Safety and Reliability of Embedded Systems

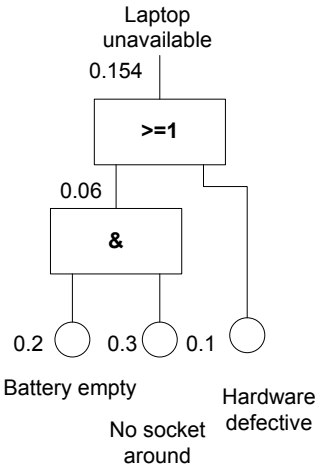
(Sicherheit und Zuverlässigkeit eingebetteter Systeme)

Foundations of Fault Tree Analysis

Content

- Fault Tree Analysis Basics
- Basic Terms
- Gates
- Other Notational Elements
- Informal Use of Fault Trees
- Qualitative Analysis
- Quantitative Analysis
- History
- Standards and Important Literature

What are Fault Trees?



- Fault trees trace back influences to a given hazard or failure
- Help to find all influences
- Graphically explain causal chains leading to the hazard
- Find event combinations that are sufficient to cause hazard (qualitative analysis)
- Calculate hazard probability from influence probabilities (quantitative analysis)

Fault Tree Analysis Basics

- Developed in 1961 by Bell Telephone Laboratories. Later modified by Boeing for computer-aided application
- Analysis method for the qualitative and quantitative evaluation of a specific failure of a system
  - Goal of the qualitative analysis is the systematic identification of all possible failure combinations which lead to a predetermined undesired event
  - Goal of the quantitative analysis is the determination of reliability parameters, e.g. failure rates w.r.t. the undesired event or unavailability of the system
- Causes for the effect can be defective system components
- FTA is applied particularly in complex systems in order to analyze safety-critical effects of failures

Fault Tree Analysis Basics

- Good fault effect model (graphical model of the failure combinations and their effects)
- System evaluation with regard to operation and safety
- Intuitive for engineers due to the familiar logical symbols
- Wide-spread usage in aerospace, nuclear, chemical, and automotive industry
- Fault tree analysis is a standardized method (DIN 25424, IEC 61025, NUREG 0492, Fault Tree Handbook with Aerospace Applications)

Basic Terms

- **Root**: **"Top-Event"** — The hazard or failed state (or the accident or failure event)
- **Leaves**: **"Basic Events"** — The causes that cannot or shall not be refined any further
- **Gates**: Logical connectives

Originally only plain Boolean logic!

What about Inhibit, Sequential AND etc?
Do FTs express causation?

What is an event?
Something happening suddenly?
A state of a component?
A proposition?

In probability theory, "event" means everything that can happen with a given probability

Gates

AND (US Style) | **AND** (European Style) | **OR** (US Style) | **OR** (European Style)

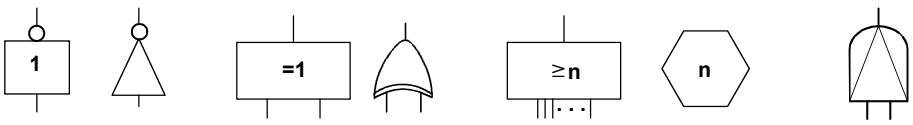
AND: All input events together are necessary to cause the output event

OR: Each one of the input events is sufficient to cause the output event

?

AND-Gate: Can events occur simultaneously?

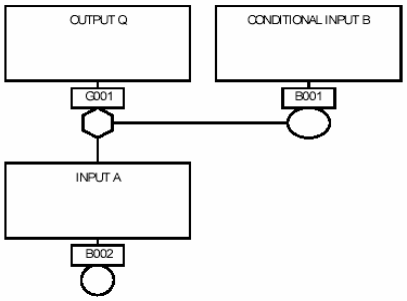
More Gates (taken from different standards!)



