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

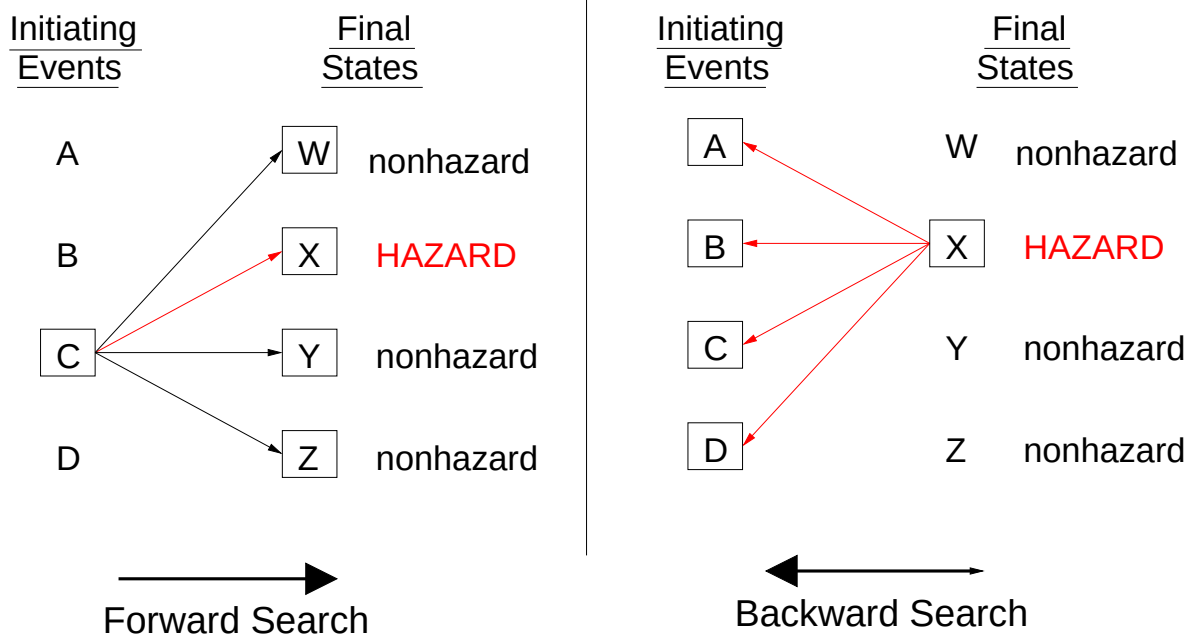
  could contribute to system hazards.
- Refines high−level safety design constraints
- Validates conformance of system design to design constraints
- Traces safety design constraints to individual components. (based on functional decomposition and allocation)

