Chapter 8.
PFD formulas in IEC 61508

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:

- Introduce and explain the simplified formulas in IEC 61508, part 6 for calculating the average probability of failure on demand (PFD$_{avg}$)
- Introduce and discuss some of the related concepts and assumptions

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

Outline of Presentation

1. Introduction
2. General Assumptions for Analytical Formulas in IEC 61508
3. Equivalent Mean Downtime
4. Group failure frequency
5. PFD formulas
6. Inclusion of CCFs
7. Markov

Remark

IEC 61508 formulas may be explained in different ways, and the approach selected in the following slides is not the only one. A more thorough explanation of background for formulas in IEC 61508 is provided by Dr. Fares Innal in his PhD thesis:

- Innal, F. (2008) *Contribution to modeling safety instrumented systems and to assessing their performance. Critical analysis of IEC 6|508 standard.* PhD thesis. University of Bordeaux, Bordeaux, France.

General Assumptions

IEC 61508 (part 6) presents simplified formulas for selected voted configurations, derived with basis in the following assumptions:

$$PFD_{\text{avg}}^{(G)} = \lambda_{D,G} t_{GE}$$

where $\lambda_{D,G}$ is the Group failure frequency of dangerous failures, $\lambda_{D,G}$ and t_{GE} is the Group-equivalent mean downtime. Assumptions underlying formulas:

- Any parallel structure of channels constitutes *identical* components.
- Time to failure and repair times are exponentially distributed.

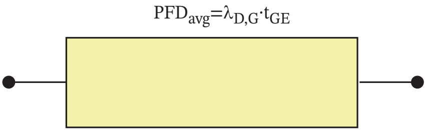
Visualization I: RBD

Recall that the average unavailability. $\overline{A}_{avg}$, (from Chapter 5) of a system could be expressed as:

$$\overline{A}_{avg} = \lambda_S \cdot MDT_S$$

where the system is represented by as "super item" with failure rate λ_S mean downtime MDT_S.

In IEC 61508 formulas, $\overline{A}_{avg}$ corresponds to PFD$_{\text{avg}}$, λ_S to $\lambda_{D,G}$ and MDT_S to t_{GE}.


$\text{PFD}_{\text{avg}}=\lambda_{\text{D,G}}\cdot \text{t}_{\text{GE}}$

Equivalent mean downtimes

IEC 61508 refers to t_{GE} as the **equivalent mean downtime**.

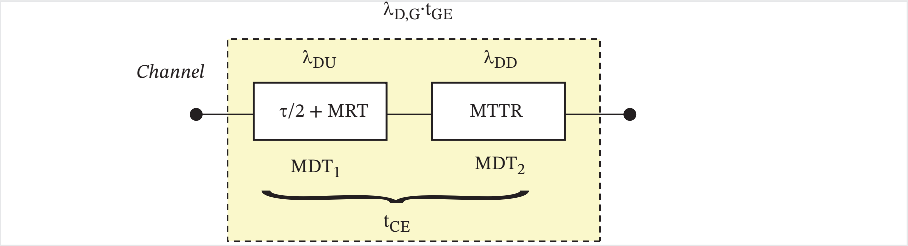
There are three **main categories** of equivalent mean downtimes:

- Channel equivalent mean downtime, t_{CE}, calculated for a single dangerous (D) failure
- Group equivalent mean downtime (while system in the failed state), t_{GE}, calculated for the lowest combination of D failures that result in system failure
- Group equivalent downtime in degraded mode, t_{GjE} for $j = 1..n - k$, associated with any multiplicity of D failures $j < n - k + 1$

Note that for $j = 1$ (i.e. for single channel), we use t_{CE} as the notation instead of t_{G1E}.

Example: Single System

For a single channel, the super-item may be split up into **two sub-items**, representing the failure rate and the associated conditional mean downtime, t_{CE}, for DU and DD failures.



