Chapter 5.
Fault Tree Analysis (FTA)

Mary Ann Lundteigen Marvin Rausand

RAMS Group
Department of Mechanical and Industrial Engineering
NTNU

(Version 0.1)

NTNU – Trondheim
Norwegian University of
Science and Technology

Learning Objectives

The main learning objectives associated with these slides are to:

- Give an overview and brief introduction to fault tree analysis
- Describe the relationship between reliability block diagrams and fault trees

The slides include topics from Chapter 5in **Reliability of Safety-Critical Systems: Theory and Applications**. DOI:10.1002/9781118776353.

Outline of Presentation

Fault Tree and Fault Tree Analysis

A **fault tree** (FT) is a **top-down logical diagram** that displays the interrelationshos between a critical system event and its causes.

The main elements of a fault tree are:

- **TOP event**, which is the description of the critical system event
- **Basic events**, the are the lowest level of identified causes
- **Logic gates**, such as OR or AND gates, which gives the logical relationship between the TOP event and the basic events
- There are also some additional symbols which are explained in the textbook

Fault tree analysis is the qualitative and quantitative analyses that can be carried out on the basis of a fault tree.

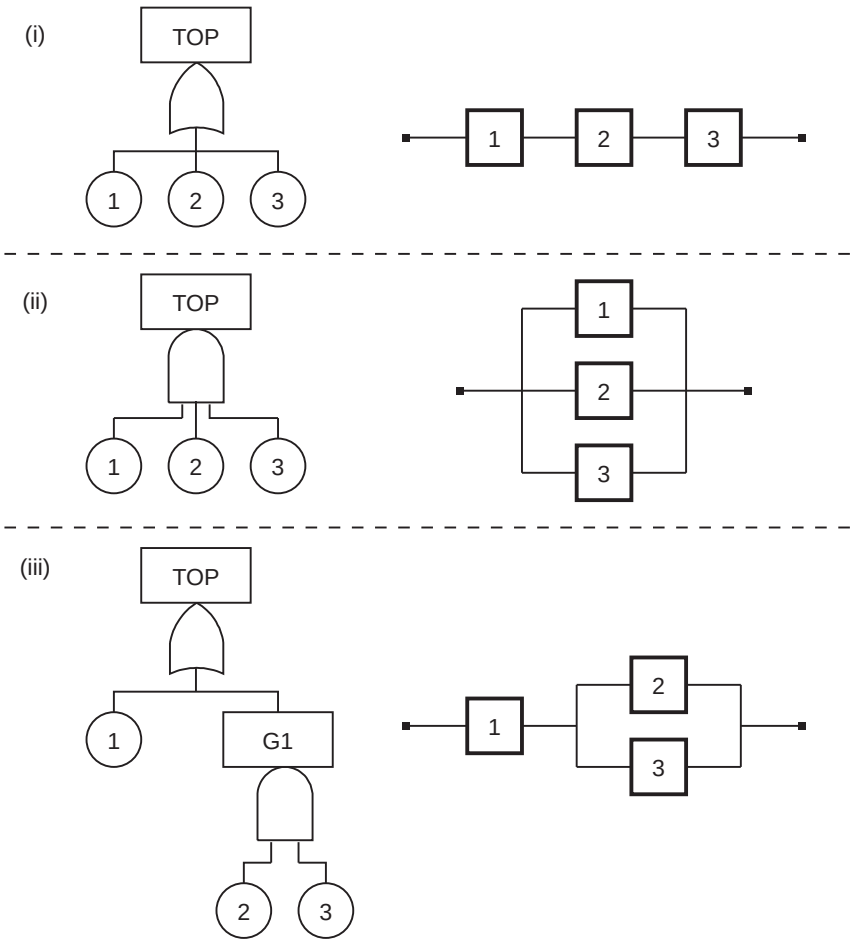
Fault Tree Analysis Steps

Fault tree analysis is often carried out in five steps:

1. Definition of the problem, system, and boundary conditions of the analysis
2. Construction of the fault tree
3. Identification of minimal cut sets
4. Qualitative analysis of the fault tree
5. Quantitative analysis of the fault tree

Fault Tree vs Reliability Block Diagram

A fault tree may be converted into a reliability block diagram and vice verse, as illustrated below.