Hazard Causal Analysis

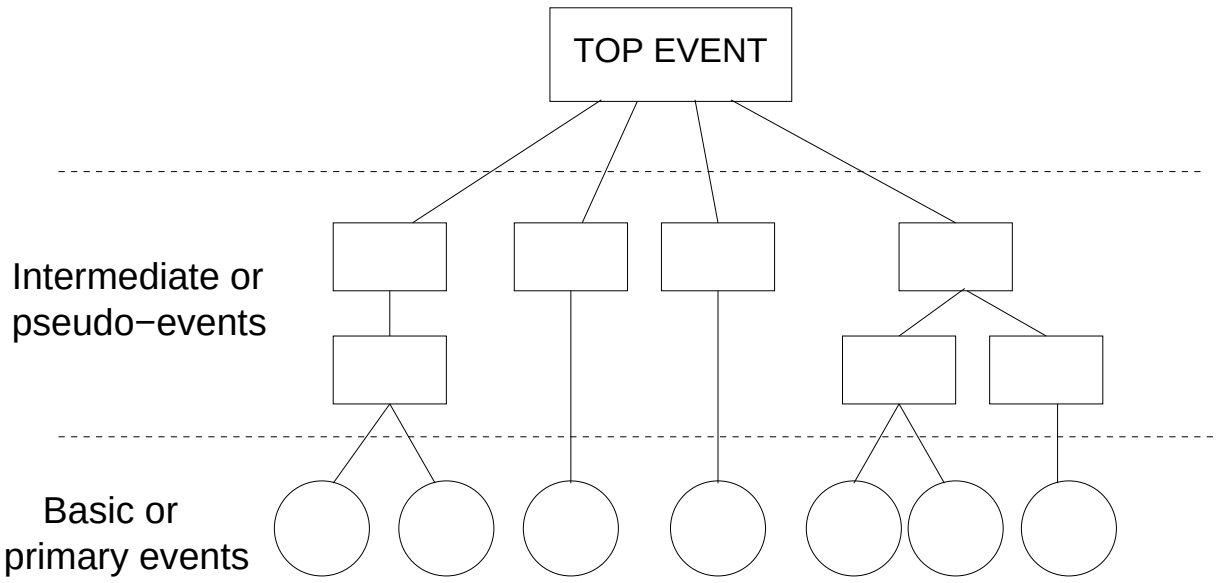
- Used to refine the high−level safety constraints into more detailed constraints.
- Requires some type of model (even if only in head of analyst)
- Almost always involves some type of search through the system design (model) for states or conditions that could lead to system hazards.