We note that:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{2} + \text{MRT}\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot \text{MTTR}$$

where $\lambda_D = \lambda_{DU} + \lambda_{DD}$

Formulas for Equivalent Mean Downtimes

Channel equivalent mean downtime, t_{CE}:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

Group equivalent mean downtime, t_{GE}:

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{n-k+2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

Group equivalent mean downtime in degraded mode, $t_{GjE}, j = 2..(n-k)$[1]:

$$t_{GjE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{j+1} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

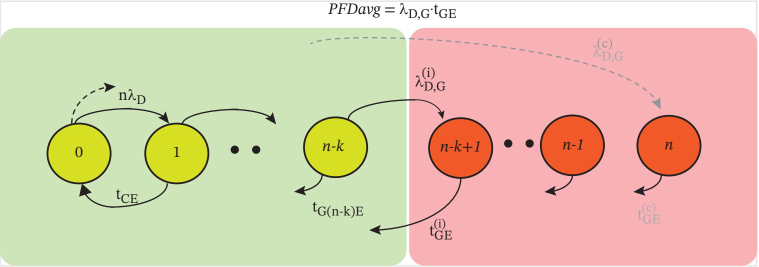
For the group we assume that the downtime of DD failures is not affected by how many channels being down.

[1] We skip $j = 1$, since we use $\mathrm{t_{CE}}$

Visualization II: Markov

Visualization using Markov (see illustration below):

- Recall that a *koon* system fails when $n - k + 1$ up to n components fail.
- The largest contributor to unavailability is the state corresponding to the $(n - k + 1)$ (considering independent failures) and state corresponding to nth failure in case of CCFs
- An *approximation* for PFD_{avg} would therefore be the average time spent in these states. The question is how to quantify $\lambda_{\text{D,G}}$ and t_{GE}.

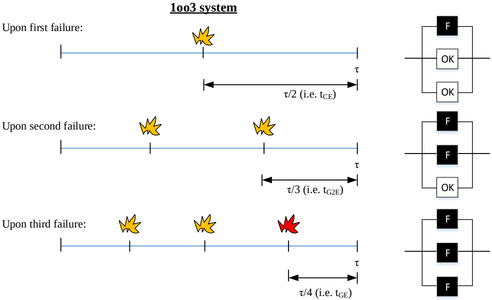


Explanation for DU failures: 1oo3 voted system

This system can experience from one to three failures

- The first DU failure will on the average be down $\tau/2$
- The second DU failure will on the average be down $\tau/3$
- The third DU failure will on the average be down $\tau/4$

..assuming equal distribution. This can be illustrated as follows:



Dangerous group frequency, $\lambda_{D,G}$

The dangerous group frequency, $\lambda_{D,G}$, is the average system failure rate.

This means that $\lambda_{D,G}$ is:

- ...the sum of all transitions into a failed state (corresponding to states $n - k + 1, \ldots, n$ in a *nook* system
- ...dominated by the transitions into the $(n - k + 1)$th state for independent failures
- ...dominated by the transition into the nth state for CCFs (standard beta factor model)

How to Determine $\lambda_{D,G}$? 1oo2 system

Consider a 1oo2 system with identical and independent channels with failure rate λ_D. As the channels are independent, they will not fail at exactly the same time.

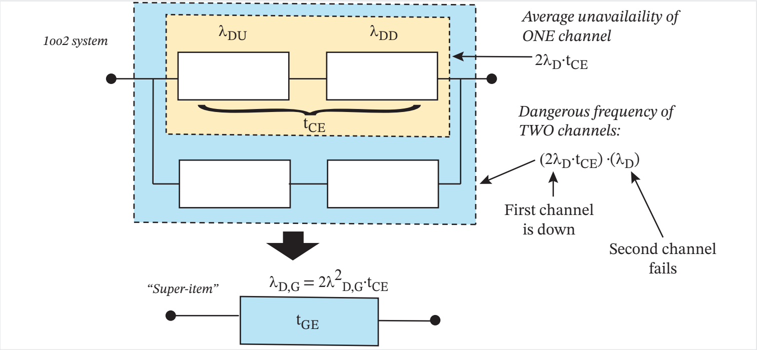
- The first D failure occurs with rate $2\lambda_D$, since any of the two components may fail first. The mean downtime of a single channel is t_{CE}.
- A *dangerous group failure* occurs if the second channel fails while the first channel is unavailable.