1 | 2 | 3 | 4

1. **NOT**: Output event is true when input event is false
   - **NOT is not included in all tools**
2. **Exclusive OR (XOR)**: Output occurs when exactly one of the input events is true
3. **N-out-of-M Voter** alias **Combination Gate**: Output occurs if at least n of the m input events occur
4. **Priority AND**: Output occurs when all input events occur in the specified order

More Gates (taken from different standards!)



Note that B has condition semantics.

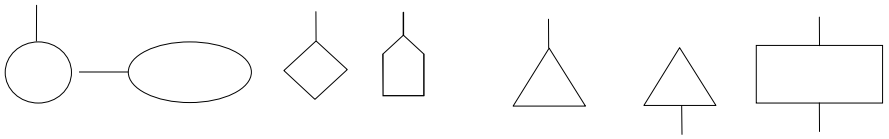
- **INHIBIT**: Output event occurs if all of the input events occur in the absence of an inhibiting condition
  - Additional “ingredient” that is necessary for event A to cause output Q
  - Conditional probability that Q occurs given the occurrence of A

More Gates (taken from different standards!)

- Different spare gates
  - hot / cold / warm spare
  - cf. more complex "Reserveverknüpfung" ("Spare Gate") from German DIN 25424
- Functional dependency
- Sequence enforcing
- Gates modeling different kinds of secondary events

There are (even in standards) gates that are not intuitively clear and informally specified. Their usage should be considered carefully.

Other Notational Elements



1. Basic Event
2. Conditioning Event
3. Undeveloped Event / Secondary Fault (DIN 25424)
4. House Event (Event assumed to occur during operation)
5. Transfer In (Continued from another page)
6. Transfer Out (Continue on another page)
7. Comment / Intermediate Event

Informal Use of Fault Trees

- FTs are useful even without any analysis
  - Help understanding the system
  - Reveal problem areas immediately
  - Build up awareness for safety and reliability issues
- Event can be any proposition
  - E.g. “Subsystem is down for more than 5 minutes without this fact being noticed”
- If later analysis is intended, events should be chosen so that
  - they have a semantics that is clear to any person involved
  - they are self-contained and independent
  - a probability can be assigned to them

Qualitative Analysis

- Check, if the top-event is reachable
- Find minimal cut sets
  - e.g. list all cut sets with order 1 or 2
  - e.g. list all cut sets with total probability > 0.01 (requires quantitative analysis)
- Find minimal path sets

Quantitative Analysis

- Quantitative analysis produces numerical results
  - Probability or rate of top-event / of a given cut set
  - Importance of basic events / cut sets
    - How much impact has an event on the total failure probability?
    - By how much is the total failure probability influenced by changes / uncertainties regarding a particular event?

?

What means probability of an event?

History

- 1960s: Foundations
- 1961 Minute Man Launch Control System (Watson, Bell Labs)
- 1966 Computer Application (BACSIM at Boeing)
- Spreads from Aerospace to Nuclear Industry
- 1967 Apollo 1 Launch Pad Fire -> New Safety Programme including FTA
- 1970s: New algorithms, importance measures
- 1977 Three Mile Island Nuclear Power Plant Accident -> Review using FTA
- 1980s: More powerful algorithms (BDDs), much research, FTA becomes a broadly accepted standard technique
- 1986 Challenger Explosion: Review of Space Shuttle using FTA
- 1990s: Increasing PC performance makes mass market tools possible, research work regarding FTA and formal methods

Standards and Important Literature

- DIN 25424
  - Only in German
  - Explanation of minimal-cut-set-based analysis
  - Separate formulas for enduring events (states) and sudden events
- IEC 61025
- NUREG 0492 Fault Tree Handbook (Vesely et al 81)
- FT-Handbook with Aerospace Applications
  www.hq.nasa.gov/office/codeq/doctree/fthb.pdf

☝ **For algorithms (e.g. BDD) and other details you will probably have to refer to scientific publications**