Hazard Log Information

- System, subsystem, unit
- Description
- Cause(s)
- Possible effects, effect on system
- Category (hazard level)
- Safety requirements and design constraints
- Corrective or preventative measures, possible safeguards, recommended action
- Operational phase when hazardous
- Responsible group or person for ensuring safeguards provided.
- Tests (verification) to be undertaken to demonstrate safety.
- Other proposed and necessary actions
- Status of hazard resolution process.

System Hazard Analysis

- Builds on PHA as a foundation (expands PHA)
- Considers system as a whole and identifies how

  system operation
  interfaces and interactions between subsystems
  interface and interactions between system and operators
  component failures and normal (correct) behavior

  could contribute to system hazards.
- Refines high−level safety design constraints
- Validates conformance of system design to design constraints
- Traces safety design constraints to individual components. (based on functional decomposition and allocation)

Models

- Provide a means for
  - Understanding phenomena
  - Recording that understanding so can communicate to others
- All models are abstractions
  - Omit assumed irrelevant details
  - Focus on features of phenomenon assumed most relevant
  - Selection process usually arbitrary and dependent on choice of modeler
  - Selection is critical in determining usefulness and accuracy of model

Accident models

- Underlie all attempts to engineer for safety.
- Used to explain how accidents occur.
- Assume common patterns in accidents; not just random events
  - Imposing pattern on accidents influences factors considered in safety analysis
  - Model may act as filter and bias toward considering only some events and conditions

    or

    May force consideration of factors often omitted.

Accident models (2)

- Forms basis for:
  - Investigating and analyzing accidents
  - Preventing accidents
    - Hazard analysis
    - Design for safety
  - Assessing risk (determining whether systems are suitable for use)
  - Performance auditing and defining safety metrics
- So influences causes identified, countermeasures taken, and risk evaluation
- May not be aware using model, but always exists

Chain−of−Events Models

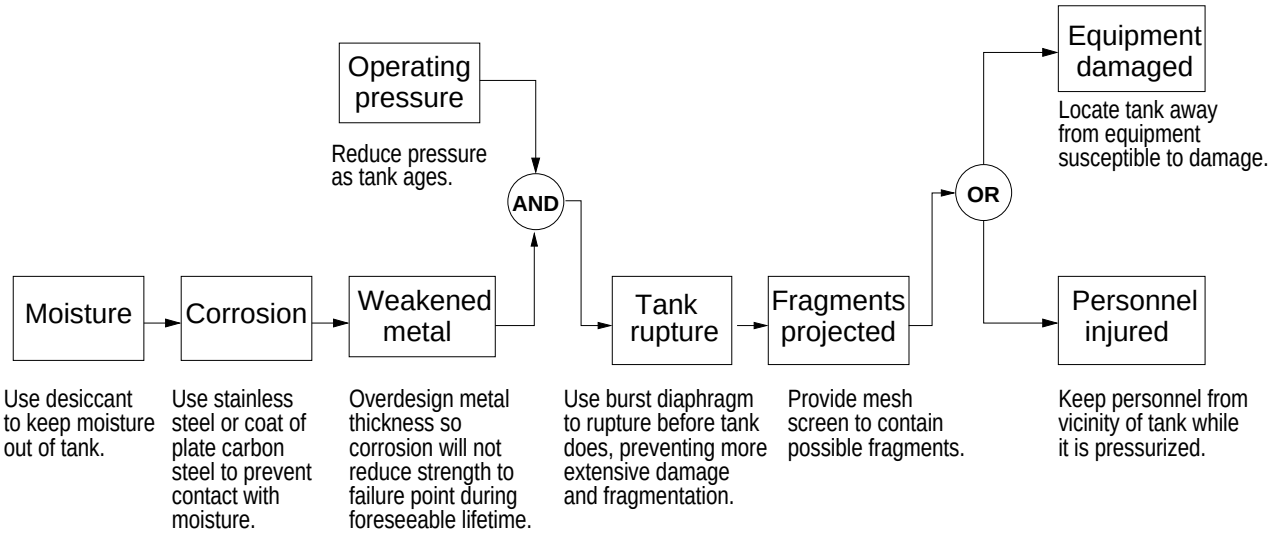
- Explain accidents in terms of multiple events, sequenced as a forward chain over time.
  - Simple, direct relationships between events in chain
  - Contrapositive (if A hadn't occurred, then B would not have)
- Events almost always involve component failure, human error, or energy−related event
- Form the basis of most safety−engineering and reliability engineering analysis:

  e.g., Fault Tree Analysis, Probabilistic Risk Assessment, FMEA, Event Trees

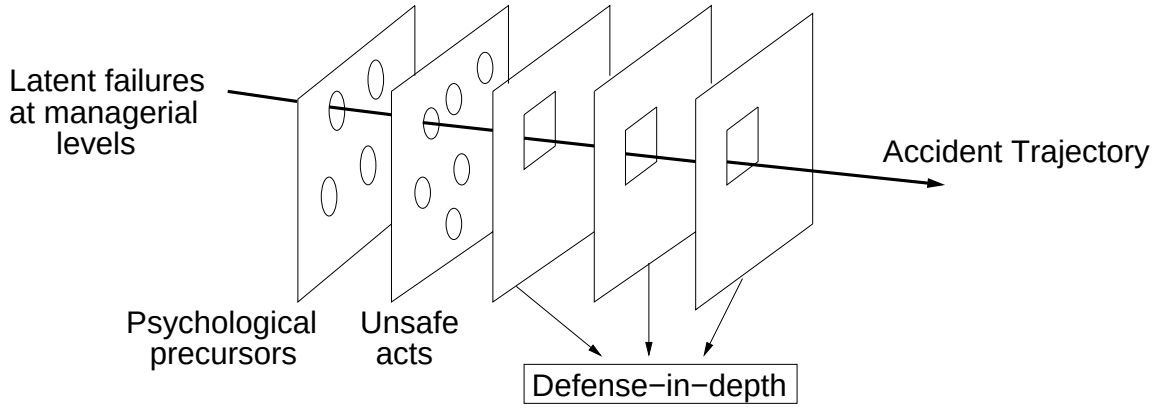
  and design:

  e.g., redundancy, overdesign, safety margins, ...