  Top−down
  Bottom−up
  Forward
  Backward

Forward vs. Backward Search



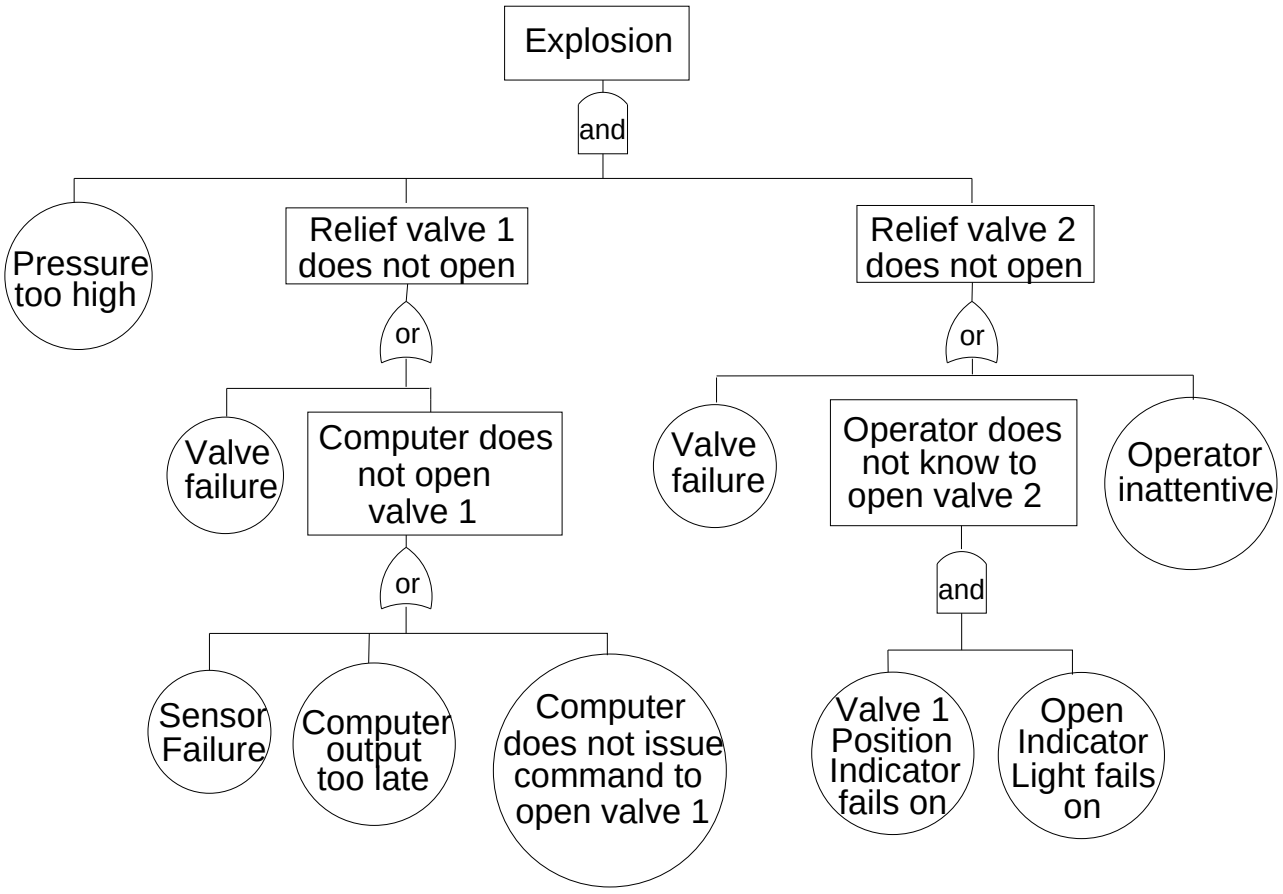
Top−Down Search



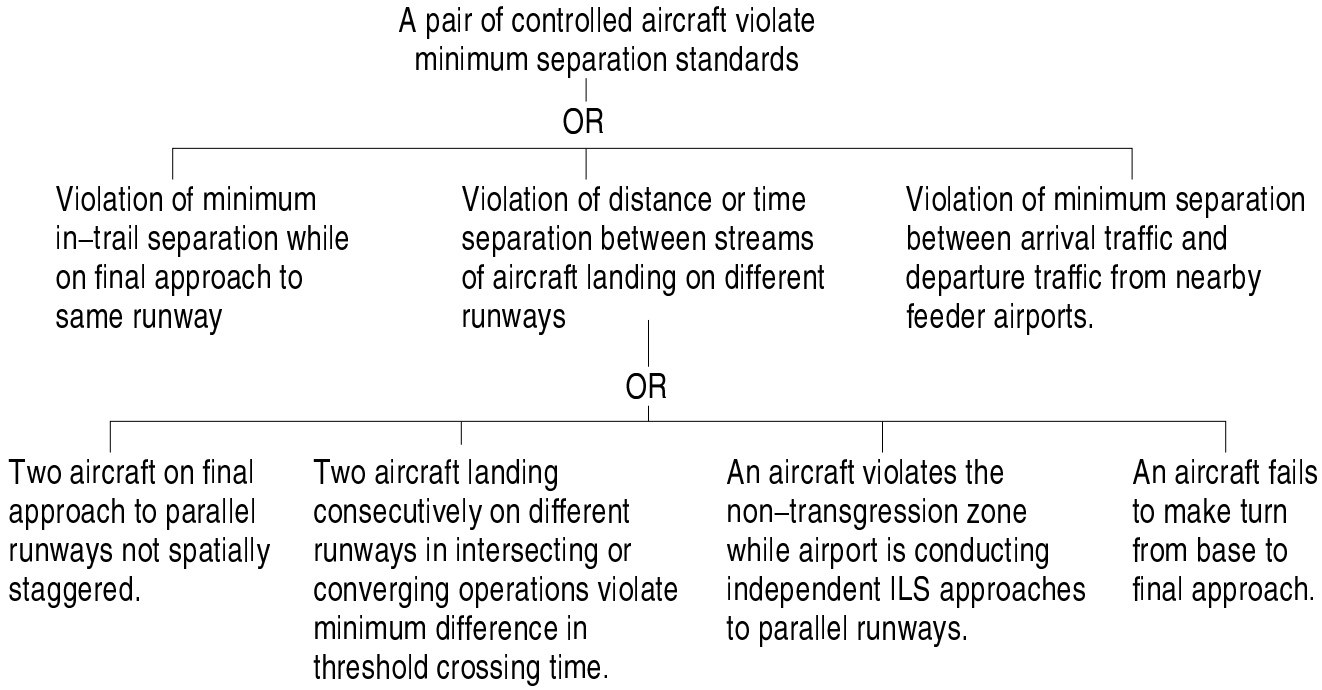
Fault Tree Analysis

- Developed originally in 1961 for Minuteman.
- Means of analyzing hazards, not identifying them.
- 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.