This means that the group failure rate for a 1oo2 system is:

$$\lambda_{D,G}^{(1oo2)} \approx (2\lambda_D t_{CE}) \cdot \lambda_D = 2\lambda_D^2 t_{CE}$$

Illustration: 1oo2 System

The creation of super-item for a 1oo2 system is illustrated below:


1oo2 system
λ_{DU}
λ_{DD}
t_{CE}
Average unavailaility of ONE channel
$2\lambda_D \cdot t_{CE}$
Dangerous frequency of TWO channels:
$(2\lambda_D \cdot t_{CE}) \cdot (\lambda_D)$
First channel is down
Second channel fails
"Super-item"
$\lambda_{D,G} = 2\lambda^2_{D,G} \cdot t_{CE}$
t_{GE}

Note that t_{CE} is as before and $t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{3} + \text{MRT}\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot \text{MTTR}$

How to Determine $\lambda_{D,G}$? 2oo3 System

For a 2oo3 system with identical and independent channels with failure rate λ_D, we may assume that:

- The first (D) failure occurs with rate $3\lambda_D$, since any of the three components may fail first. This first channel is down t_{CE}
- A dangerous group failure occurs when a **second channel fails** while first channel is unavailable.

This means that:

$$\lambda_{D,G}^{(2oo3)} \approx (3\lambda_D \cdot t_{CE}) \cdot (2\lambda_D) = 6\lambda_D^2 \cdot t_{CE}$$

How to Determine $\lambda_{D,G}$? 1oo3 System

For a 2oo3 system with identical and independent channels with failure rate λ_D, we may assume that:

- The first (D) failure occurs with rate $3\lambda_D$, since any of the three components may fail first. This first channel is down t_{CE}
- The second (D) failure occurs with rate $2\lambda_D$, since any of the two remaining components may fail. This second channel is down t_{G2E}
- A dangerous group failure when a **third channel fails** while two are already failed.

This means that:

$$\lambda_{D,G}^{(1oo3)} \approx (3\lambda_D \cdot t_{CE}) \cdot (2\lambda_D t_{G2E})\,(\lambda_D) = 6\lambda_D^3 \cdot t_{CE} \cdot t_{G2E}$$

What is $\lambda_{D,G}$? *koon* system

Now consider a *koon* system.

- The first failure occurs with rate $n\lambda_D$. The probability that the second failure occurs while the first one is down is $(n-1)\lambda_D t_{CE}$, the probability that a third failure occurs while two are down is $(n-2)\lambda_D t_{GE2}$, and so on till the group failure (involving n-k+1 failures) occurs with probability that $(n-k+1)\lambda_D t_{GE(n-k)}$.

$$\lambda_{D,G}^{(koon)} \approx \lambda_D^{n-k+1} k \prod_{j=1}^{n-k} (n-j+1) t_{GjE}$$

where t_{GjE} is the equivalent downtime due to the jth failure:

$$t_{GjE} = \frac{\lambda_{DU}}{\lambda_D}(\frac{\tau}{j+1} + MRT) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

Note that t_{G1E} is what we previously have defined as t_{CE}.

What is $\lambda_{D,G}$? Example equations

The equation developed for *koon* may be used to set up the equations for specific combinations of k and n:

k/n	Group failure frequency
1oo1	λ_D
1oo2	$2\lambda_D^2 t_{CE}$
1oo3	$6\lambda_D^3 t_{CE} t_{G2E}$
2oo3	$6\lambda_D^2 t_{CE}$
1oo4	$24\lambda_D^4 t_{CE} t_{G2E} t_{G2E}$
2oo4	$24\lambda_D^3 t_{CE} t_{G2E}$

What is PFD$_{\text{avg}}$?