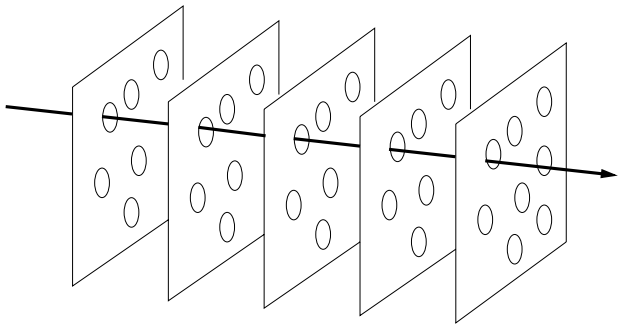
Chain−of−Events Example



Reason's "Swiss Cheese" Model



A variant of the model

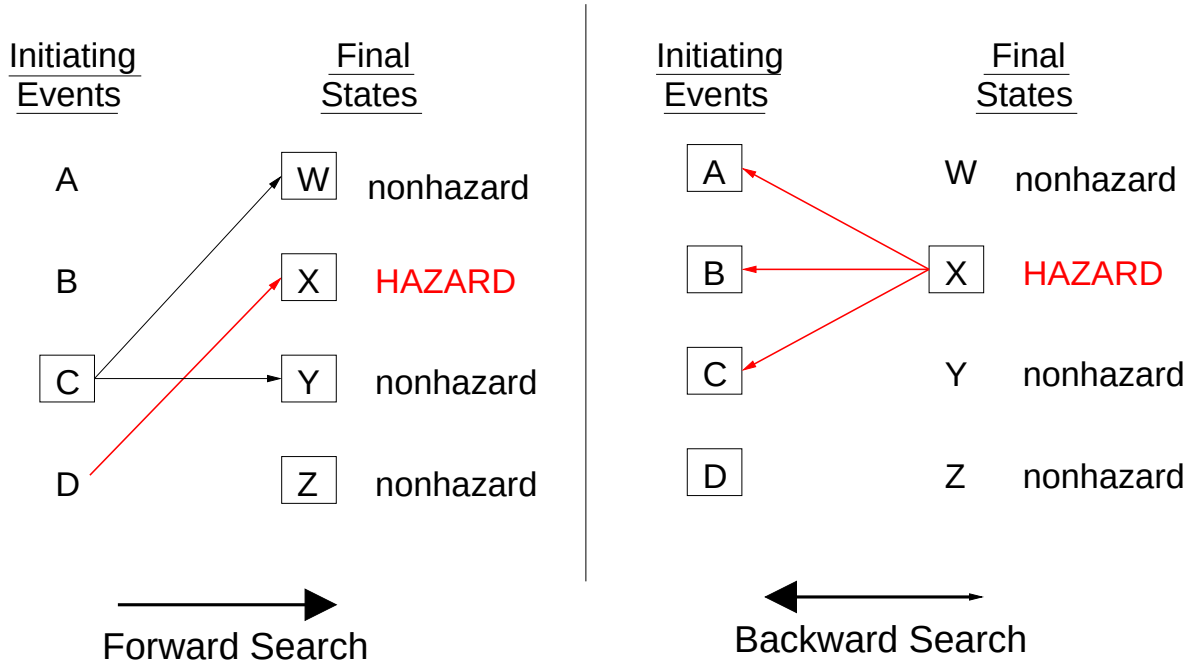


Hazard (Causal) Analysis

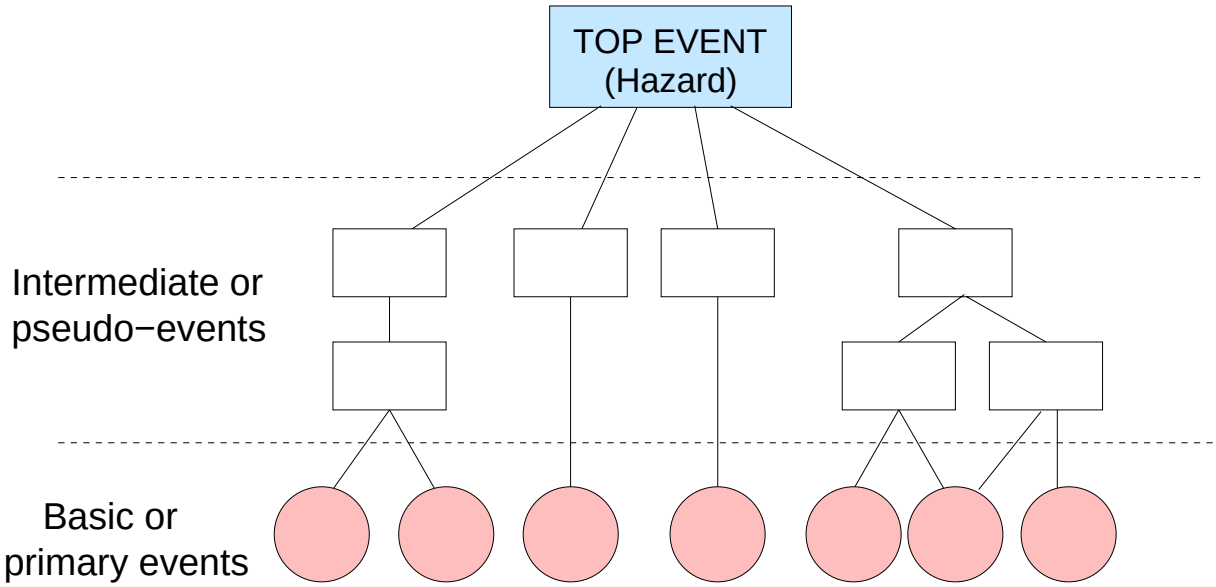
- "Investigating an accident before it happens"
- Requires
  - An accident model
  - A system design model (even if only in head of analyst)
- Almost always involves some type of search through the system design (model) for states or conditions that could lead to system hazards.