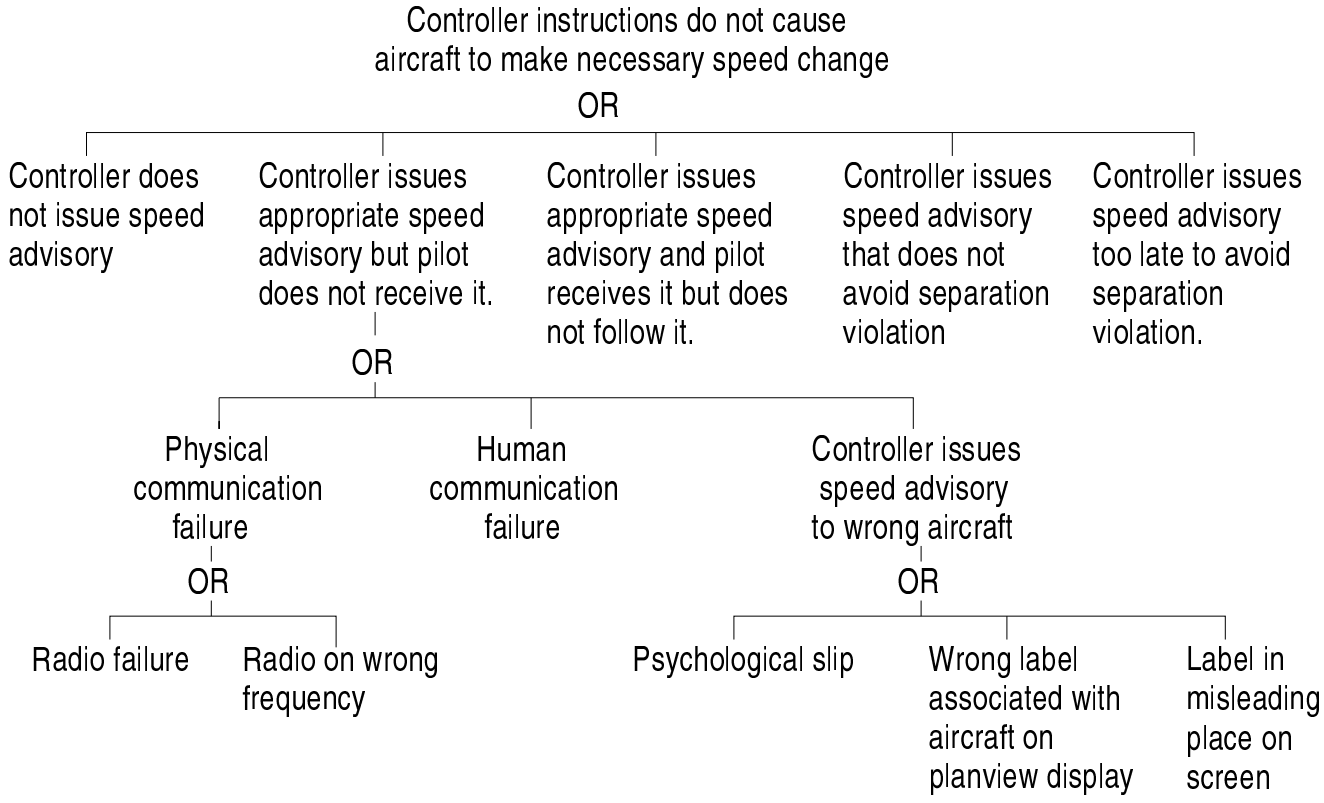
Fault Tree Example



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.
- Cuts sets denote weak points of a complex design.
- Dependencies (common−cause failure points) not easy to see.
- Requires a detailed knowledge of design, construction, and operation of system.

