Chapter 8.
Calculation of PFD using 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:

- Present and discuss the application of fault tree analysis for calculating the PFD
  - First, with basis in the SIS text book
  - Second, with basis in a referenced paper ("procedure")[1]
- Highlight some of the challenges related to using (some) commercial software

The slides include topics from Chapter 8 in **Reliability of Safety-Critical Systems: Theory and Applications**. DOI:10.1002/9781118776353.

[1] Reliability assessment of safety instrumented systems in the oil and gas industry: A practical approach and a case study by Lundteigen, M.A. and Rausand, M., The International Journal of Reliability, Quality and Safety Engineering (IJRQSE) Vol. 16 (2009), see `http://dx.doi.org/10.1142/S0218539309003356`

Outline of Presentation

1. Introduction
2. FTA Basics
3. PFD basics
4. Beyond SIS Textbook
5. Procedure
6. Reflections

Application and Characteristics

Fault tree analysis (FTA) is a widely used and popular method for reliability analysis, and is suggested in IEC 61508 as a relevant approach for reliability analysis of SIS.

A more detailed introduction to the characteristics of FTA is found in chapter 5 of the SIS textbook

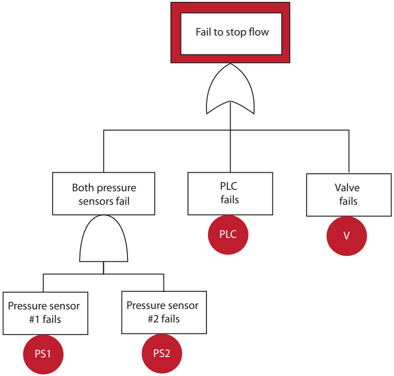
Fault Tree Analysis (FTA) - for SIS

Main elements of a fault tree:

- TOP event
- Gates (and, or, *koon*).
- Basic events
- Transfer symbols (triangles)

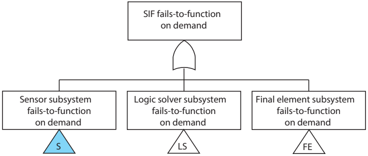
Typical TOP events for a SIS:

- TOP_1: The SIF cannot be performed (e.g., fail to stop flow upon demand)
- TOP_2: The SIF is activated spuriously (e.g., the stops flow when not demanded)



Fault tree analysis (FTA) - for SIS

A fault tree may be split into several sub-trees (sub-trees shown for sensor system, without and with CCFs included):



SIF fails-to-function on demand

Sensor subsystem fails-to-function on demand

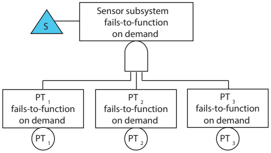
S

Logic solver subsystem fails-to-function on demand

LS

Final element subsystem fails-to-function on demand

FE



S

Sensor subsystem fails-to-function on demand

PT_1 fails-to-function on demand

PT_1

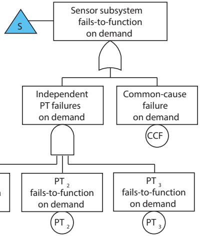
PT_2 fails-to-function on demand

PT_2

PT_3 fails-to-function on demand

PT_3

or



S

Sensor subsystem fails-to-function on demand

Independent PT failures on demand

Common-cause failure on demand

CCF

PT_1 fails-to-function on demand

PT_1

PT_2 fails-to-function on demand

PT_2

PT_3 fails-to-function on demand

PT_3

Fault tree for *koon* systems

A SIS is often split into subsystems, where each is voted *koon*. Each subsystem can be studied separately using the upper bound approximation

Consider a *koon* system:

- The system fails if $(n - k + 1)$ components fail.
- This implies that the minimal cutsets are of order $(n - k + 1)$.
- The number of minimal cut sets are $\kappa = \binom{n}{n-k+1}$.

Example

The number of minimal cutsets in a 2oo4 system is:

$$\binom{4}{3} = \frac{4!}{(4-3)!3!} = \frac{4 \cdot 3 \cdot 2 \cdot 1}{1 \cdot 3 \cdot 2 \cdot 1} = 4$$

FTA versus RBD

When should we use FTA and when should we use a reliability block diagram (RBD)?

- With AND and OR gates, a FT can always be transferred to an RBD and visa verse.
- Some prefer failure oriented modeling, rather than success oriented.
- A RBD often aims for a structure that resembles the physical structure of the system. Many of the simplified formulas developed for RBDs assume that the system may be split into a series structure of subsystems, but this is not always possible for more complex systems.
- With FTA, we base the calculations on the minimal cutsets, and we do not need be concerned about how we model as long as we have algorithms to extract these.

Approach for calculating PFD

In FTA we may calculate the average PFD by:

- First finding the failure function $Q_0(t)$for the top event and then calculate the PFD average by:

$$\text{PFD}_{\text{avg}} = \frac{1}{\tau}\int_0^{\tau} Q_0(t)\,dt$$

- or, use the upper bound approximation using the minimal cut sets (MCSs)[2].

$$\text{PFD}_{\text{avg}} \leq 1 - \prod_{\text{j=0}}^{\kappa}(1 - \check{Q}_{j,avg})$$

- The latter approach is often preferred, but how shall the $\check{Q}_{j,avg}$ be calculated?

[2] Minimal cut sets: the sets that contain the least combinations of component failures that result in the TOP event

Calculation problem for *koon* system

Consider first the *koon* system with identical and independent components:

- The main approach for calculating the probability of a minimal cutset occuring in a time interval t, here referred to as $\check{Q}_j(t), j = 1 \ldots \kappa$, where $\kappa = \binom{n}{n-k+1}$ is:

$$\check{Q}_j(t) = \prod_{i=1}^{n-k+1} q_i(t)$$

  where $q_i(t)$ is the probability that component i fails in the time interval.

Calculation problem for *koon* system

Most software programs calculate the PFD *at the basic event level* rather than at the level of the minimal cutset.

$$\check{Q}_{j,avg} = \prod_{i=1}^{n-k+1} \mathrm{q}_{i,avg}$$

where $\mathrm{q}_{i,avg} = \frac{\lambda_{DU}\tau}{2}$. This means that:

$$\check{Q}_{j,avg} = \left(\frac{\lambda_{DU}\tau}{2}\right)^{n-k+1}$$

For comparison, the simplified formulas for a *koon* system has previously been found as:

$$\mathrm{PFD}_{avg}^{1oo(n-k+1)} = \frac{(\lambda_{DU}\tau)^{n-k+1}}{n-k+2}$$

This is not conservative since $n - k + 2 < 2^{n-k+1}$. Check for yourself for e.g. a1oo2 system.

Correction factor for minimal cut sets

The following correction factor (CF) may be used in relation to each minimial cut set, if the average failure probability in $(0, \tau)$ is calculated at the basic event level:

$$\mathrm{CF} = \frac{2^{n-k+1}}{n-k+2}$$

Minimal Cut Sets with Non-Identical Components

The slides beyond this point are not covered by the SIS textbook, but by the referenced paper.

Non-identical, but independent components

Consider a minimal cutset j with m_j[3] *independent* and non-identical components with test interval τ. The $\mathrm{PFD_{mcs,j}}$ of this minimal cut is

$$\begin{aligned}
\mathrm{PFD_{mcs,j}} &= \frac{1}{\tau}\int_0^\tau \prod_{i=1}^{m_j}\left(1 - e^{-\lambda_{\mathrm{DU},j,i}\cdot t}\right)\,dt \\
&\lessapprox \frac{1}{\tau}\int_0^\tau \prod_{i=1}^{m_j}\left(\lambda_{\mathrm{DU},j,i}\cdot t\right)\,dt = \frac{\left(\prod_{i=1}^{m_j}\lambda_{\mathrm{DU},j,i}\right)\cdot\tau^{m_j}}{m_j+1} \\
&= \frac{\left(\bar{\lambda}_{\mathrm{DU},j}\cdot\tau\right)^{m_j}}{m_j+1}
\end{aligned}$$

where

$$\bar{\lambda}_{\mathrm{DU},j} = \left(\prod_{i=1}^{m_j}\lambda_{\mathrm{DU},j,i}\right)^{\frac{1}{m_j}}$$

is the *geometric mean* of the m_j DU-failure rates $\lambda_{\mathrm{DU},j,1}, \lambda_{\mathrm{DU},j,2}, \ldots, \lambda_{\mathrm{DU},j,m_j}$.

[3] Assuming that there is a list of MCSs can have different dimensions

Example

For a minimal cut j of **two** independent components with failure rates $\lambda_{\mathrm{DU},j,1}$ and $\lambda_{\mathrm{DU},j,2}$, the average $\mathrm{PFD}_{\mathrm{MC}_j}$ is:

$$\mathrm{PFD}_{\mathrm{MC}_j} \lessapprox \frac{\lambda_{\mathrm{DU},j,1} \cdot \lambda_{\mathrm{DU},j,2} \cdot \tau^2}{3}$$

This is 3/4 of the non-conservative approximation ($\lambda_{\mathrm{DU},j,1} \cdot \lambda_{\mathrm{DU},j,2} \cdot \tau^2/4$). In general (for a 1oo$m_j$ voted configuration), the correction factor is:

$$\frac{2^{m_j}}{m_j + 1}$$

Modeling CCFs

Components are not always failing independent of each other, and we need to include the contribution from common cause failures (CCFs).

☞ Common cause failure (CCF): A dependent failure in which two or more component fault states exist simultaneously or within a short time interval, and are a direct result of a shared cause.

It is common to use the standard beta factor model in relation to fault tree analysis.

- Some minimal cutsets may constitute identical components
- More common is perhaps that they constitute some identical and some non-identical components

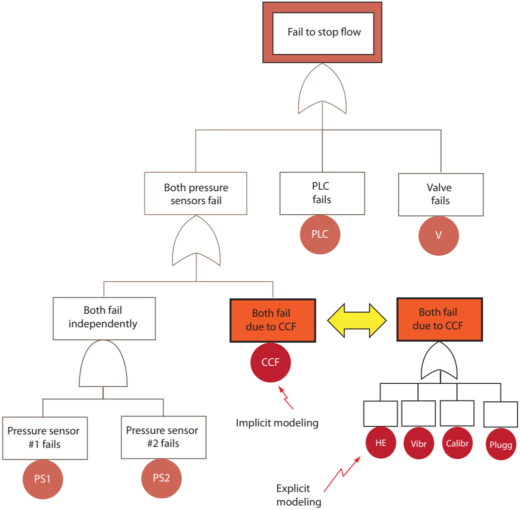
It is therefore not always straigt forward to find or determine representative values of beta.

Model CCFs as basic events into the FT

Common cause failures (CCFs) may be included in a fault tree by:

- Explicit modeling
- Implicit modeling

In this way, the MCSs will constitute independent as well as CCF events.



Post-Processing of CCFs

There are some arguments to why CCFs should be added in the post-processing of minimal cut sets, and not added as CCF basic events in the fault tree.

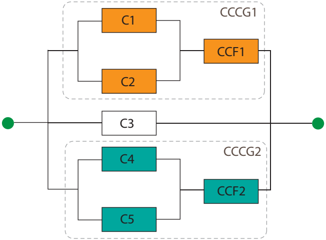
- In many cases, the minimal cut sets include basic events, with potential dependencies, from different sections of the FT. It is not obvious where and how CCFs should be added as basic events in the fault tree.
- Within the same minimal cut set, there may be some basic events that are dependent while others are independent. We may refer to this as minimal cut sets having different *internal dependencies*. This can be easier to evaluate, once the minimal cut sets have been derived.

Remark: A $koon$ gate (with $n > 1, k > 1$) in a fault tree generates $\binom{n}{n-k+1}$ minimal cut sets, but CCFs cannot be added to each of these using the assumption that *all* n components fail in a $koon$ system in case of a CCF.

Internal Dependencies

Illustration of the situation where a minimal cutset (MCS) has different *internal dependencies*:

- This MCS number has order 5 ({C1, C2, C3, C4, C5}) when considering independent failures only
- For CCFs, it s assumed that there are two sets ("common cause component groups, CCCG) of internal dependencies: CCCG_1 for {C1,C2} and CCCG_2 for {C4,C5}.



Procedure (based on article)

A procedure has been proposed for deriving at formulas for PFD_{avg}. The most important attributes of the approach are:

- Simplified formulas are used to calculate PFD_{avg} at the minimal cut set (MCS) level
- The existence of dependencies, including common cause component groups, are investigated after the MCSs have been generated, and the contribution of CCFs is added to each minimal cut set using the standard beta factor model

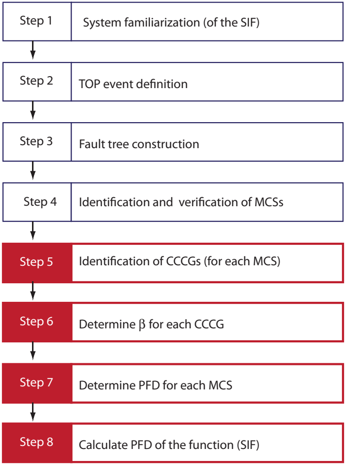
Note that steps 5-8 are covered here, and reference is made to the referenced paper about the content of the other steps.

Terminology

The following terms are used:

- Common cause component group (CCCG): A collection of basic events in a MCS where there exists a shared dependency. The same MCS may have more than one CCCG.

Procedure steps



Step 1 System familiarization (of the SIF)

Step 2 TOP event definition

Step 3 Fault tree construction

Step 4 Identification and verification of MCSs

Step 5 Identification of CCCGs (for each MCS)

Step 6 Determine β for each CCCG

Step 7 Determine PFD for each MCS

Step 8 Calculate PFD of the function (SIF)

Note: Only the steps colored red (steps 5-8) are covered in the following slides.

Step 5: Identification of CCCGs

Step 5 concerns the identification of the CCCFs for each MCS$_j$.

- Look for potential **coupling factors** among components in the MCS, and place components that share a coupling factor in the *same* CCCG.
- For each CCCF$_i$ in MCS$_j$, define a CCF-event CCF$_i$.
- Determine a value for a beta factor for each CCF$_i$, by using data sourses, checklists, or expert judgment. In case of expert judgments, it is important to identify possible root causes for the coupling factors, and evaluate how likely they are or have been to occur.

Often and in practice, only one CCCG is defined for each MCS since it may be difficult to support each CCCG by separate CCF data. Several guidelines and standards include checklists for root causes and coupling factors.

Step 6: Determine β for each CCCG

Step 6 aims to determine the value of β_i for each CCCG$_i$, $i = 1 \ldots k$. Applicable approaches are::

- Checklists
- Expert judgments
- Estimation

Expert judgments is for example used in the OLF 070 guideline, whereas checklists may be found in IEC 61508, part 6, Unified Partial Method (UPM), and in an article by Humphreys, R. A. (1987). The latter approach may need to be calibrated in light of current state of the art technology.

Step 7: Determine PFD for each MCS

Step 7 is used to calculate the PFD_{avg} for each MCS_j. The PFD_{MC_j} is influenced by:

- The order m_j of the minimal cut.
- Whether or not the components of the minimal cut are identical .
- Whether or not the components of the minimal cut are dependent .
- Whether or not the components of the minimal cut are tested simultaneously .

Three alternatives have been introduced:

- Alternative 1: Identical and independent.
- Alternative 2: Identical and dependent, with one CCCG.
- Alternative 3: Non-identical and dependent, with one CCCG.
- Alternative 4: More complex, with more than one CCCG.

Step 7: Determine PFD for each MCS

Alternative 1: Independent components with failure rates $\lambda_{\mathrm{DU},j,1}, \lambda_{\mathrm{DU},j,2}, \ldots, \lambda_{\mathrm{DU},j,m_j}$:

- We may then use the formulas:

$$\begin{aligned}
\mathrm{PFD}_{\mathrm{MC}_j} &= \frac{1}{\tau}\int_0^{\tau} \prod_{i=1}^{m_j} \Big(1 - \exp(-\lambda_{\mathrm{DU},j,i} \cdot t\Big)\; dt \\
&\lessapprox \frac{1}{\tau}\int_0^{\tau} \prod_{i=1}^{m_j} \Big(\lambda_{\mathrm{DU},j,i} \cdot t\Big)\; dt = \frac{\Big(\prod_{i=1}^{m_j} \lambda_{\mathrm{DU},j,i}\Big) \cdot \tau^{m_j}}{m_j + 1} \\
&= \frac{\Big(\bar{\lambda}_{\mathrm{DU},j} \cdot \tau\Big)^{m_j}}{m_j + 1}
\end{aligned}$$

where

$$\bar{\lambda}_{\mathrm{DU},j} = \left(\prod_{i=1}^{m_j} \lambda_{\mathrm{DU},j,i}\right)^{\frac{1}{m_j}}$$

Step 7: Determine PFD for each MCS

Alternative 2: Identical and dependent components:

- Consider a minimal cut with m_j identical and dependent components with DU failure rate $\lambda_{\mathrm{DU},j}$ and beta factor β_j
- Assume that all the components of the minimal cut are tested simultaneously with test interval τ

The PFD for this structure, $\mathrm{PFD}_{\mathrm{MC}_j}$, then becomes :

$$\mathrm{PFD}_{\mathrm{MC}_j} \lessapprox \frac{\left((1-\beta_j)\lambda_{\mathrm{DU},j}\cdot\tau\right)^{m_j}}{m_j+1} + \frac{\beta_j\lambda_{\mathrm{DU},j}\cdot\tau}{2}$$

Step 7: Determine PFD for each MCS

Alternative 3: Non-identical and dependent components:

- Example: A temperature transmitter and a pressure transmitter, located in the same area, can be vulnerable to vibration
- Problem: What β should we choose?
  - Geometric mean: Ok, as long as the failure rates are not too different in magnitude
  - If they are, the CCF rate may be greater than the *lowest* failure rate of the components being considered[4]
  - Instead, we choose beta as a fraction of the lowest component failure rate

[4] Which is unrealistic when we assume the standard beta factor model

Step 7: Determine PFD for each MCS

Alternative 3 (continued):

- $\mathrm{PFD}_{\mathrm{MCS}_j}$ then becomes:

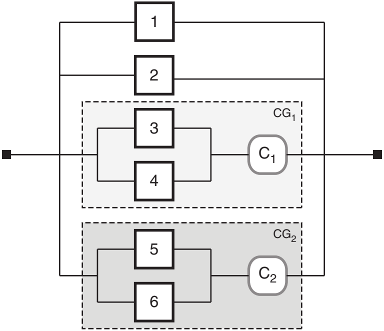
$$\mathrm{PFD}_{\mathrm{mcs,j}} \approx \frac{\left[\left(1-\beta_j\right)\bar{\lambda}_{\mathrm{DU},j}\cdot\tau\right]^{m_j}}{m_j+1}+\frac{\beta_j\lambda_{\mathrm{DU},j}^{\min}\tau}{2}$$

where $\lambda_{\mathrm{DU},j}^{\min}=\min_{i\in\mathrm{mcs,j}}\{\lambda_{\mathrm{DU},j,i}\}$ is the lowest DU failure rate in MC_j.

Step 7: Determine PFD for each MCS

Alternative 4: More complex MCSs (i.e., with more than one CCCG per MCS)

- A MCS may have more than one CCCG
- In the illustration below, the MCS may have order 4, 5, and 6



Step 7: Determine PFD for each MCS

Alternative 4 (continued):

- It is usually sufficient to calculate the PFD for the (virtual) cut set with the lowest order
- In the illustration on the previous frame, this is for $\{1, 2, \mathrm{C}_1, \mathrm{C}_2\}$

We then get (the index j has been omitted):

$$\mathrm{PFD}_{\mathrm{MC}}^{(1)} \approx \frac{\left(\lambda_1^{(I)}\lambda_2^{(I)}\beta_1\beta_2\lambda_{\mathrm{DU}}^{\mathrm{min},1}\lambda_{\mathrm{DU}}^{\mathrm{min},2}\right)\tau^4}{5}$$

The PFD for the MCS, considering all 'virtual cuts' is:

$$\mathrm{PFD}_{\mathrm{MC}_j} \approx 1 - \prod_{\mathrm{All``virtual''cuts}\ k} \left(1 - \mathrm{PFD}_{\mathrm{MC}_j}^{(k)}\right)$$

Step 8: Determine PFD of the SIF

The formula for calculating the PFD of the safety instrumented function (SIF), taking all the MCSs into account, is also based on the upper bound approximation:

$$\mathrm{PFD}_{\mathrm{SIF}} \lessapprox 1 - \prod_{j=1}^{m} \left(1 - \mathrm{PFD}_{\mathrm{MC}_j}\right)$$

Example application

The application of the procedure is demonstrated for a workover control system in the referenced article (Lundteigen and Rausand, 2009).

Pros/Cons

Pros:

- Using MCS as basis for modeling CCFs may be advantageous where the fault trees are very large and where components, with potential dependencies, may end up in very different sections of the tree.
- The conservative approximation formulas are already well known by reliability analysts

Cons:

- Some more manual effort is needed (but this effort may be worth while taking to better understand the system)
- Care must be taken when using *koon* gates in FT, to avoid that the contribution from CCFs are not added more than once.