  Forward
  Backward
  Top−down
  Bottom−up
- Can be used to refine high−level safety constraints into more detailed constraints.

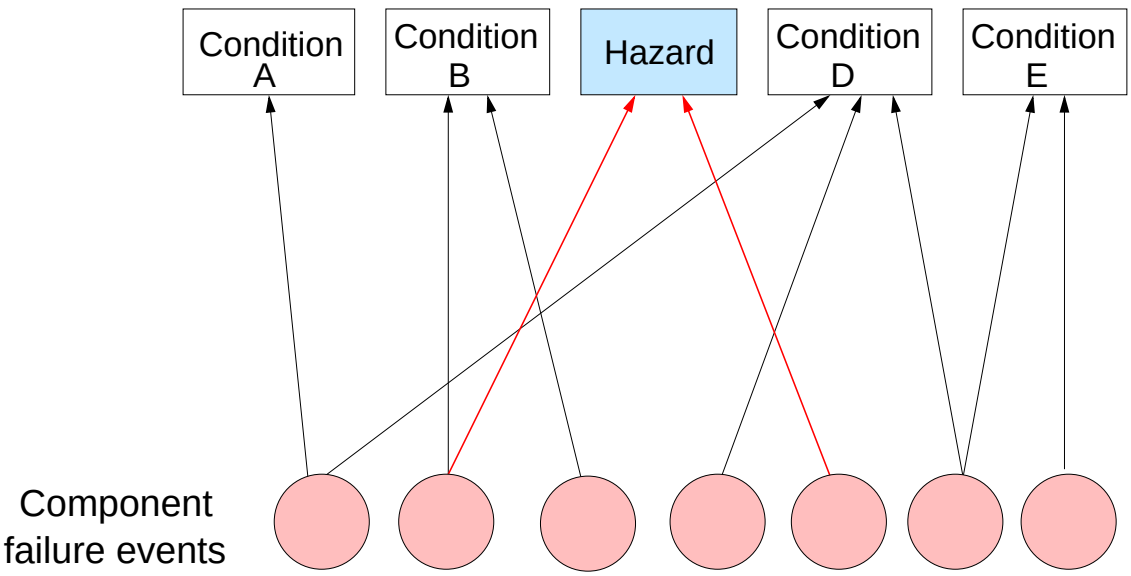
Forward vs. Backward Search



Top−Down



Bottom−Up



Fault Tree Analysis

- Developed originally in 1961 for Minuteman.
- Top−down search method.
- Based on converging chains−of−events accident model.
- Tree is simply a record of results; analysis done in head.
- FT can be written as Boolean expression and simplified to show specific combinations of identified basic events sufficient to cause the undesired top event (hazard).
- If want quantified analysis and individual probabilities for all basic events are known, frequency of top event can be calculated.

Example:

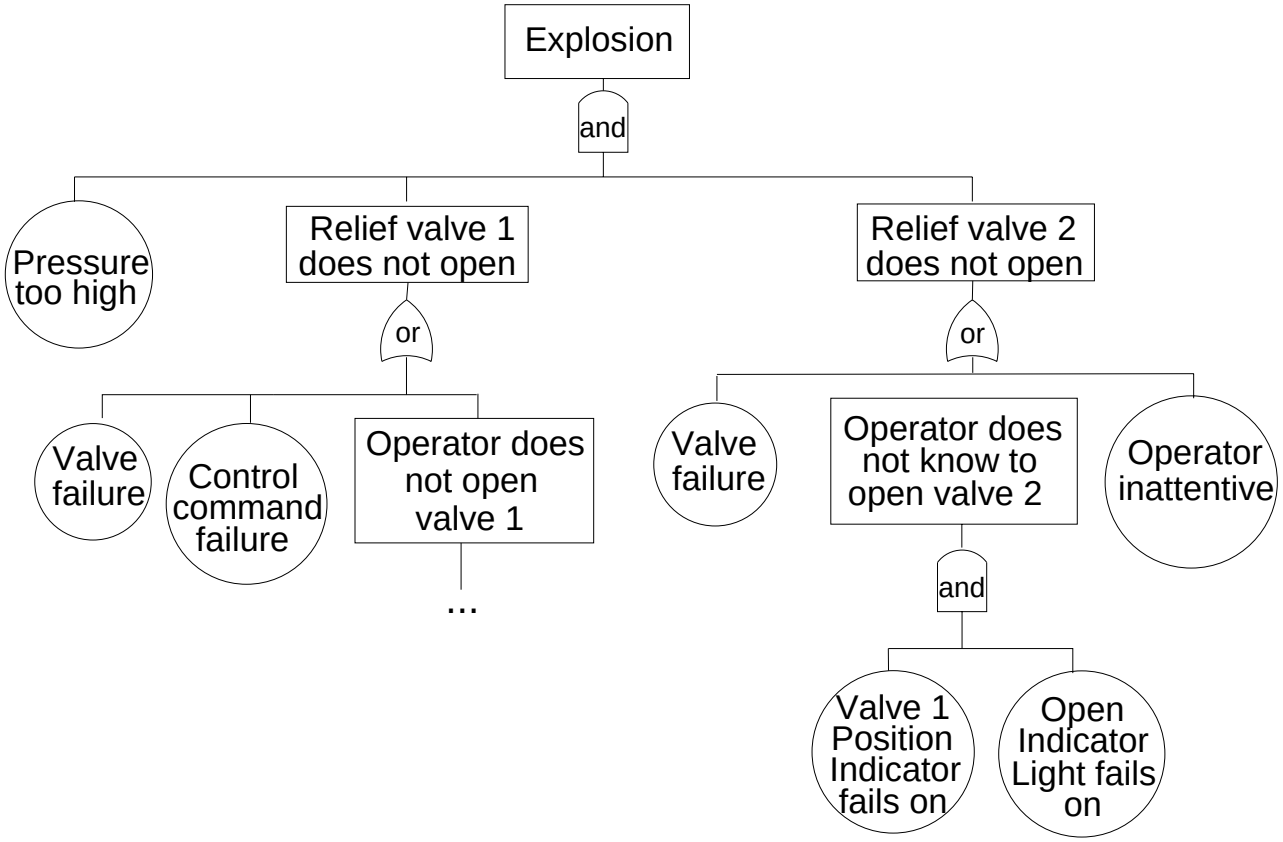
Hazard: Explosion

Design:

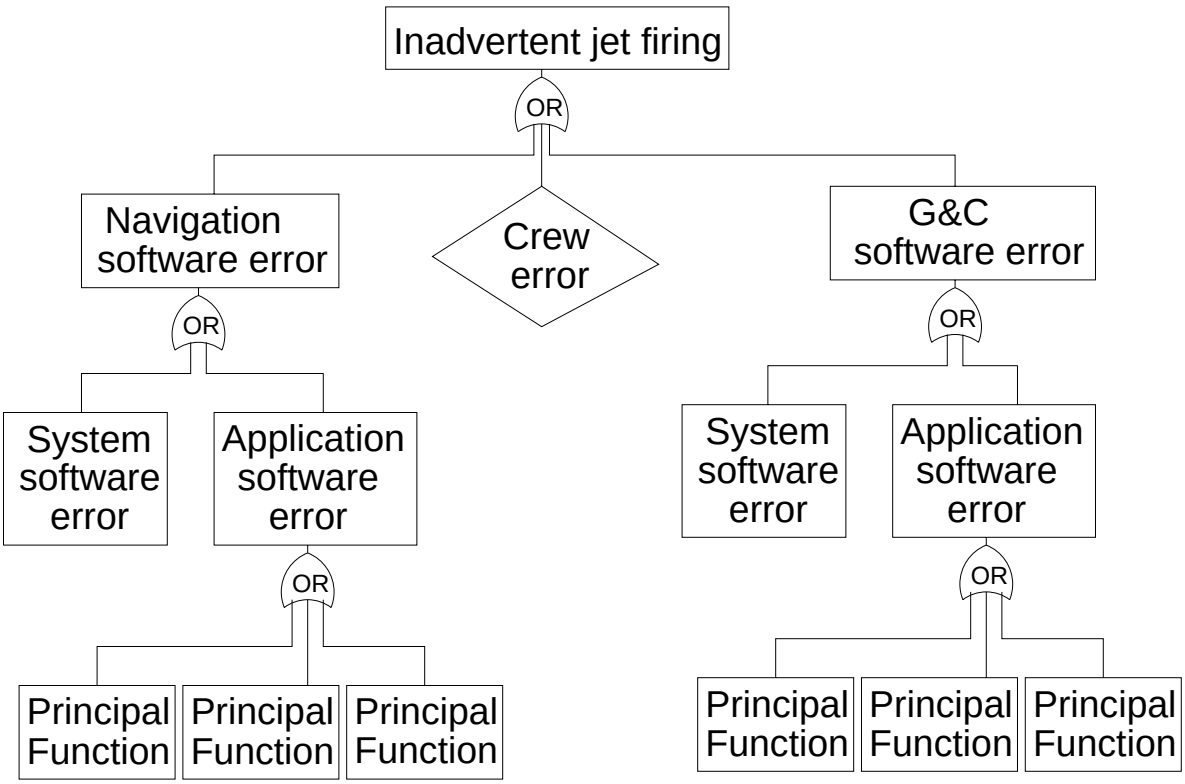
System includes a relief valve opened by an operator to protect against overpressurization. A secondary valve is installed as backup in case the primary valve failed. The operator must know if the first valve does not open so the second valve can be activated.

Operator console contains both a primary valve position indicator light and a primary valve open indicator light.