FTA Evaluation (2)

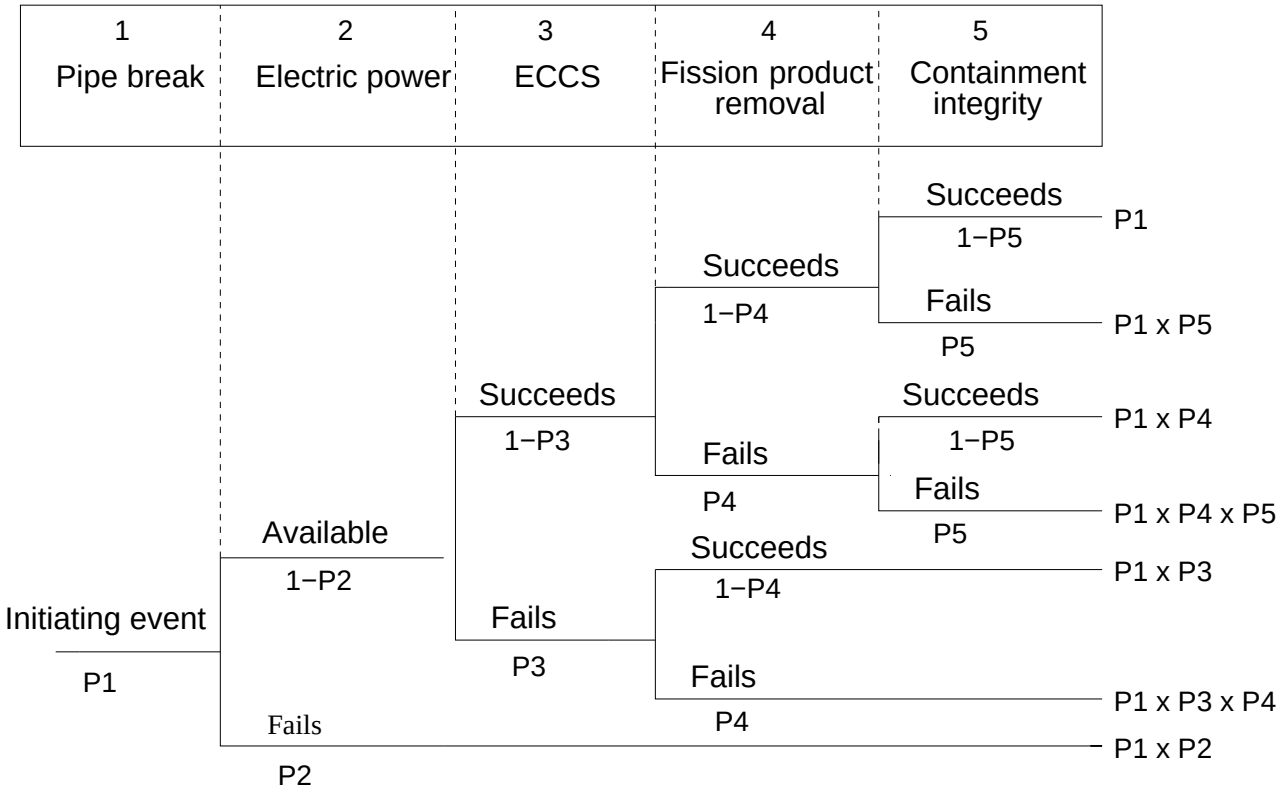
- A simplified representation of a complex process— sometimes too simplified.
- Tends to concentrate on failures.
- Quantitative evaluation may be misleading.

