Dependable Systems

6. Chapter

Static Modeling: Fault Trees

Prof. Matthias Werner
Operating Systems Group

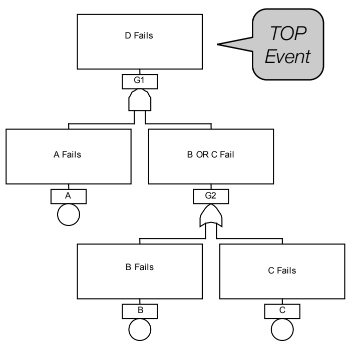
Motivation

- **Until now**:description of error behaviors for single systems and "simple" compositions (in terms of set theory and reliability block diagrams)
- **Fehlerbaumanalyse (Fault Tree Analysis, FTA) :** describes **possible ways** in which an **undesired system state** can occur
  - Inventor H.A. Watson (Bell Labs), 1961
  - Identifies undesired events and faults/conditions it depends on
  - Used by Boeing since 1966, meanwhile adopted by different industries

6.1 Construction

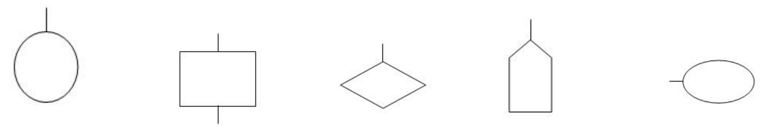
Construction of Fault Trees

- Dependencies between events and faults by boolean net
- Basic events (faults) can be associated with component hardware failures, human errors, software errors, or any other pertinent events
- Includes only faults that contribute to the top event
- Events and gates are **not** system components
- In itself not a quantitative model, but can be evaluated as one



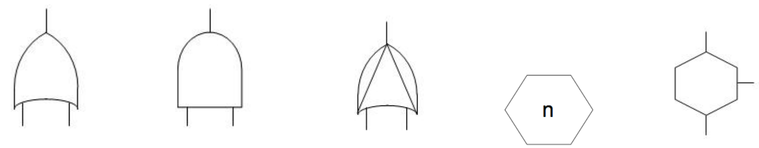
Elements

- **Events**



basic event | intermediate event | undeveloped event | extern event | conditioning event

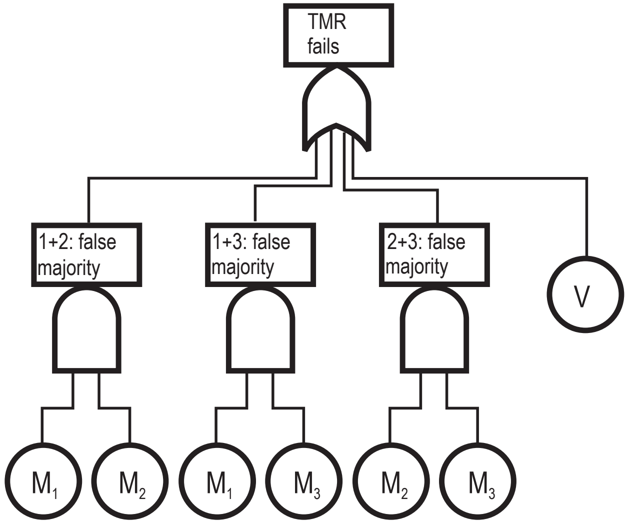
- **Gates**



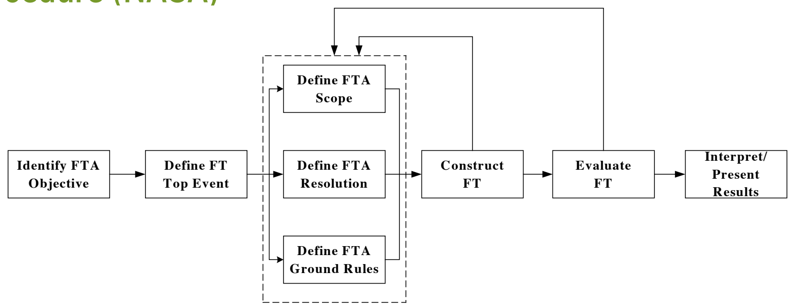
or gate | and gate | xor gate | voting gate | inhibit gate

