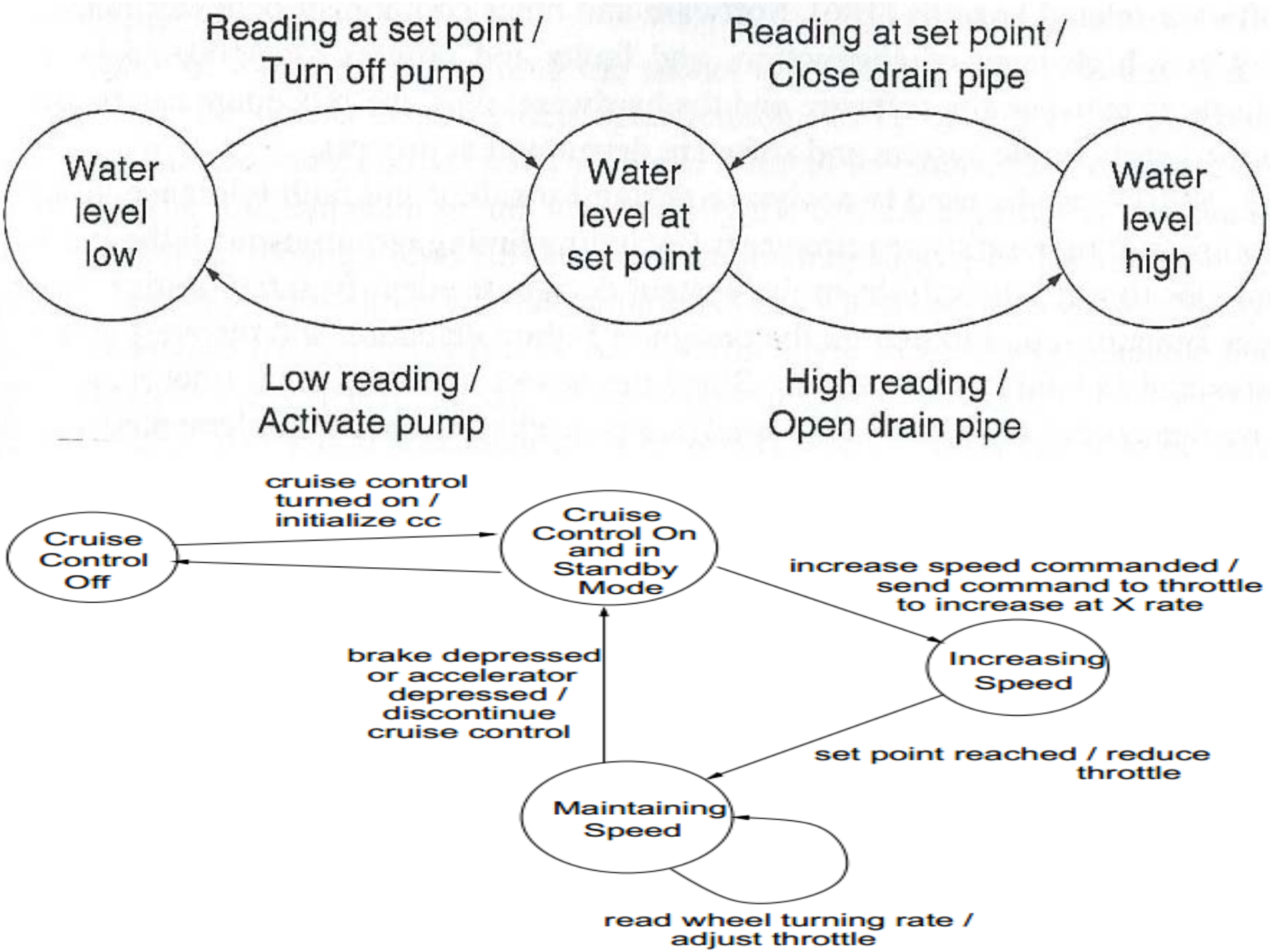
Subsystem _____ Prepared by _____ Date _____

Item	Failure Modes	Cause of Failure	Possible Effects	Prob.	Level	Possible Action to Reduce Failure Rate or Effects
Motor Case	Rupture	a. Poor workmanship b. Defective materials c. Damage during transportation d. Damage during handling e. Overpressurization	Destruction of missile	0.0006	Critical	Close control of manufacturing processes to ensure that workmanship meets prescribed standards. Rigid quality control of basic materials to eliminate defectives. Inspection and pressure testing of completed cases. Provision of suitable packaging to protect motor during transportation.

State Machine Hazard Analysis

- A model of states for a system and the transitions between them
- State machines make a good model for describing and analyzing digital systems and software.
- Check specified software behavior satisfies general software system safety design criteria.
- Have a mathematical basis so can be analyzed and have graphical notations that are easily understandable.
- Requires a model of the component's behavior.

- This approach starts from the initial state of the system
- Generates all possible paths from that state.
- Then determines if any are hazardous conditions that could emerge.


Reading at set point /
Turn off pump
Reading at set point /
Close drain pipe
Water level low
Water level at set point
Water level high
Low reading /
Activate pump
High reading /
Open drain pipe
cruise control turned on / initialize cc
Cruise Control Off
Cruise Control On and in Standby Mode
increase speed commanded / send command to throttle to increase at X rate
Increasing Speed
brake depressed or accelerator depressed / discontinue cruise control
set point reached / reduce throttle
Maintaining Speed
read wheel turning rate / adjust throttle

Task and Human Error Analysis Techniques

- Emphasis on human error rather than equipment failure

- Qualitative Techniques
  - Procedure or Task Analysis- reviews procedures, labels each, recommendations for minimal error result (protective clothing)
  - Operator Task Analysis- operator task is broken down and checked for difficulties
  - Action Error Analysis- includes effect of human malfunction on physical equipment
  - Work Safety Analysis- breaks a task down into a sequence of steps, then examines with respect to a list of consequence (forgetting a work step, performing a step to early or late, unavailability of usual equipment)

- Quantitative Techniques
  - Rely on human judgment to assign error rates to task
  - Technique for Human Error Rate Prediction (THERP) is a technique used in the field of Human reliability Assessment (HRA), for the purposes of evaluating the probability of a human error occurring throughout the completion of a specific task.
  - Human Reliability Analysis (HRA)
    - Task analysis
    - Specific potential error are identified
    - Determine likelihood events
    - Each error is entered on a tree as a binary event
    - Probabilities are assigned to each event

Conclusions

- Given the widespread use of hazard analysis techniques, there is still a small amount of careful evaluation. (criticism)
- Very few software techniques
- Evaluations of Hazard Analysis Techniques

Questions?