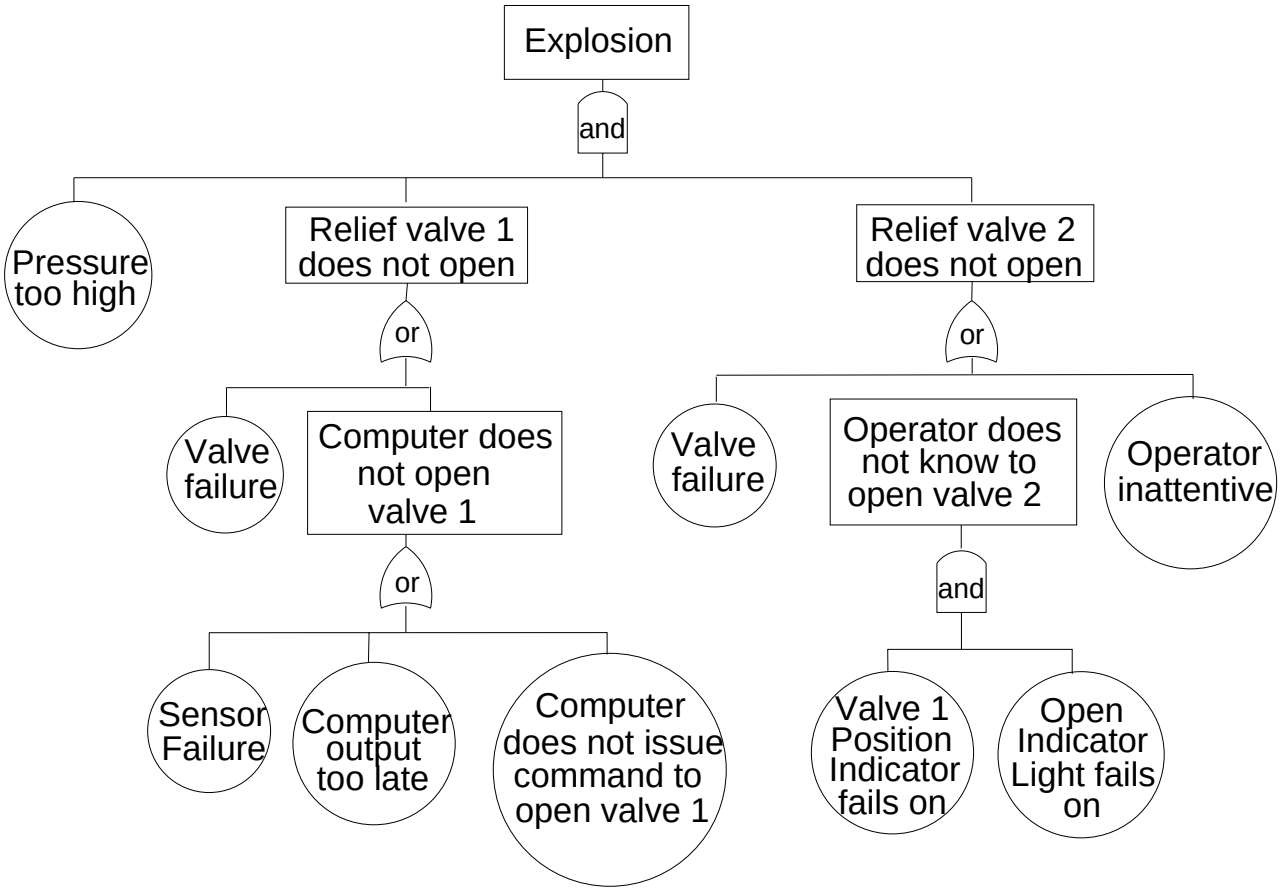
Fault Tree Example



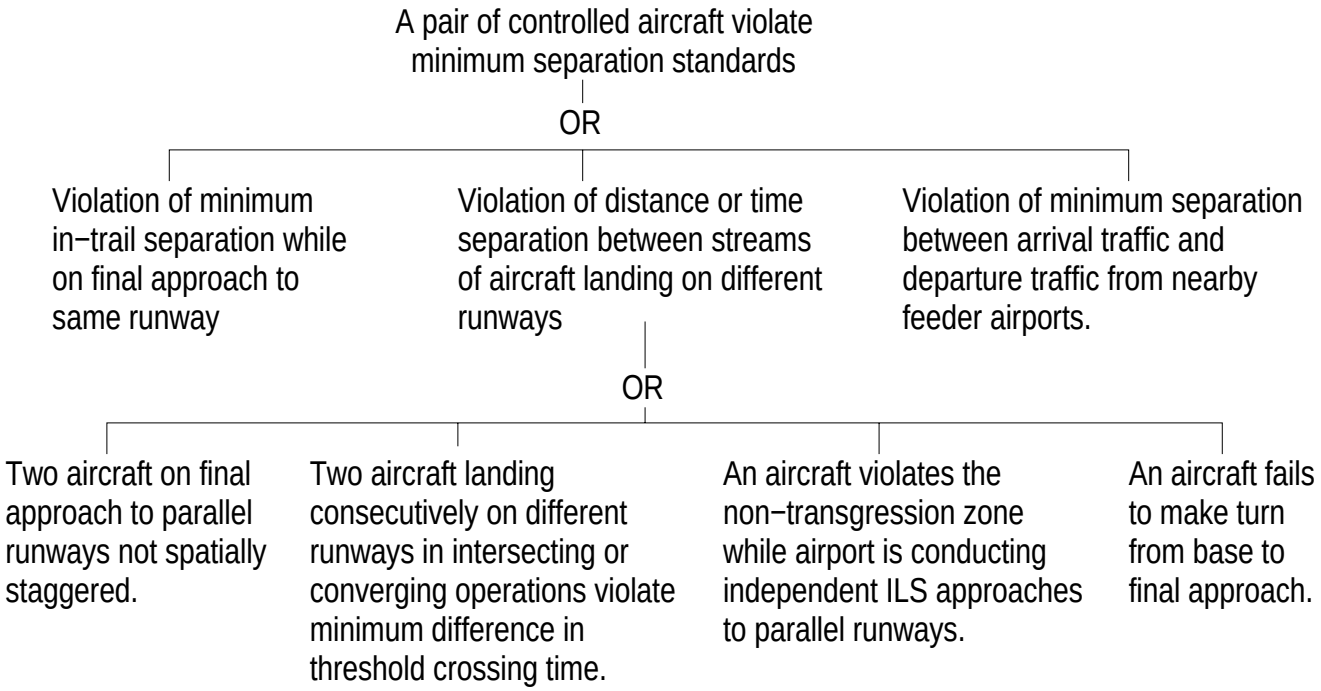
Critical Function: RCS Jet Firing (from NSTS 22254)