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

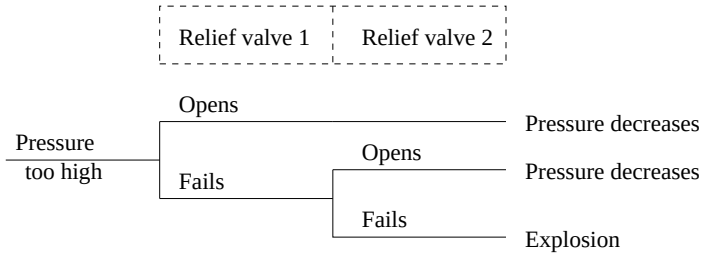
Event Tree Analysis

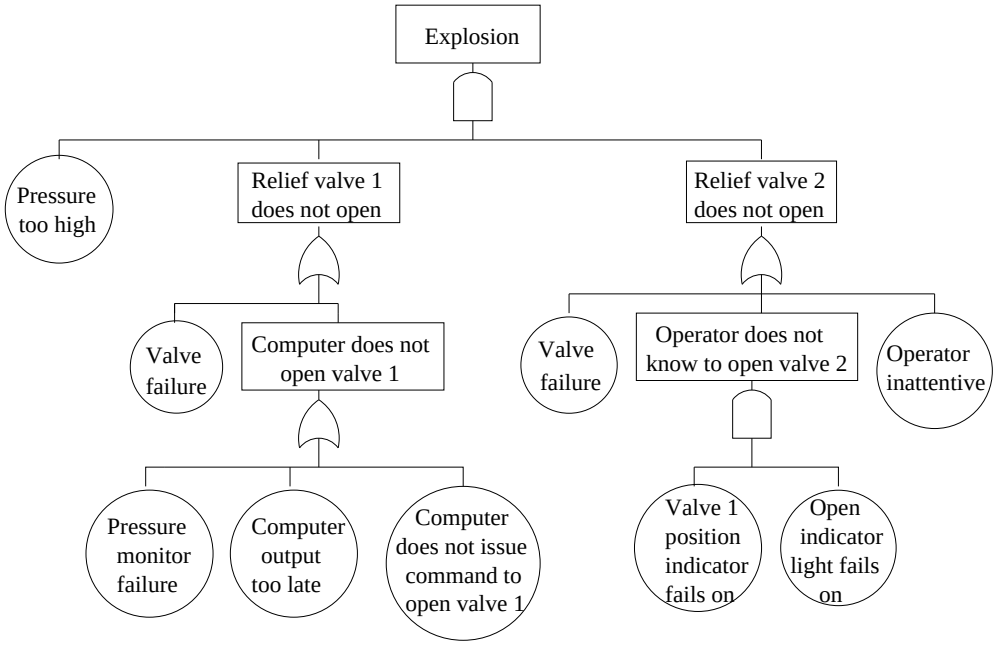
- Developed for and used primarily for nuclear power.
- Underlying single chain of events model of accidents.
- Forward search
- Simply another form of decision tree.
- Problems with dependent events.