Minimal Cut Sets

Identification of **minimal cutsets** is one of the most important qualitative analysis of a fault tree.

☞ Cut set: A cut set in a fault tree is a set of basic events whose (simultaneous) occurrence ensures that the TOP event occurs.

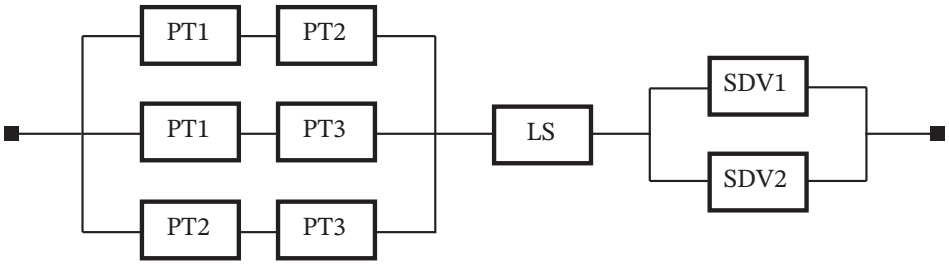
☞ Minimal cut set: A cut set that cannot be reduced without losing its status as a cut set.

The TOP event occurs if one or more of the minimal cut sets occur.

Fault tree modeling

Example

Consider the reliability block diagram of the SIF shown below:

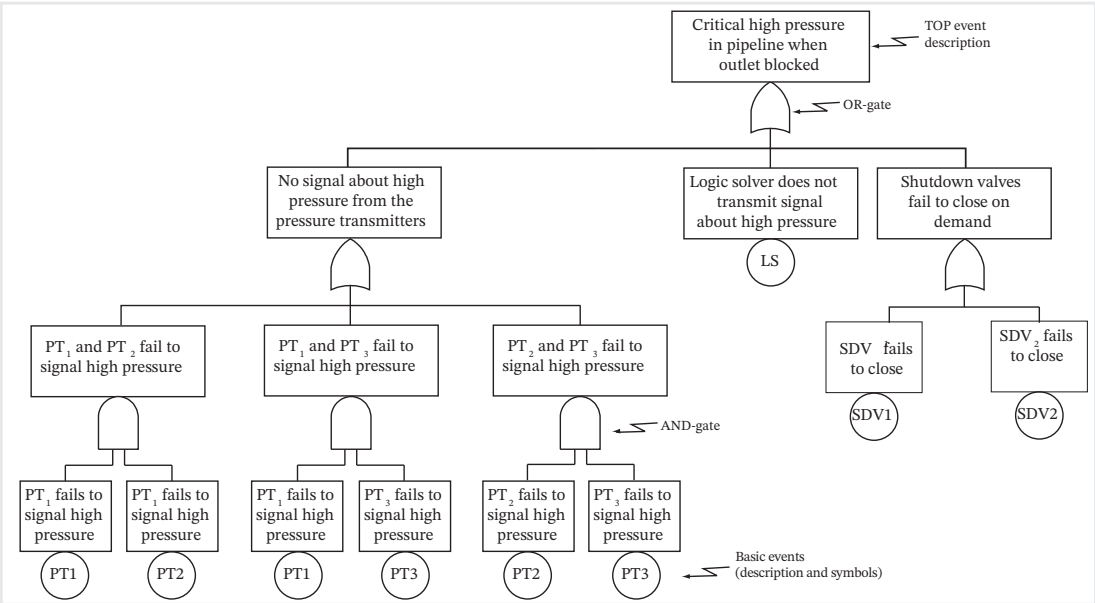


We can already now, on the basis of the fault tree, identify the minimal cut sets (denoted C_i):

$$
\begin{aligned}
C_1 &= \{PT1, PT2\} \\
C_2 &= \{PT1, PT3\} \\
C_3 &= \{PT2, PT3\} \\
C_4 &= \{LS\} \\
C_5 &= \{SDV1, SDV2\}
\end{aligned}
$$

Fault Tree Example

Consider a SIF that comprises three pressure transmitters (voted 2oo3), one logic solver, and two shutdown valves (voted 1oo2). The critical event is that the pressure becomes to high, due to a failure of the SIF. The corresponding fault tree can be as shown below.