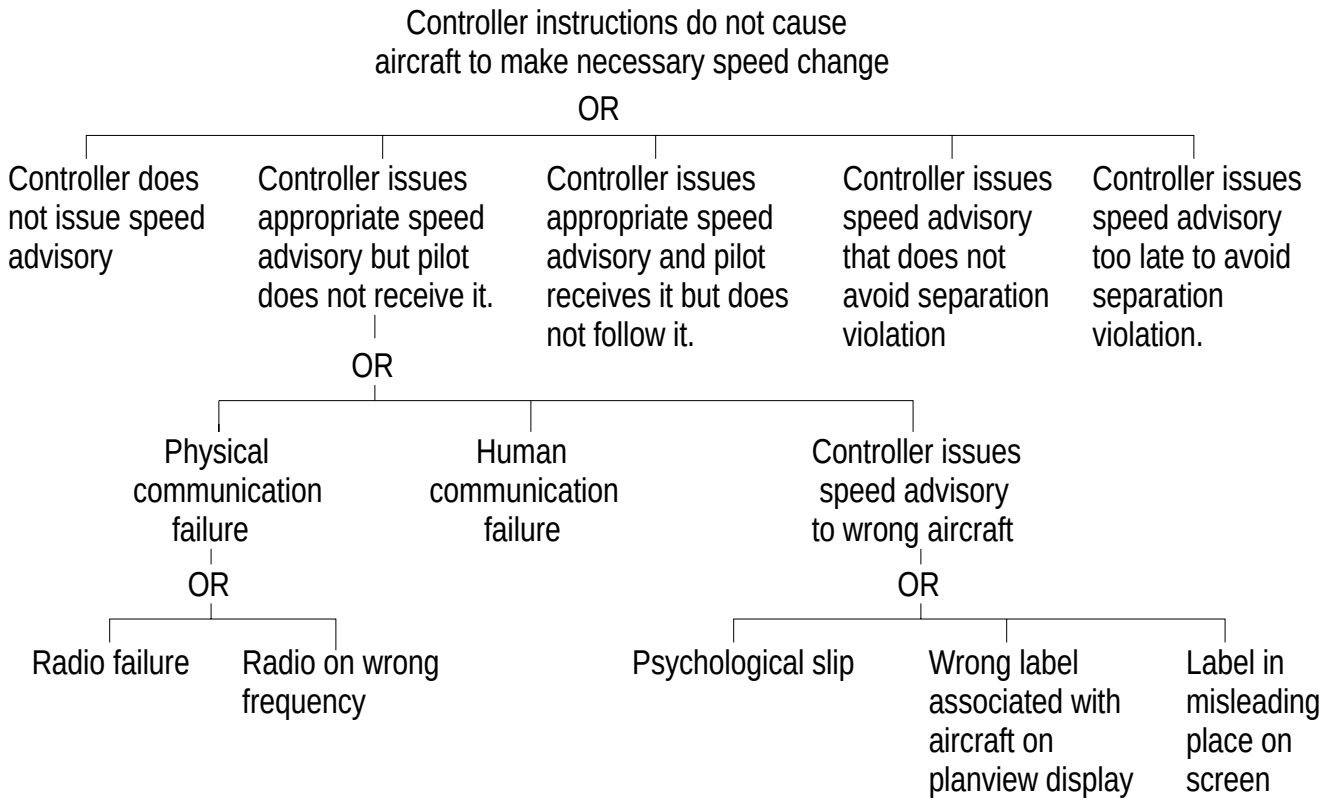
Fault Tree Example



Example Fault Tree for ATC Arrival Traffic



Example Fault Tree for ATC Arrival Traffic (2)



FTA Evaluation

- Graphical format helps in understanding system and relationship between events.
- Can be useful in tracing hazards to software interface and identifying potentially hazardous software behavior.
- Little guidance on deciding what to include
- Tends to concentrate on failures, but does not have to do so
- Quantitative evaluation may be misleading and may lead to accidents.

"On U.S. space programs where FTA (and FMEA) were used, 35% of actual in−flight malfunctions were not identified or were not identified as credible."

See http://sunnyday.mit.edu/nasa−class/follensbee.html
(list of aircraft accidents with risk of 10^{-9} or greater)

Example of unrealistic risk assessment contributing to an accident

System design:

Previous overpressurization example

Events:

The open position indicator light and open indicator light both illuminated. However, the primary valve was NOT open, and the system exploded.

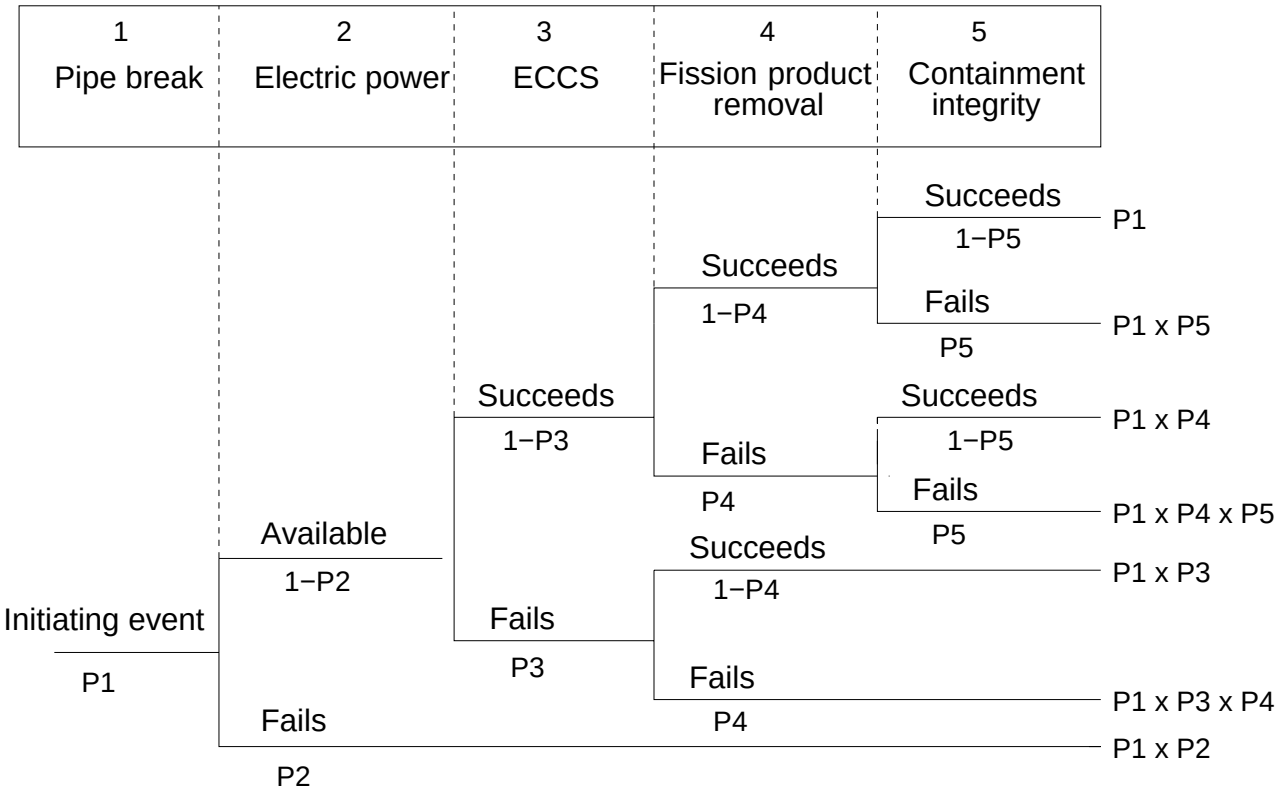
Causal Factors:

Post−accident examination discovered the indicator light circuit was wired to indicate presence of power at the valve, but it did not indicate valve position. Thus, the indicator showed only that the activation button had been pushed, not that the valve had opened. An extensive quantitative safety analysis of this design had assumed a low probability of simultaneous failure for the two relief valves, but ignored the possibility of design error in the electrical wiring; the probability of design error was not quantifiable. No safety evaluation of the electrical wiring was made; instead confidence was established on the basis of the low probability of coincident failure of the two relief valves.

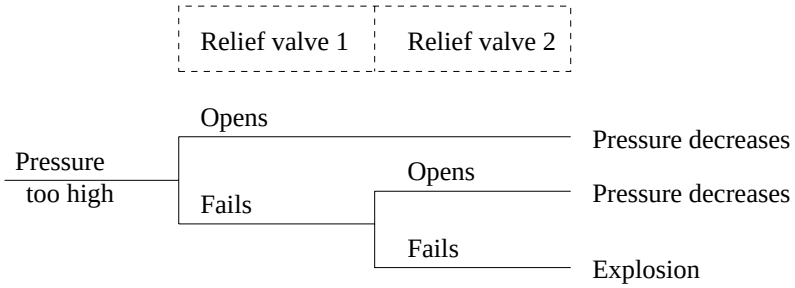
Event Tree Analysis

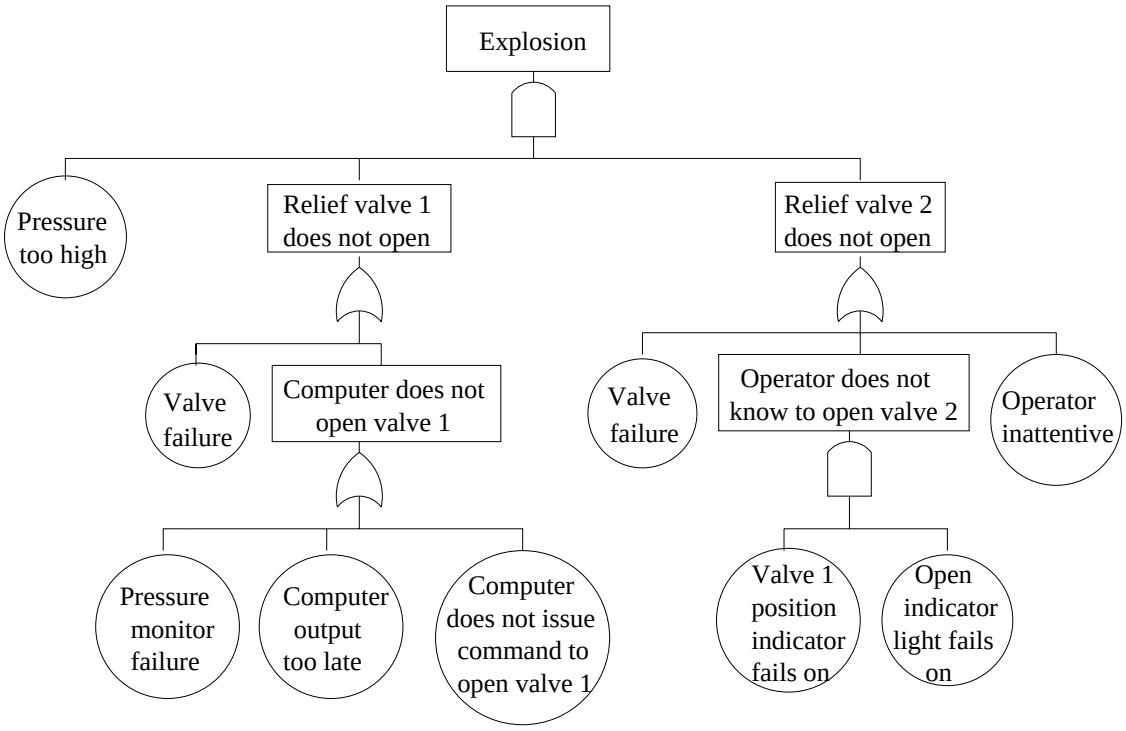
- Developed for and used primarily for nuclear power.
- Underlying single chain of events model of accidents.
- Forward search
- Simply another form of decision tree.
- Problems with dependent events.

Event Tree Example



Event Trees vs. Fault Trees





ETA Evaluation

- Events trees are better at handling ordering of events but fault trees better at identifying and simplifying event scenarios.
- Practical only when events can be ordered in time (chronology of events is stable) and events are independent of each other.
- Most useful when have a protection system.
- Can become exceedingly complex and require simplication.

