Techniques for Safety Assessment

Introduction

hazard: condition that has potentially harmful consequences (for people or environment)

accident: hazard, that results in harmful consequences

accidental event: event, that leads up to an accident

incident, near accident, near miss: an event, that could be an accident, but nothing bad happened

severity: impact of possible hazard

risk: severity and possibility

Hazard Analysis

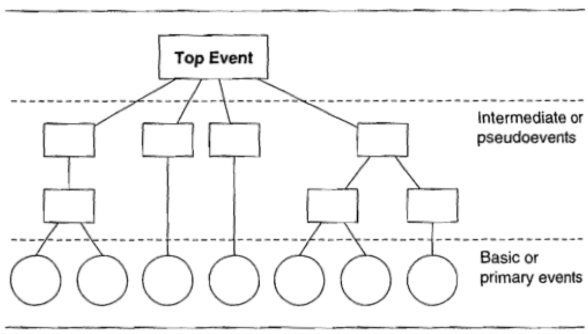
- collection of different techniques

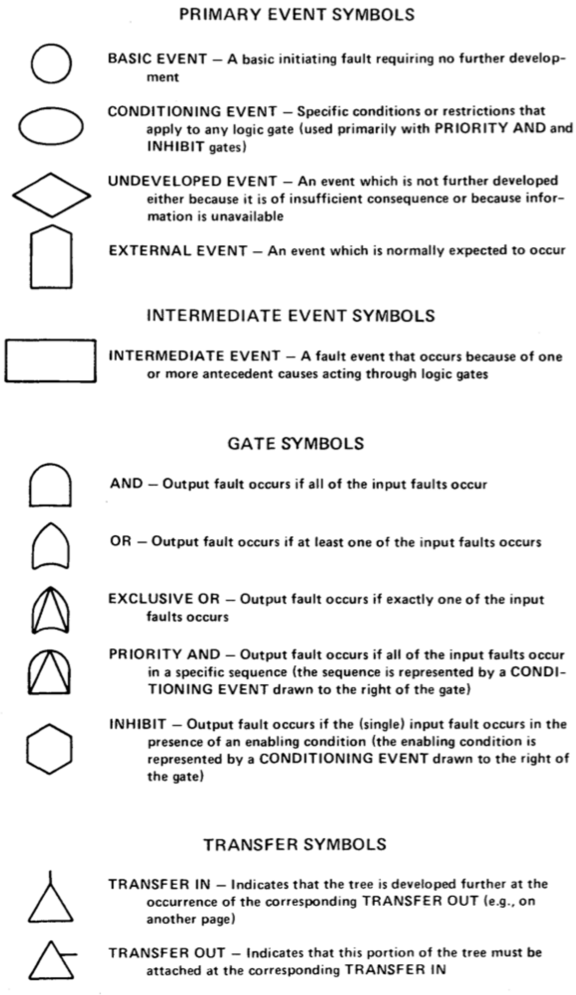
  inductive start by considering the initiating causes of given hazard, trace them forward through event propagation to corresponding safety consequences ⇒Failure Mode Effects Analysis

  deductive consider unintended behavior of system, trace it backward to corresponding causes ⇒Fault Tree Analysis (FTA)

Fault Tree Analysis (FTA)

- used in all fields of safety engineering
- deductive analytical technique
- *top-level event* (TLE) is specified and the system is analyzed for possible chain of *basic events*, that may cause the TLE
- analyze cause of hazard, not find hazards
- typical representation is a *fault tree* (FT), makes use of logical gates (AND, OR)