- One finds different symbols in different source

Example: Fault Tree of TMR System



Procedure (NASA)



- General goal: to evaluate different designs
- Objective should be phrased in terms of a system failure to be analyzed
- Define **scope** (design version, components to be included), **resolution** (based on available probability data) and **ground rules** (naming scheme for events and gates)
- Focus on necessary and sufficient immediate events

Procedure regarding K. B. MISRA

1. Define the undesired event to be analyzed – what, where, when
2. Define boundary conditions for the analysis
   - Physical boundaries – What constitutes the system?
   - Environmental stress boundaries - What is included (earthquake, bombs, ...)?
   - Level of resolution - How detailed should be the analysis for potential reasons?
3. Identify and evaluate fault events
   - Primary failures as basic event, secondary failures as intermediate event
4. Complete the gates
   - All inputs should be completely defined before further analysis of them

Procedure regarding K. B. MISRA (cont.)

- Common mistakes
  - **Ambiguous TOP event**: Too general TOP event makes FTA unmanageable, too specific TOP event cannot provide a sufficient system analysis with FTA
  - **Ignoring significant environment conditions**: External stress might be relevant
  - **Inappropriate level of resolution:** Detail level of the fault tree should match the detail level of the available information
- Proper and consistent naming is very important (**what** failed and **how**)
- Basis events should be independent
- Logic can be tested in **success domain** by inverting all statements and gates

6.2 Evaluation

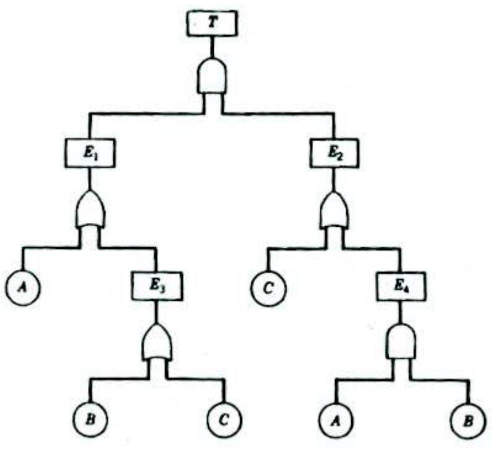
Evaluation

- Two kinds of evaluation
  - **Qualitative evaluation**
    Identify event sets which cause failure
  - **Quantitative evaluation**
    Determine failure probability
- Quantitative evaluation depends on qualitative evaluation

Cut Sets

- **Cut set**: Any group of basic events which, if all occur at the same time, cause the TOP event
- **Minimal cut set (mincut)**: Minimal combination of basic events that induce TOP
  - "Minimal" ➡ All basic events are needed to let the TOP event occur
  - A long mincut shows low vulnerability, a short mincut shows high vulnerability
  - A **singleton cut set** shows a **single point (of) failure**
- Analysze cut set for
  - Weak points in the design
  - Bypass of intended safety features
  - Common cause problems
- Methods for cut set finding:
  - Boolean reduction, bottom-up reduction, top-down reduction, mapping to binary decision diagram, Shannon decomposition, genetic algorithms, ...

Example for Boolean Reduction



$$T = E_1 \cap E_2$$
$$T = (A \cup E_3) \cap (C \cup E_4)$$
$$T = (A \cup (B \cup C)) \cap (C \cup (A \cap B))$$

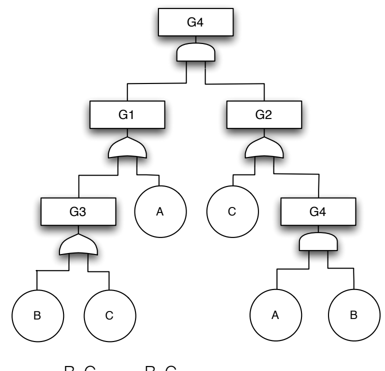
Simplification

$$T = (C \cup (A \cup B)) \cap (C \cup (A \cap B))$$
$$T = C \cup ((A \cup B) \cap (A \cap B))$$
$$T = C \cup (A \cap B)$$

➡ 2 cut sets: $\{C\}$ and $\{A, B\}$

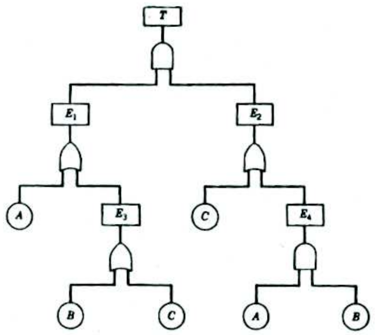
Method for Obtaining Cut Sets by RAUSAND

- Start at the TOP event
- OR gate: Each input to the gate is written in separate rows
- AND gate: Each input to the gate is written in separate columns
- Iteratively replace gates in rows and columns
- Each resulting row forms a cut set



G1,G2	G3, G2 A, G2	G3, C G3, G4 A, G2	B, C C, C B, G4 C, G4 A, G2	B, C C, C B, A, B C, A, B A, G2	B, C C, C B, A, B C, A, B A, G2	B, C C, C B, A, B C, A, B A, C A, G4	B, C C, C B, A, B C, A, B A, C A, A, B	➡	B, C **C** **A, B** C, A, B A, C

Quantitative Analysis



Probability

- Addition:
  $\Pr(X_1 \cup X_2) =$
  $\Pr(X_1) + \Pr(X_2) - \Pr(X_1 \cap X_2)$
- Multiplication:
  $\Pr(X_1 \cap X_2) = \Pr(X_2) \cdot \Pr(X_2)$

from qualitative analysis:
$T = C \cup (A \cap B)$

$$\Pr(T) = \Pr(C) + \Pr(A)\Pr(B) - \Pr(C)\Pr(A)\Pr(B)$$

Quantitative Analysis (cont.)

- Quantitative analysis helps to find **dominant minimal cut set**
  - Calculate the probability of each minimal cut set
  - Sort by probability
- Determine of importance of cut sets or single events
- ...

Attention

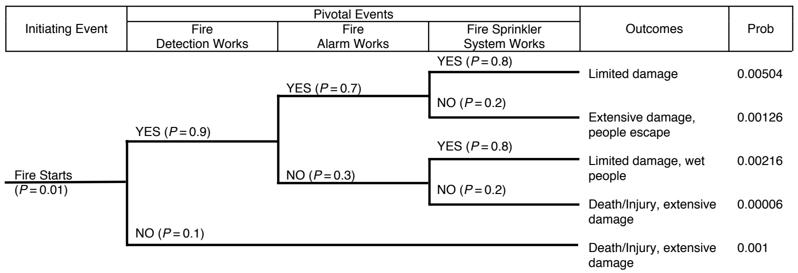
Independence of basic events must be always ensured!

6.3 Discussion

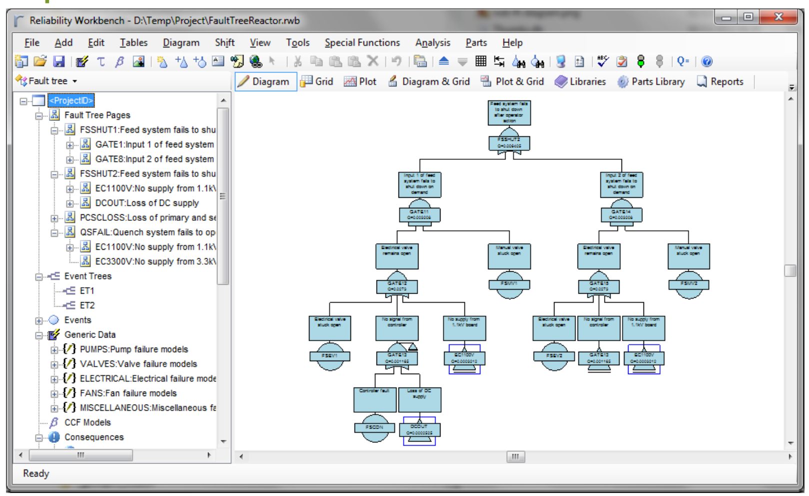
Discussion

- FT tend to become complex
  - Use of hierarchical approaches
  - Combination of FTs of subsystems
  - Tool support
  - Amend FTA by **event tree analysis**

Transfer in Transfer out



Example of a FTA Software



Source: Isograph Ltd

FTA-based Decision Making

- Use FTA to...
  - understand the logic leading to the top event, especially in complex systems
  - prioritize the contributors leading to the top event (typically 10% - 20%)
  - proactively prevent the TOP event by applying targeted upgrades
  - minimize and optimize resources – identify what is unimportant
  - assist the system design
  - monitor the performance of the system by FTA re-evalutation, based on former defects and failures
  - gain input data for FME(C)A

FME(C)A

- **Failure Mode and Effects (and Criticality) Analysis**
- Management (!) tool to risk assessment, used in several areas, e.g.,
  - transportation, esp. automotive and aviation/space
  - medical engineering
  - food industry
  - ...
- FMEA utilizes other analysis techniques (beside fault trees, e.g., Pareto analysis) and is in turn used in other approaches (e.g., 6σ)

FME(C)A: Risk Priority Number

- FMEA is used in case of imprecise and fuzzy knowledge
- Goal: determine a **Risk Priority Number** (RPN)
- RPN: no absolut statement, but used to rank risks
- Following parameters are considered:
  - S Severity of failures' impact (*severity number*)
  - O Occurence probability (*occurrence number*)
  - D Detection probability (*detection number*)
- All parameter values are in range from 1..10
  - 1 = non-critical, 10 = highly critical

FMEA Process

1. Determine fault
2. Determine impact (failure) of fault (e.g. with help of fault tree analysis)
3. Determine severity of impact ($S \in [1, ..., 10]$)
4. Determine probability of failure causes ($O \in [1, ..., 10]$)
5. Determine discover probability ($D \in [1, ..., 10]$)
6. Compute RPN:

$$RPZ = S \cdot O \cdot D$$

7. Rank, take actions, re-iterate

Example of FMEA Data Acquisition

Hazard	Severitiy	Cause	Probability of Har...	Risk	Method of Control	Control Measures	New Probabilit...	New Risk
Device falls over	Catastrophic	Material failure in support structure	Remote	8	Design	Support materials must be sufficiently strong so as to accommodate any reasonable	Improbable	12
Device catches fire	Catastrophic	Materials in device reach critical flash point, or electrical spark ignites flammable materials	Remote	12	Design	Use flame-resistant materials	Improbable	12
Device heats 1°C over target	Significant	Improper control of heating element	Occasional	6	Design	Optomize circuit for close temperature control	Improbable	15
Device heats 1°C under target	Significant	Improper control of heating element	Occasional	6	Design	Optomize circuit for close temperature control	Improbable	15
Device infects occupant	Significant	Improper disinfecting of unit	Remote	10	Training	Teach users proper disinfection techniques	Improbable	15
Device loses power	Marginal	Failure (or depletion) of power source	Occasional	11	Design	Use long-lasting power source	Remote	14
Airflow inhibited	Significant	Blockage of air passageways	Remote	10	Design	Create large airflow passages, in spatial configurations unlikely to	Improbable	15
Device rolls away	Significant	Improper locking of wheels.	Improbable	15	Design/Training	Use easy-to-lock castors or device support / train staff to lock castors whenever device is occupied	Improbable	15
Device shocks infant	Significant	Insulation of electical system fails	Improbable	15	Design	Design circuitry to be placed far from infant	Improbable	15
Visibility impared by fog or	Marginal	Moisture from unit aggregates on clear portion of device	Frequent	7	Design	Use fog-resistant materials for see-through components	Occasional	14
Heating lamp burns out	Negligible	Inevitable event - tungsten in bulb reaches end of life	Frequent	13	Design/Training	Use long-lasting bulbs and train staff to replace periodically	Improbable	20
Device dehydrates patient	Catastrophic	Improper control of device moisture content	Remote	8	Design	Optomize circuit for close humidity control	Improbable	12