ETA Evaluation (2)

- Separate tree required for each initiating event.
  - Difficult to represent interactions between events
  - Difficult to consider effects of multiple initiating events.
- Defining functions across top of event tree and their order is difficult.
- Depends on being able to define set of initiating events that will produce all important accident sequences.

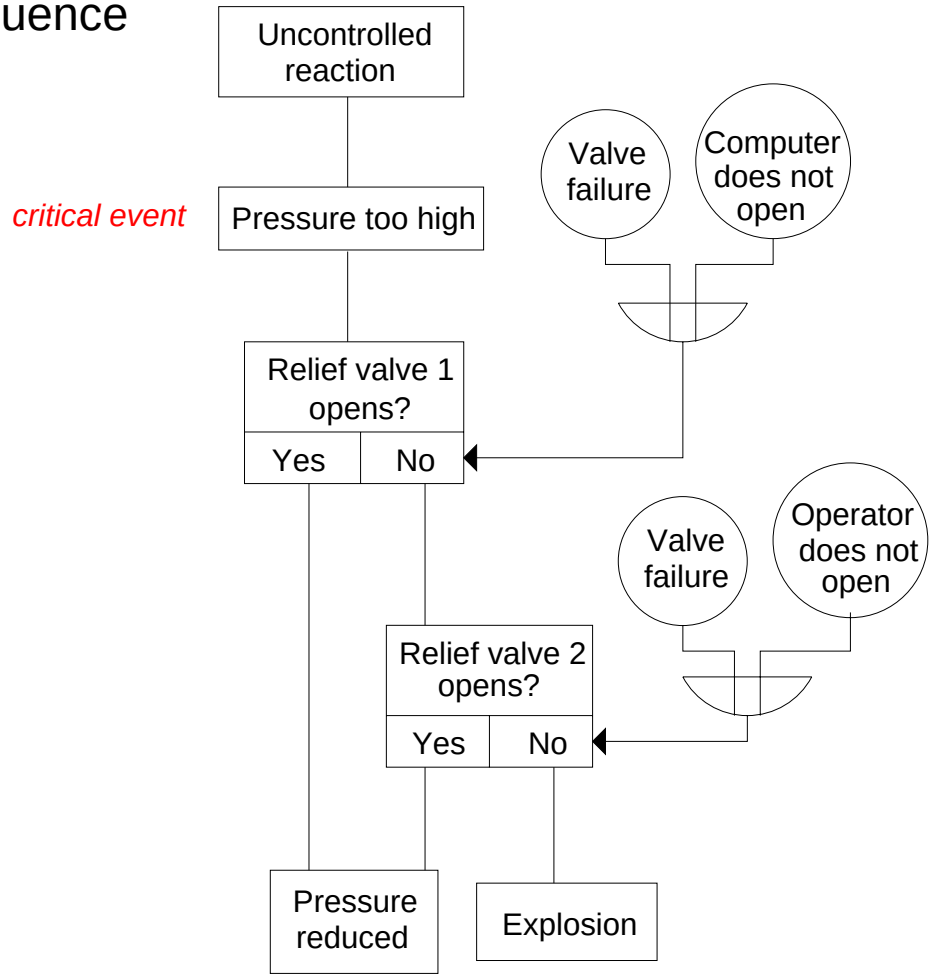
  Probably most useful in nuclear power plants where
  - all risk associated with one hazard (overheating of fuel)
  - designs are fairly standard
  - large reliance on protection systems and shutdown systems.

Cause–Consequence Analysis

- Used primarily in Europe.
- A combination of forward and top–down search.

  Basically a fault tree and event tree attached to each other
- Again based on converging chain–of–events.
- Diagrams can become unwieldy.
- Separate diagrams required for each initiating event.

Cause–Consequence Diagram



FMEA or FMECA

Failure Modes and Effects (Criticality) Analysis

- Developed to predict equipment reliability.
- Forward search based on underlying single chain−of−events and failure models (like event trees).
- Initiating events are failures of individual components.

HAZOP: Hazard and Operability Analysis

- Based on model of accidents that assumes they are caused by deviations from design or operating intentions.
- Purpose is to identify all possible deviations from the design's expected operation and all hazards associated with these deviations.
- Unlike other techniques, works on a concrete model of plant (e.g., piping and wiring diagram).
- Applies a set of guidewords to the plant diagram.

HAZOP Guidewords

Guideword	*Meaning*
NO, NOT, NONE	The intended result is not achieved, but nothing else happens (such as no forward flow when there should be)
MORE	More of any relevant physical property than there should be (such as higher pressure, higher temperature, higher flow, or higher viscosity).
LESS	Less of a relevant physical property than there should be.
AS WELL AS	An activity occurs in addition to what was intended, or more components are present in the system than there should be (such as extra vapors or solids or impurities, including air, water, acids, corrosive products).
PART OF	Only some of the design intentions are achieved (such as only one of two components in a mixture).
REVERSE	The logical opposite of what was intended occurs (such as backflow instead of forward flow).
OTHER THAN	No part of the intended result is achieved, and something completely different happens (such as the flow of the wrong material).

Example Entry in a HAZOP report

Guide Word	*Deviation*	*Possible Causes*	*Possible Consequences*
NONE	No flow	1. Pump failure 2. Pump suction filter blocked 3. Pump isolation valve closed.	1. Overheating in heat exchanger. 2. Loss of feed to reactor.

Task and Human Error Analyses

- Qualitative Techniques
  - Break down tasks into a sequence of steps.
  - Investigate potential deviations and their consequences.

- Quantitative Techniques
  - Assign probabilities for various types of human error.
  - Most effective in simple systems where tasks routine.
  - Not effective for cognitively complex tasks operators often asked to perform today.