AND both events are required to occur

OR alternate causes

inhibit, NOT less common

basic events leafs (depicted by a circle)

intermediate events nodes between leafs and root (depicted by a square)

undeveloped event not further analyzed, because not important (depicted by a diamond)

an event needs to be developed considering *immediate*, *necessary* and *sufficient* results

elementary faults ⇒basic events

transfer symbols may link different parts of tree

inhibit gates, conditioning events can be used to constrain the ways that faults are propagated inside FT

dynamic gates like *priority AND* ⇒temporal constraints

- fault tree can be shown as tree, formula or truth table
  tree is most readable
- important notations:

  scope & boundary define, which parts of the system will be included in the analysis & under which hypothesis/ operational constraints the system will be analyzed

  boundary initial state of system, and assumptions about environment

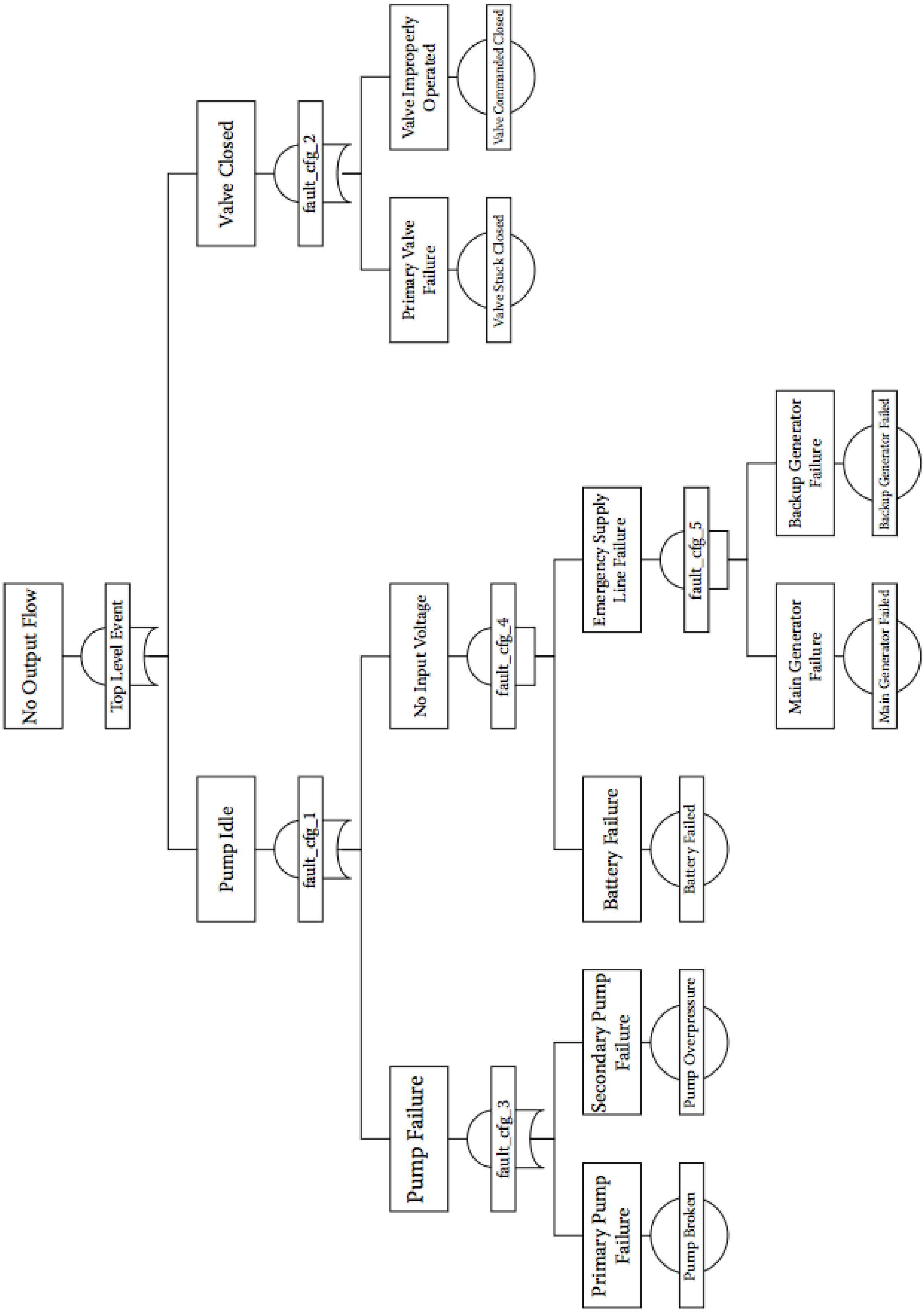
  level of resolution level of detail used to trace back an event (which must be traced farther down, which can be left undeveloped)
- there may be different choices for intermediate events
- *localized* fault ⇒*primary, secondary, command* faults are investigated

  primary fault is in an environment, the component is specified for

  secondary fault is in an environment, the component is not specified for

  command fault is due to correct operation, but at the wrong time
- qualtitative analysis can be conducted after tree has been completed
  - *Minimal Cut Set* minimal set of events needed for the top event ⇒top event, OR, all events needed
  - shows up weaknesses of system
- quantitative analysis can be conducted after tree has been completed

– use minimal cut set to calculate probability of the top event (from the probability of basic events)



- automatic FT synthesis possible if design is purely hardware
- software FTA
  – verification ⇒code already has to be written (Or the logic has to be fully described)

- if loops present in software ⇒human assistance needed

- quantitative analysis very costly ⇒may be more feasible, if some designs and only small differences
- additional analysis needed for effective safety program
- suited for discrete events (valve open/ close) but not for rate- or time- dependent events
- ⚡ not suited for *phased mission* (missions, where there are different phases) (one fault tree needed for each phase, as same components may be used in different configurations and environments)

Failure Mode and Effect Analysis (FMEA)

- inductive technique
- introduced 1940 by US military, later for Apollo (NASA)
- extensive spread in variety of domains
- starts with identification of failure modes ⇒forward reasoning ⇒asses their effects on complete system
- usually consider effects on same level (and usually one level higher)
- also *scope* and *boundary* ⇒by safety engineer and take user requirements into account
- can be applied to hardware component level or at functional level
- typically consider only single faults, combinations can be considered in particular cases
- extension: *Failure Modes, Effects and Criticality Analysis* (FMECA)
  - also take criticality of consequences of component failures into account
  - can identify weaknesses in development process (e.g. assembly or manufacturing) ⇒*process FMECA*
- results ⇒FMEA-table
- results of FMEA ⇒*Failure Mode Effects Summary* (FMES) ⇒failure modes leading so same effect are grouped

HAZard and OPerability studies (HAZOP)

- inductive method
- developed in chemical domain in 1960s
- used primarily in process industries (chemical, petrochemical, nuclear)
- team approach to hazard analysis, members have different backgrounds and competences
- investigate basic set of operations ⇒consider deviations from normal operation ⇒potentially hazardous effects
-

Event Tree Analysis (ETA)

- bottom-up
- developed in nuclear industry in 1960s
- starts from an *initiating event*, proceed from from left to right, branch on further events during analysis ⇒determine potential effects
- typically binary branching
- can get quite large ⇒prune illogical branches and branches, that cause nothing bad
- events can be quantified ⇒assign probabilities for each branch

Risk Analysis

- combines *measure of severity* of the consequences of a safety hazard and a *measure of the likelihood* (probability/ frequency)
- always refers to undesired future consequences, expectation of loss (human live, economic, ...)

Risk Measures

- qualitatively or quantitatively

quantitatively risk is defined on probability measures (e.g. number of fatalities)

Individual Risk Per Annum (IRPA) probability, that an individuum dies within a 1-year exposure to hazard

fatal accident rate expected number of fatalities per 10^8 hours of exposure

qualitatively depends on the kind of consequences (e.g. are they dead or just hurt)

Classification of Hazards: Severity

- degrees of severity (depends on standard used): *catastrophic*, *critical*, *hazardous*, *negligible*

Classification of Hazards: Frequency

- frequency of occurrence (depend on standard): *frequent*, *probable*, *remote*
- different units, e.g. number of events per flight hour

Classification of Risks

- combination of qualitative and quantitative measure

⇒ *risk class* or *risk level*

Risk Management and Acceptance

- reduce likelihood of potential accidents
- mitigate consequences of potential accidents
- different ways to achieve this
  - eliminate potential hazards
  - prevent occurrence of accidental events
  - reduce effect of accidents
- thus includes several techniques
  - hazard identification
  - hazard assessment
  - risk evaluation
  - risk reduction
- produce safety argument, that risk management has been done (for safety critical systems) ⇒certification authorities
- definition of *acceptable risk* is a decision to be taken ⇒cost/ benefit analysis

As Low As Reasonable Practicable the cost of further risk reduction is disproportionate with the reduction gained

Safety Integrity Levels

- ⇒the likelihood that a system will perform all its safety critical functions in a satisfactory way with respect to given operational conditions and period of time

- can be further classified into
  - hardware integrity
  - systematic integrity
  - software integrity
- safety integrity level is orthogonal to risk classification

CheckLists

- make a repository of mistakes (e.g. in company), pass down information already learned
- lists of hazards or specific design features
- used in all life-cycle phases
- ✚ list known hazards, so that none are overlooked
- ✚ ensure consistent procedures (e.g. preflight checklist)
- ↯ may be relied on to much
- ↯ may become very big
- ↯ induce false confidence (if everything is checked, it surely will be ok, won't it . . .)

Harzard Indices

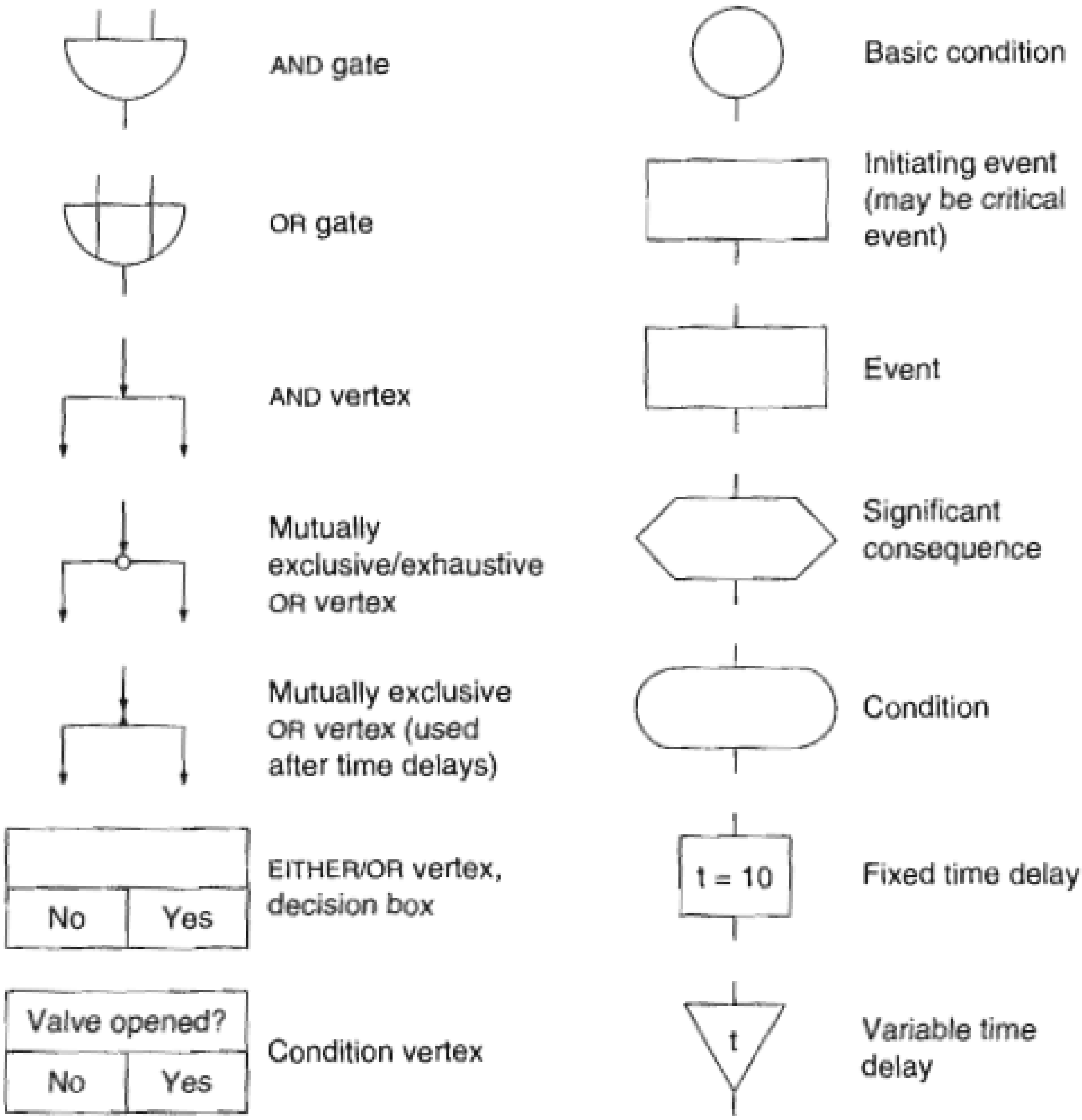
- loss potential due to *fire*, *explosion*, *chemical reactive* hazards in process industry
- *Dow Chemical Company Fire and Explosion Index Hazard Classification Guide* (Dow Index) 1964
  - evaluate processes for maximal property damage
  - divide plant into units (locally separate entities)
  - index indicates the fire and explosion hazard level of a unit (number from 1 to 40)
  - extension: *Mond Index* includes also toxic material
- quantitative indication of potential for hazards associated with design
- not very good for unique design or design, where components develop very quickly

Management Oversight and Risk Tree analysis (MORT)

- can be used as accident investigation or hazard analysis technique
- underlying model: accidents are caused by uncontrolled energy releases
- standard fault tree + analysis of managerial functions, human behavior, environmental factors
- advantages and disadvantages of checklists

Cause-Consequence Analysis (CCA)

- starts with *critical event*, determines the causes top-down and the consequences (forward search)
- shows time and causal dependency
- table of symbols
  - event and condition symbols ⇒type of event or condition
  - logic symbols ⇒gates, relation between events
  - vertices ⇒relations between consequences



Interface Analysis

- evaluate connections and relationships between components ⇒incompatibilities and possibility for common-mode failures
- physical, functional or flow category
- types of problems
  - no output from unit or interconnection failing
  - degraded output or partial interconnection failure
  - erratic output (intermittent or unstable operation)
  - excessive output
  - unprogrammed output
  - undesired side effects (e.g. heat damages nearby unit)
- similar to HAZOP, but more generalized

State Machine Hazard Analysis (SMHA)

- build a state machine, check for hazard state

Task and Human Error Analysis

Qualitative Techniques

Procedure Task Analysis review procedures to verify they are effective and within context for mission task

Operator Task Analysis operators task broken down into separate operations

Action Error Analysis (AEA) forward search strategy to identify potential deviations in human performance

- potential deviations: forget a step, wrong order of steps, taking too long for a step

Work Safety Analysis (WSA) similar to HAZOP, search process is applied to work steps ⇒identify hazards and causes

Quantitative Techniques

- humand error results from human-task mismatch, poor interfaces, poor operating procedure design

Simple and Vigilance Tasks sequence of simple tasks with little to no decision required

- assign probabilities with which the task breaks
- series tasks ⇒product of probabilities
- tree tasks ⇒logic combination
- also possible: use empirical data for probabilities

Complex Control Tasks simple task model inadequate, when technology changes fast ⇒decision making, complex problem solving