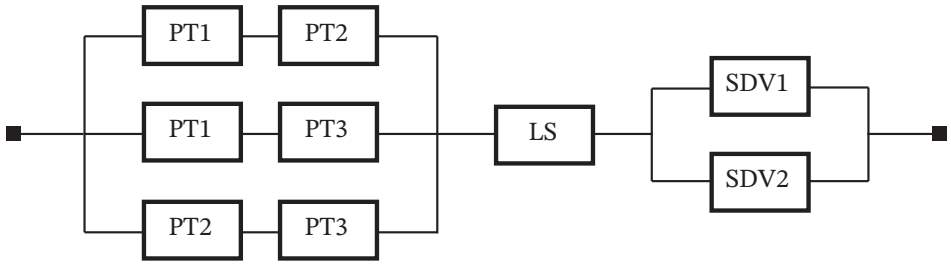
We can from this small fault tree identify the following cut sets:

$$
\begin{aligned}
C_1 &= \{PT1, PT2\} \\
C_2 &= \{PT1, PT3\} \\
C_3 &= \{PT2, PT3\} \\
C_4 &= \{LS\} \\
C_5 &= \{SDV1, SDV2\}
\end{aligned}
$$

With larger and more complex fault trees we need to use special tools (implementing algorithms for extraction) of minimal cut sets.

Comparison with Reliability Block Diagram

The system on the previous slide may also be represented by reliability block diagram, as seen below.



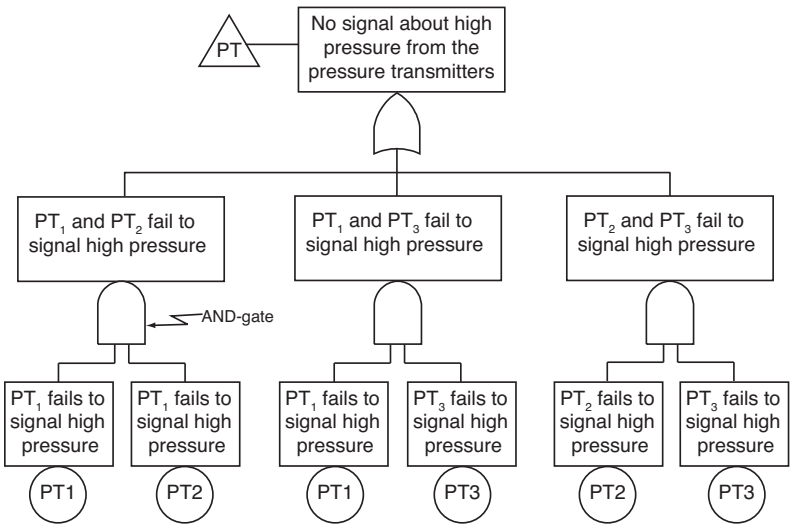
With this simple structure, we identify easily the same minimal cut sets (denoted C_i):

$$
\begin{aligned}
C_1 &= \{PT1, PT2\} \\
C_2 &= \{PT1, PT3\} \\
C_3 &= \{PT2, PT3\} \\
C_4 &= \{LS\} \\
C_5 &= \{SDV1, SDV2\}
\end{aligned}
$$

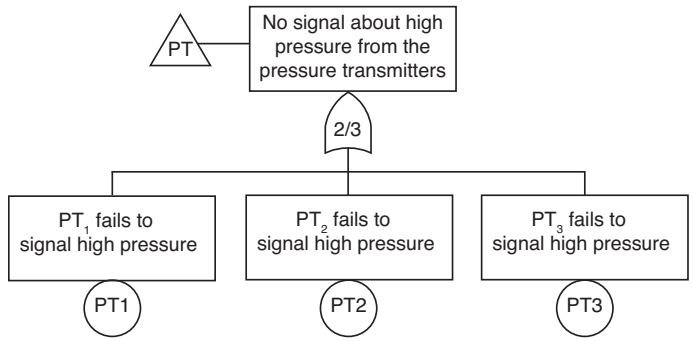
Fault Tree Symbols for *koon* Systems

The fault tree structure below indicates that the subsystem of pressure transmitters are voted 2oo3.

Original structure:



Modified with gate symbol for *koon*:



Note that the k/n gate is $(n-k+1)/n$ if it represents the failure of *koon* system.

Qualitative Analysis

Qualitative analysis of the fault tree may include:

- Analysis of minimal cut sets, including:
  - To identify and verify any single points of failure?
  - To identify that other main contributors (e.g. for minimal cutsets up to order 3) seem correct
- Common cause and dependency analysis:
  - This may include to check if logical events connected by local AND-gates are independent
  - Review minimal cut sets up to e.g order 3 to check if there are dependencies and if they must be modelled

Quantitative Analysis

- The TOP event occurs if one of the minimal cut sets occurs
- The main challenge is therefore to identify the minimal cut sets
- If all minimal cut sets were independent, we could calculate the the probability of the top event by:

$$Q_0(t) = 1 - \prod_{j=1}^{k} [1 - \check{Q}_j(t)]$$

where $Q_j(t)$ is the failure probability of minimal cut set C_j:

$$\check{Q}_j(t) = \prod_{i \in C_j} q_i(t)$$

Upper Bound Approximation

- In reality, the minimal cut sets will not (normally) be independent, since the same basic event may belong to the several minimal cut sets.
- This type of dependency is called *positive dependency*, which increases the reliability.
- This "double counting" of basic events results in a higher failure probability of the TOP event, and consequently, we can claim that "true" TOP event failure probability will be lower than:

$$Q_0(t) \quad \leq \quad 1 - \prod_{j=1}^{k} [1 - \check{Q}_j(t)]$$

and we can therefore use this formula as a conservative approximation for the calculations.

Failure Probabilities at Basic Event Level

Consider the state of the basic event i, E_i. The choice of failure probability is dependent on the following factors:

- Alternative 1: The item is in continuous operation and non-repairable.

  In this case we may be interested in the probability that item i has failed at time t, $q_i(t)$,which is:

  $$q_i(t) = Pr[E_i(t)] = Pr(T < t)$$

  If we assume exponential time to failure, $q_i(t)$ becomes:

  $$q_i(t) = 1 - e^{-\lambda_i t}$$

Failure Probabilities at Basic Event Level

- Alternative 2: The item is in continuous operation and repairable.

  We assume that the item runs to failure and is then repaired. In this case, we may want to determine the mean unavailability of the item:

$$q_i = \frac{MTTR_i}{MTTF_i + MTTR_i} \approx \lambda_i MTTR_i$$

  where MTTR_i is the mean time after the failure, and MTTF_i is the mean time to failure.

  Note that we here have assumed (again) exponentially distributed time to failure so that $1/MTTF_i = \lambda_i$

Failure Probabilities at Basic Event Levels

- Alternative 3: The item is normally passive and therefore subject to regular testing and repair.

  In this case, we may want to choose the mean unavailability or mean downtime due to a hidden failure:

$$\begin{aligned} q_i &= \frac{\lambda_i \tau}{2} + \Pr(\text{Failure found}) \cdot \text{Mean repair time} \\ &\approx \frac{\lambda_i \tau}{2} + \lambda_i \tau \frac{MRT_i}{\tau} \end{aligned}$$

- Note that λ_i in this case represents the dangerous undetected (DU) failures, and that the mean down time due to other failure categories may need to be added in addition.

Inclusion of Common Cause Failures (CCFs)

There are mainly three strategies to modeling CCFs in relation to fault tree analysis:

1. Include in FT (explicit): Model each CCF cause as a separate basic event that may lead to the failure of several items
2. Include in FT (implicit): Model a CCF as a basic event that covers several causes that may lead to the failure of several items
3. Exclude from FT: Add the contribution from CCFs in the quantification after the minimal cut sets have been extracted.

The last option may be favorable when the system complexity is high, and where dependency may exist between basic events at different levels and section of the fault tree.

Important Measures

Several importance measures have been developed to measure the relative importance of basic events. One of particular importance is the *Birnbaum* measure, where the relative importance of basic event i is measures by:

$$I^B(i|t) = \frac{\delta Q_0(t)}{\delta q_i(t)}$$

This may also be calculated more easily as:

$$I^B(i|t) = Q_0(t|E_i(t) = 1) - Q_0(t|E_i(t) = 0)$$