Event Tree Example



Event Trees vs. Fault Trees





ETA Evaluation

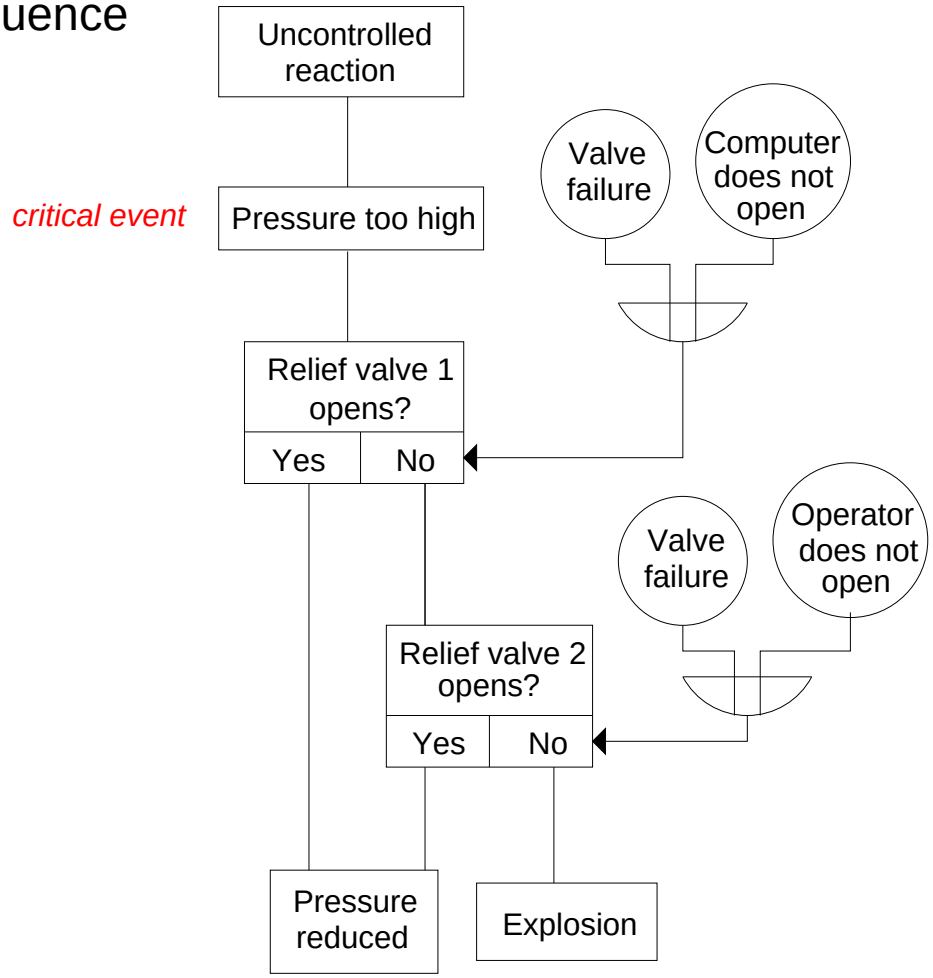
- Events trees are better at handling ordering of events but fault trees better at identifying and simplifying event scenarios.
- Practical only when events can be ordered in time (chronology of events is stable) and events are independent of each other.
- Most useful when have a protection system.
- Can become exceedingly complex and require simplication.
- 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 (serious 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.
- Again based on converging chain−of−events.
- Diagrams can become unwieldy.
- Separate diagrams required for each initiating event.

Cause−Consequence Diagram



HAZOP: Hazard and Operability Analysis

- Unlike most techniques, HAZOP can identify hazards.
- 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.
- Software Deviation Analysis (Jon Reese)

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.

Interface Analyses

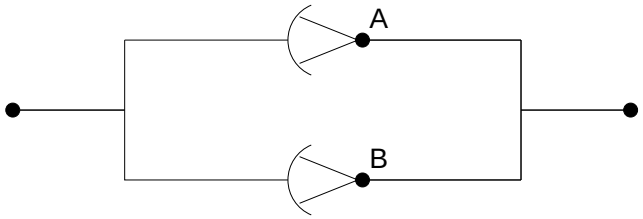
- Various types used to evaluate physical, functional, or flow relationships.
- Generally use structured walkthroughs.
- Like HAZOP, effectiveness depends on procedures used and thoroughness of application.

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.

FMECA Example (1)



Component	Failure probability	Failure mode	% failures by mode	Effects	
				Critical	Noncritical
A	$1x10^{-3}$	Open	90		X
		Short	5	$5x10^{-5}$	
		Other	5	$5x10^{-5}$	
B	$1x10^{-3}$	Open	90		X
		Short	5	$5x10^{-5}$	
		Other	5	$5x10^{-5}$	

FMECA Example (2)

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.

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: