

NE529

RISK ASSESSMENT

Fault & Event Trees

5

R. A. Borrelli

University of Idaho



Idaho Falls Center for Higher Education

Learning objectives

Chapter 14, 16 in the book

Skipping decision trees in chapter 12 for later

Quantifying risk using fault and event trees

Identifying where these tools fall short

See [case studies](#) in OER

Learning nodes

Defense in depth

Getting failure rate data

Failure over lifecycle

Pyroprocessing failures

Data perception

Monte Carlo analysis

Human error

Delphi technique

Event tree analysis

Fire

Pump

Gas fracking

LOCA

Limitations

Fault tree analysis

TAM airline

Building the fault tree

Doorbell

Lighting the room

Car crash

Counterexample

Limitations

How likely is it to happen?

Fault and event trees require frequency analysis for initiating events

We need to establish frequencies for a PRA

Data data data data data

Data doesn't magically appear, however

We've been talking about the pyroprocessing system

Troubles with scaling up from the laboratory experiments

Expert judgment only goes so far to where you're just making it up

Then any analysis is effectively meaningless

Defense in depth

Multiple barriers reduce risk

A well designed system has multiple barriers that are implemented to stop or reduce consequences of events

The probability that an accidental event will lead to unwanted consequences will therefore depend on whether these barriers are functioning

Event and fault trees can then also be used as a design tool

Design, procedural weaknesses can be identified

Fault & event trees are needed together for PRA

Explicitly shows all the different relationships necessary to result in the top event

Thorough understanding is obtained of the logic and basic causes leading to the top event

Systematic analysis of the logic and basic causes leading to the top event

Provides a framework for thorough qualitative and quantitative evaluation of the top event

Input for Farmer's chart

Getting failure rate data

Failure rate data is probably the most important

We need to know when equipment is going to fail for basically everything

As well as the probability distributions

We can also just buy equipment and test it

Manufacturer might have the data

Though most entities outside of academics don't really have the time

There is a 30 year test bed for clay and radioactive waste in France at the repository site

Because the repository is completely new and unprecedented

We need to model behavior for at least 1000 years

Some data can be obtained from the manufacturer

Historical data (e.g., MCNP error messages)

Government and military handbooks

Reliability Information Analysis Center

U. S. Energy Information Administration

Failure over lifecycle

Failure rate of system or equipment varies over life cycle

We've shown the bathtub curve

Airplanes – Like a tylenol with wings!

Failure Knowledge Database

Table 8.2 from the book

Failure rate example

Sorting data can present a picture of what is going on

First, they sorted by **failure**

I then sorted by **temperature and hours of operation**

Observations?

Failure rate – $\lambda = \frac{20}{130300} = 1.53 \times 10^{-4}$ per hour

Mean Time Before Failure (MTBF) – $\theta = \frac{1}{\lambda} = 6515$ hours

Assumes all systems fail in the same way

Let's look at failure as a function of temperature

Above 100

$$\lambda = 2.14 \times 10^{-4} /h$$

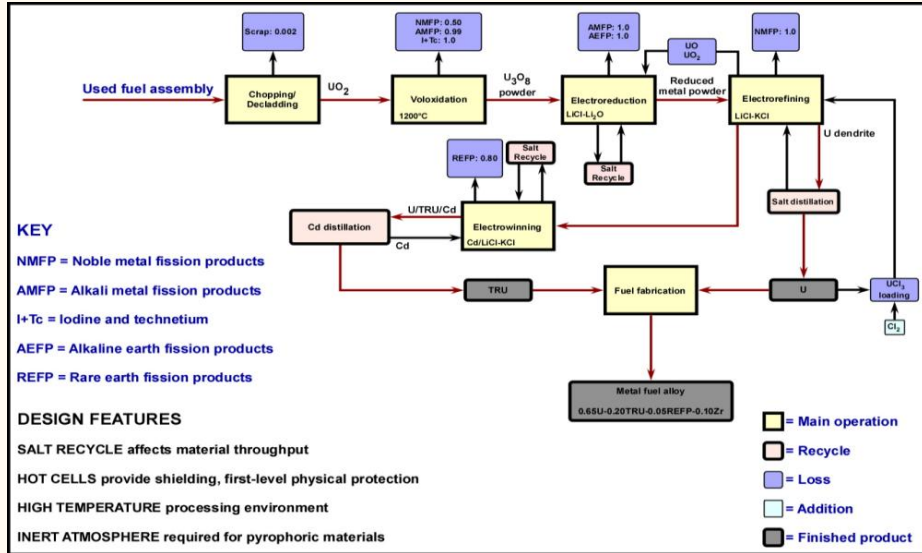
$$\theta = 4675 \text{ h}$$

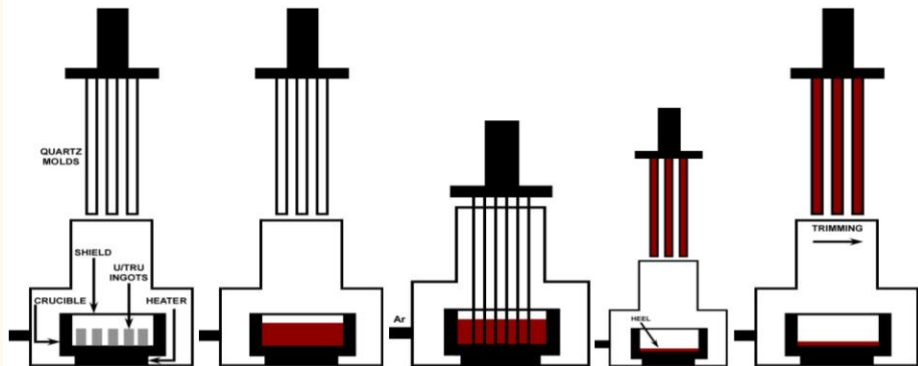
Below 100

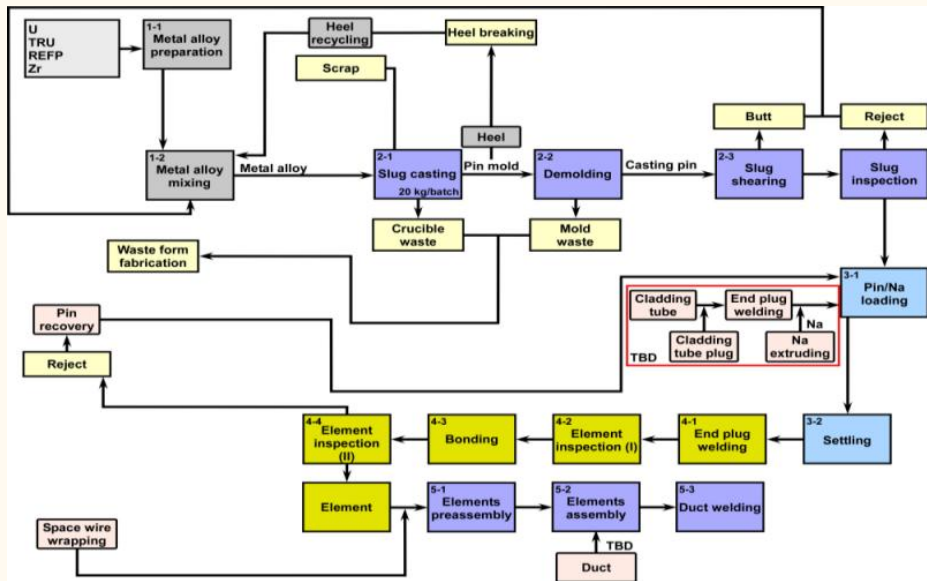
$$\lambda = 1.08 \times 10^{-4} /h$$

$$\theta = 9275 \text{ h}$$

Pyroprocessing failures







Multiple failures, much more complexity

Getting material into the crucible

Heater fails to sufficiently melt all the metal

Vacuum cannot be induced

Molds get stuck or break

Cannot remove heel

If one component fails the equipment fails

Systems do not fail in the same way

Data perception

It is important to consider how to frame failure data or what the data actually is

Space shuttle program used as an example 8.1.9

At the time, failure rate was 1 in 25

2 catastrophic failures in 132 flights currently however

Each shuttle operated for different number of missions with varying operating time (table 8.5)

Total of 30946 operating hours = 4.5 operating years

1 failure in 15000 operating hours for 5 different shuttles

There is not any normalization in terms of failures per operating year

Monte Carlo analysis

Monte Carlo can be used to establish failure rates or MTTF

Monte Carlo simulation is very famous, but not fancy

Generates values of a random variable based probability distributions

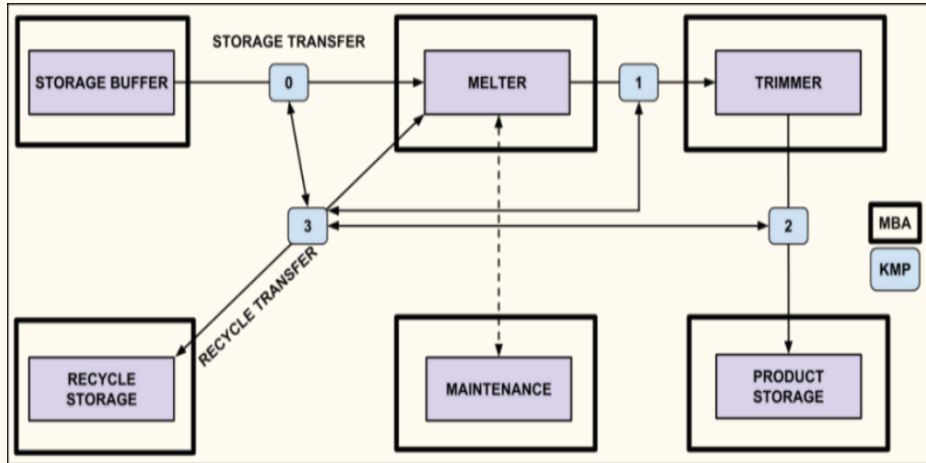
Applied to wide variety of complex problems involving random behavior

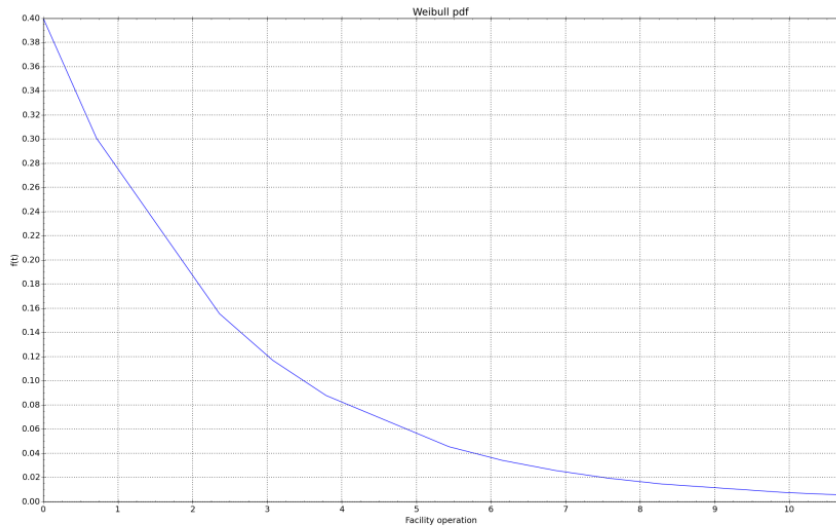
$$R(T) = e^{-\left(\frac{T}{\eta}\right)^\beta} \quad (1)$$

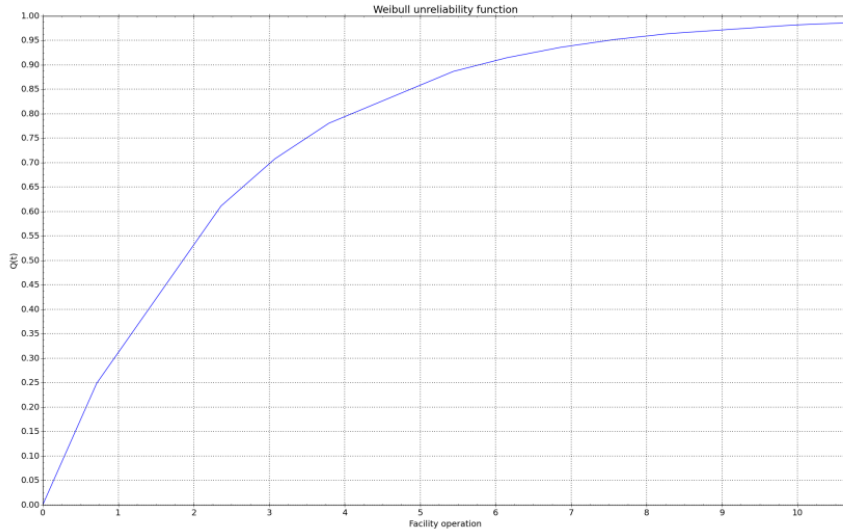
$U \equiv R(T)$ – U is a random number

$$T = -\eta(\ln U)^{\frac{1}{\beta}} \quad (2)$$

When $\beta = 1$ we have the exponential distribution







We can use the unreliability function to simulate failures

$$Q(t) = 1 - R(t) \quad (3)$$

$$Q(t) = 1 - e^{-\left(\frac{t}{\eta}\right)^\beta} \quad (4)$$

Assume $\beta = 1$ for general failures

$\lambda = 0.4$ per day

Monte Carlo simulates area under the curve at $t = T$

A 'hit' is an equipment failure

campaign: 1
operation time: 0.7144
failure probability: 0.2486
failure test: 0.1808
failure

campaign: 2
operation time: 3.0762
failure probability: 0.2486
failure test: 0.6888
no failure

New equipment is installed, so there is new distribution

Early times the likelihood of failure is low

Later times it is higher because equipment is older

Failure testing repository

Human error

Human error probability is difficult to quantify

Because people generally behave stupidly even sober

Or, different responses are elicited by people in the same environment

What would be examples of human errors that could be quantified?

Astronaut behavior in normal conditions and critical conditions

Psychological stress

Performance shaping factors account for human response to stressors

hot/cold

noise level

light level (my office is dark)

vibration

ergonomics

experience and training

management

time

stress

equipment design/human machine interface

Delphi technique

The Delphi technique

Initially developed in the 1950s by Helmer and Dalkey at Rand Corp

Controlled opinion feedback

... to solicit expert opinion to the selection, from the point of view of a Soviet strategic planner, of an optimal U.S. industrial target system and to the estimation of the number of A-bombs required to reduce the munitions output by a prescribed amount.

Delphi can be used to validate research outcomes

Impact analysis of changes to the international business environment

Identify national park selection criteria

Develop a taxonomy of organizational mechanisms

Develop rules for a ceramic casting process

Examine and explain how recruitment message specificity influences job seeker attraction to organizations

Well suited to rigorously capture qualitative data or when knowledge is incomplete

Assemble a panel of experts

Mission

Build consensus with a panel

Aircraft maintenance tasks - missing structural anomalies on an inspection (8.1.12)

For composite structural material

Select panel and eliminate bias

Airline inspectors (regulations)

Structural experts from manufacturer(s)

Repair/mechanics experts

Calibrate the panel on the topic

Historical data on detecting cracks in the structure (not the same but close)

Inspection, procedures, etc.

In book example, estimated probabilities are presented

Set problem boundaries and constraints

Present the parameters of the task to evaluate

Qualitatively assess the problem

Discuss any direct historical experience from inspectors, mechanics

What kind of structural anomalies would be present?

Perform the initial round of discussions on the error probability

Detecting anomalies 2" or less

Establish nominal probabilities for each class of crack

Discuss the results and iterate

Repeat until consensus reached for each class

Determine roadblocks

Develop performance shaping factors

What factors would lower the probability of the task?

Lack of training; experience

Environmental conditions; lighting, etc.

Time to inspect

Establish the conditions where the task can be achieved satisfactorily

For use in human reliability analysis

Event tree analysis

An event tree is a graphical representation of a series of possible events in an accident sequence

Each event is either a fail or success with associated frequency

Assumes events occur in sequence to a final state

Event sequences follow from some initial event of interest, usually a component failure

Downstream events follow from original event and subsequent events of other components

Initiating event \rightarrow event 1 \rightarrow event N \rightarrow Final State

We covered ways to assess frequency - now we ask 'What are the consequences?'

Event trees apply forward logic

We start with the initiating events and work to what eventually happens

Event trees are used to describe the major events in the accident sequence

Each event can then be further analyzed using a fault tree

Event trees are accident sequence development tools

We talked about WASH1400 that basically invented for nuclear power plants

NRC [handbook](#)

Figure 12.3 in the book

Event trees are essential to PRA

Visualize event chains following an accidental event

Visualize barriers and sequence of activation

Good basis for evaluating the need for new/improved procedures and safety functions

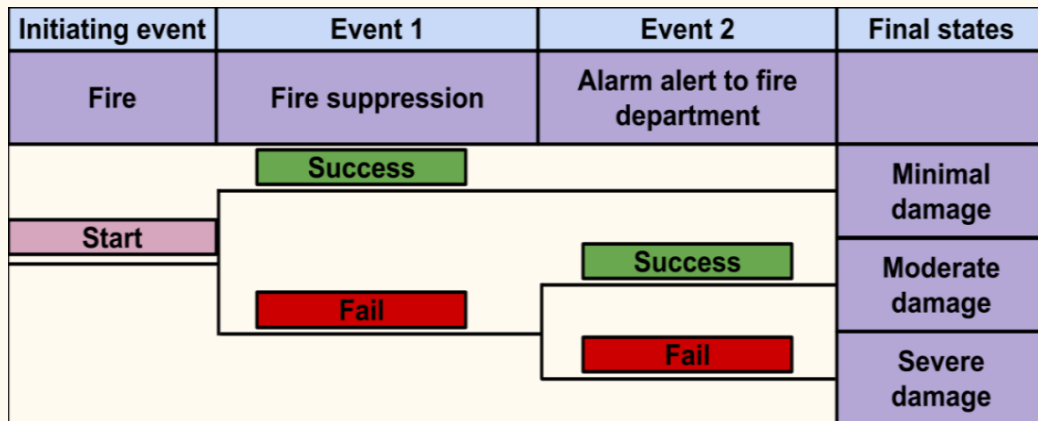
Draws on prior PRAs, etc., to determine initiating events

So it's a natural progression into PRA I,II,III

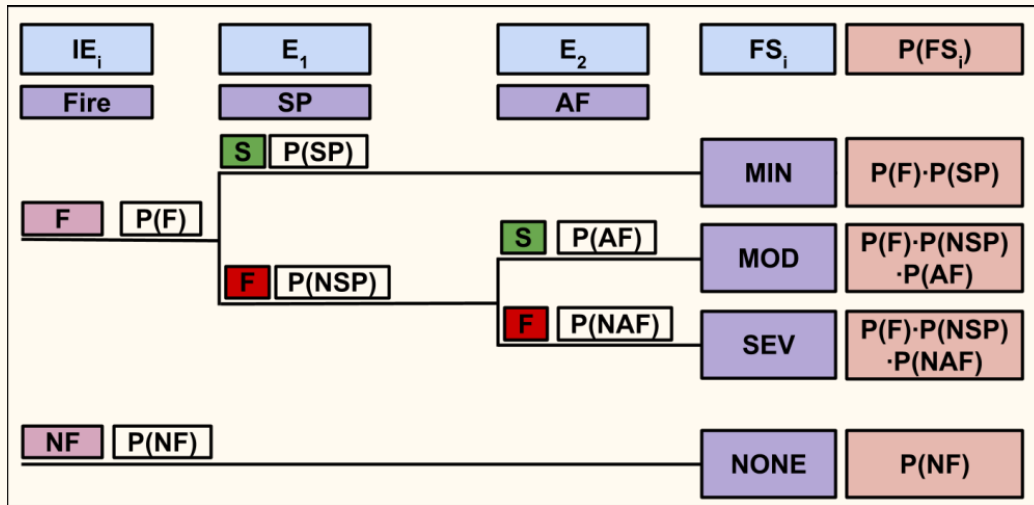
Examples

Fire

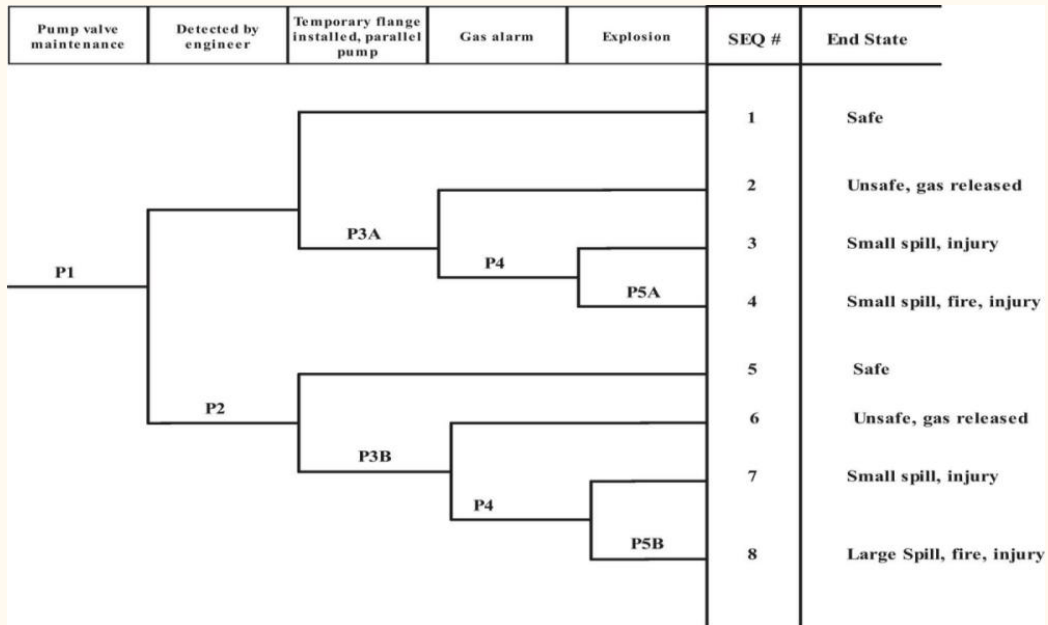
What events lead to **fire**? – Figure 12.2



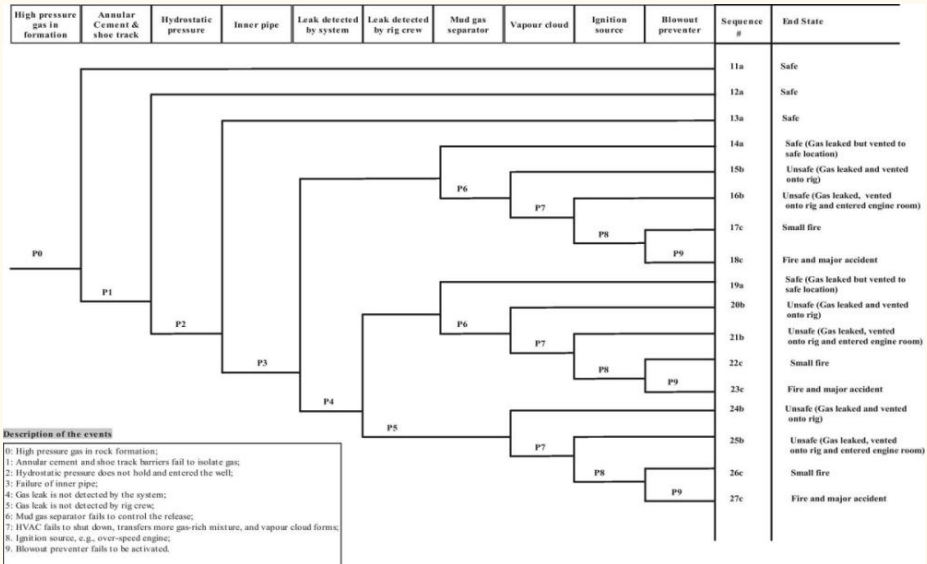
Calculate probabilities and losses



Pumps



Fracking



LOCA

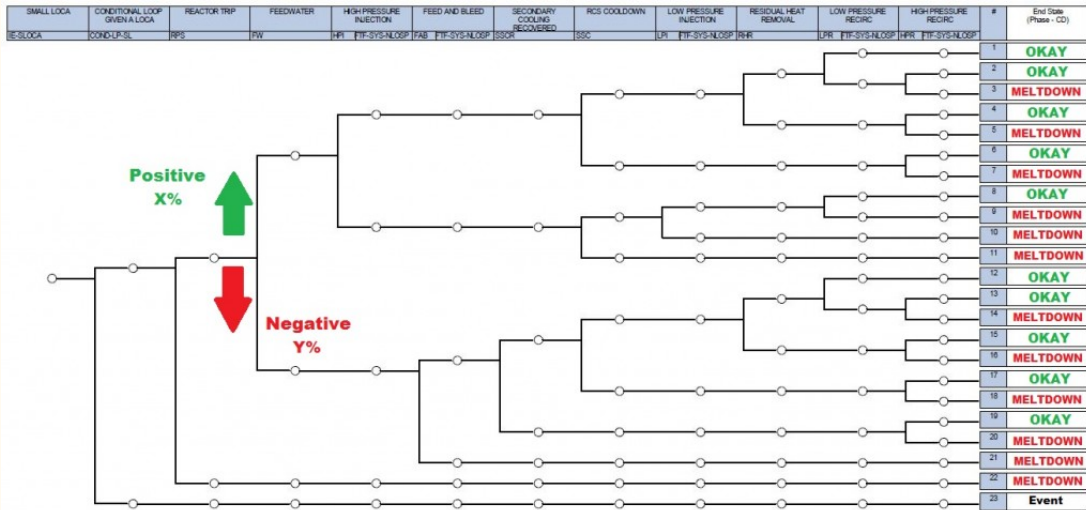


Figure G-1 Small-break loss-of-coolant accident (SLOCA) event tree

Limitations

But event trees have limitations

No standard for the graphical representation of the event tree

Only one initiating event can be studied in each analysis

Easy to overlook subtle system dependencies

Not well suited for handling common cause failures (only independent events)

Practical only when events can be ordered in time (chronology of events is stable)

Does not show acts of omission

Difficult to represent interactions among events

Difficult to consider effects of multiple initiating events

So we need other tools for comprehensive risk assessment

Fault tree analysis

Fault tree analysis is applied to identify areas to mitigate or prevent risk at all phases of system life cycle

Little things lead to catastrophic failures

Japan airlines

But before risk assessment was invented, most likely from common cause failures

Advancements in technologies increased complexity and necessitated detailed safety analysis

Developed by Bell Telephone Laboratories (1962) for Minuteman ICBM (can't find any information)

Though it seems that not formalized as part of risk assessment until WASH1400

Fault trees are a graphic to represent the interaction of failures and other events in a system

Top down, deductive failure analysis

Top event are hazards or failure modes (from event tree) – LOCA, emissions, explosions

Decompose the top event using boolean logic (AND, OR)

Bottom set of events are non-decomposable (basic events)

Identify failures as a malfunction in a component requiring repair (pump shaft)

Identify faults as malfunctions that self-repair once the governing condition is corrected (wet contacts for a switch; dry them)

Undeveloped events are neglected due to low probability or effect on system

FMEA can be used as input

Define the top event clearly and unambiguously

What is the event?

Where does the event occur?

When does the event occur?

Immediate, necessary, and sufficient causes leading to the event

Connect via logic gates (down)

Get down to independent events

For which failure data is obtained (or distributions)

Work back up to compute top event probability

Assemble a basic event matrix after defining the top event

Basic failure event – description – credible? (table 14.5)

Assessing credibility = whether to include the event in the fault tree

Coolant system flushing procedure in the car (14.7.1)

Sprinkler system failure

System design tool

TAM airline

TAM Airlines Flight 3054 overran the runway and crashed into a warehouse (2007)

Use of fault trees for accident analysis with multiple failures (14.7.3)

Airplane are an instructive example because we know a lot about them

Warehouse next to gas station, which exploded

199 fatalities

What happened

Rain caused the runway to be wet

Plane overran the runway

Crossed the road(!)

Background

20379 operating hours

Jammed braking device reported the day before (thrust reverser)

Landed and couldn't slow down

Veered left and overshot runway over the major road

Collided with warehouse

Safety issues with insufficient length of the runway (faster speed, more distance to stop)

Thrusters in climb position just before touchdown

Audio warning 2 seconds before touchdown for pilots to take manual control

One idle, one at climb position at touchdown; both needed to be in idle position

(cause of veering left)

So, what are some causes for this crash?

Como foi o acidente

2 O avião atravessa a av. Washington Luis, colide com o depósito de cargas da TAM e provoca incêndio no local

1 O Airbus A320 da TAM, voo JJ 3054 não consegue realizar a manobra na pista e derrapa



Imagem: Google Earth

Top event is the airplane crash

Wet runway (hydroplaning, loss of vehicle control)

Rain

Grooves cut in runway to drain and increase traction

Thrust reverser broken (known)

Airline policy allowed aircraft to be flown with broken thrust reverser

Short runway

Airport policy allowed larger planes to land on runway

Experienced pilots had not had training in this situation

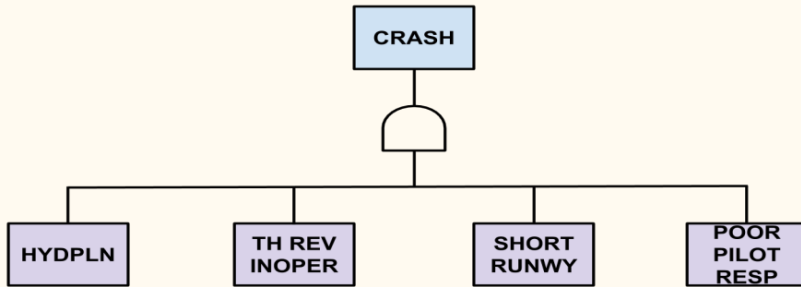
Building the fault tree

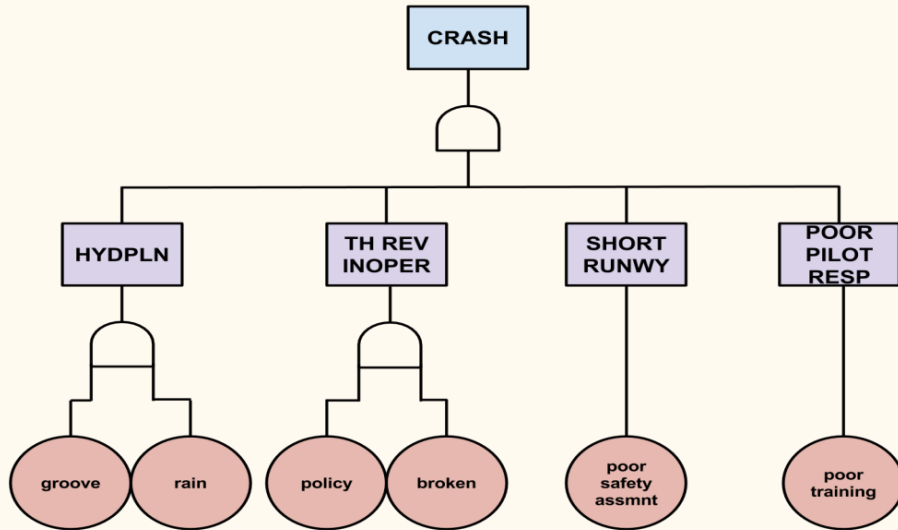
How is the probability of crash calculated?

Gates aren't limited to only two events

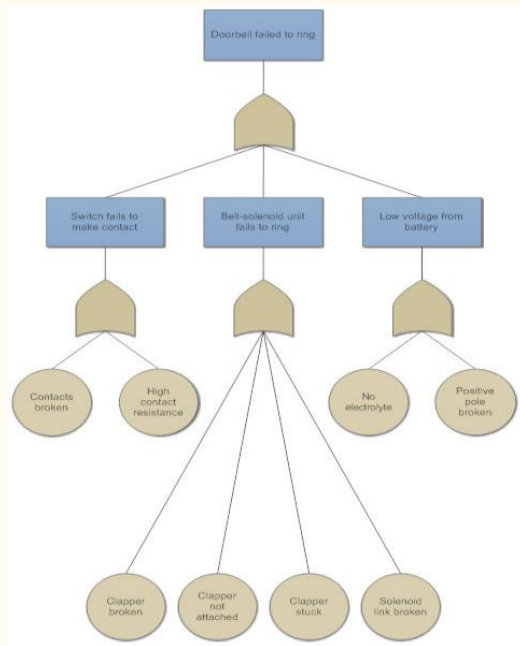
Can be more than one level of intermediate causes

CRASH

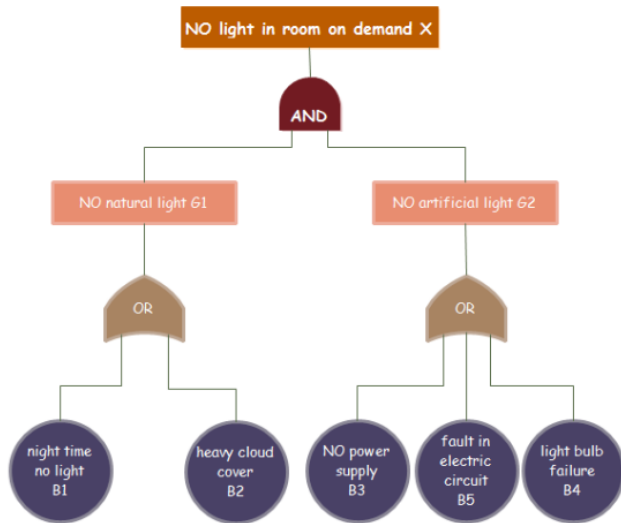




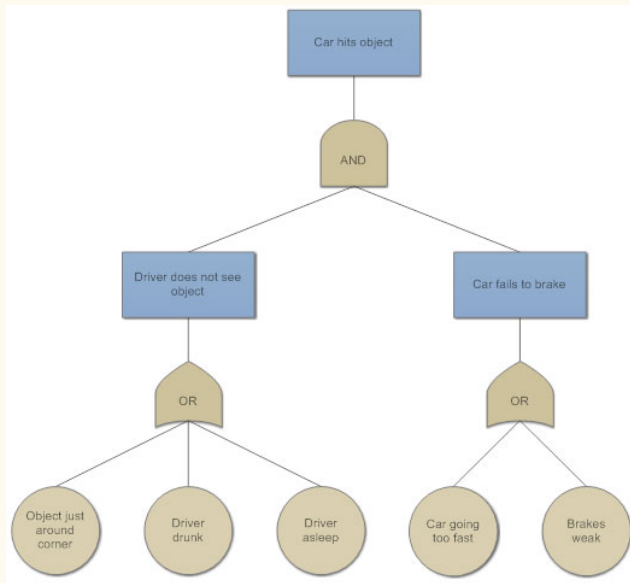
Doorbell



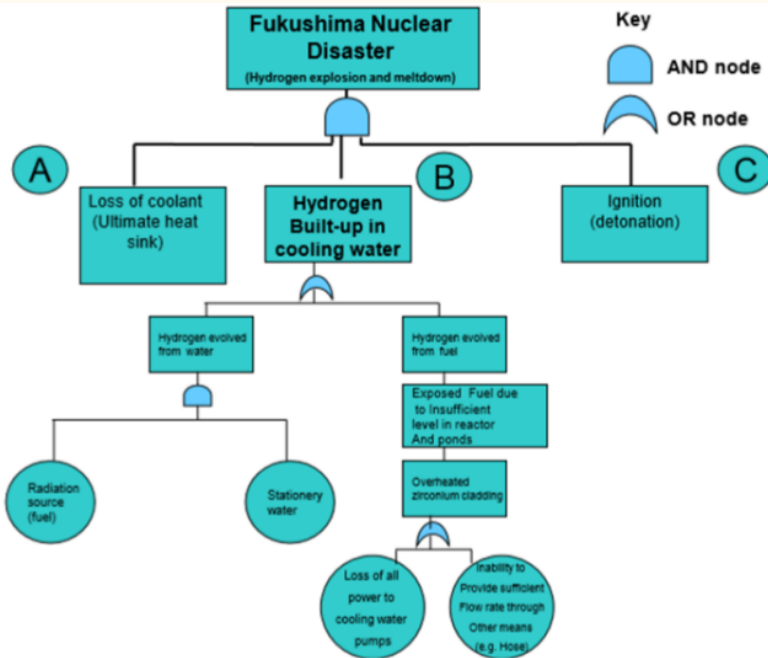
Lighting the room



Car crash



Counterexample



Limitations

Of course, there are limitations

Undesirable events must be foreseen

We don't know what we don't know

Each event analyzed singly

Significant contributors to fault/failure must be anticipated or predicted

Each initiator must be constrained to two conditional modes (AND/OR)

Initiators at beneath a common gate must be independent

Still requires detailed knowledge of the system