Recall that the general equation for PFD$_{\text{avg}}$ was:

$$PFD_{\text{avg}} = \lambda_{D,G} t_{GE}$$

We may expand this equation for a selection of systems:

k/n	PFD_{avg}	t_{GE}
1oo1	$\lambda_D \mathbf{t_{GE}}$	$\frac{\lambda_{DU}}{\lambda_D}(\frac{\tau}{2} + MRT) + \frac{\lambda_{DD}}{\lambda_D} MTTR$
1oo2	$2\lambda_D^2 t_{CE} \mathbf{t_{GE}}$	$\frac{\lambda_{DU}}{\lambda_D}(\frac{\tau}{3} + MRT) + \frac{\lambda_{DD}}{\lambda_D} MTTR$
1oo3	$6\lambda_D^3 t_{CE} t_{G2E} \mathbf{t_{GE}}$	$\frac{\lambda_{DU}}{\lambda_D}(\frac{\tau}{4} + MRT) + \frac{\lambda_{DD}}{\lambda_D} MTTR$
2oo3	$6\lambda_D^2 t_{CE} \mathbf{t_{GE}}$	$\frac{\lambda_{DU}}{\lambda_D}(\frac{\tau}{3} + MRT) + \frac{\lambda_{DD}}{\lambda_D} MTTR$
1oo4	$24\lambda_D^4 t_{CE} t_{G2E} t_{G3E} \mathbf{t_{GE}}$	$\frac{\lambda_{DU}}{\lambda_D}(\frac{\tau}{5} + MRT) + \frac{\lambda_{DD}}{\lambda_D} MTTR$
2oo4	$24\lambda_D^3 t_{CE} t_{G2E} \mathbf{t_{GE}}$	$\frac{\lambda_{DU}}{\lambda_D}(\frac{\tau}{4} + MRT) + \frac{\lambda_{DD}}{\lambda_D} MTTR$

Inclusion of CCFs

IEC 61508 includes the contribution from CCFs due to DU as well as DD failures using the standard beta factor model.

- The fraction of the DD failure rate that is CCFs is denoted β_D:

$$\lambda_{DD}^{(i)} = (1 - \beta_D)\lambda_{DD} \text{ and } \lambda_{DD}^{(c)} = \beta_D \lambda_{DD}$$

- The fraction of the DU failure rate that is CCFs is denoted β

$$\lambda_{DU}^{(i)} = (1 - \beta)\lambda_{DU} \text{ and } \lambda_{DU}^{(c)} = \beta \lambda_{DU}$$

Inclusion of CCFs

CCFs are included as a virtual functional block in the reliability block diagram, one for the CCFs associated with DD failures and one for CCFs associated with DU failures.

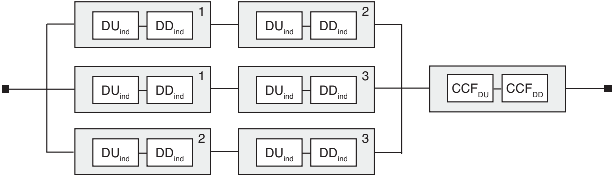


Figure: A RBD of a 2oo3 system with CCFs included

Inclusion of CCFs

Because CCFs are represented by single functional blocks, it is rather straight forward to set up the contribution toPFD$_{\text{avg}}$ from CCFs (note that $\lambda_D^{(c)} = \lambda_{DU}^{(c)} + \lambda_{DD}^{(c)}$:

$$
\begin{aligned}
PFD_{\text{avg}}^{CCF} &= \lambda_D^{(c)} t_{CE}^{(c)} = \lambda_D^{(c)} \left[\frac{\lambda_{DU}^{(c)}}{\lambda_D^{(c)}} \left(\frac{\tau}{2} + \text{MRT} \right) + \frac{\lambda_{DD}^{(c)}}{\lambda_D^{(c)}} \text{MTTR} \right] \\
&= \beta \lambda_{DU} \left(\frac{\tau}{2} + \text{MRT} \right) + \beta_D \lambda_{DD} \text{MTTR}
\end{aligned}
$$

The contribution to PFD from the independent part remains as before, except that the fraction $(1 - \beta)$ and $(1 - \beta_D)$ must be extracted for the DU and DD failure rate respectively.

Inclusion of CCFs: Example

Consider a 1oo3 system of identical components that may be subject to CCFs.

- The $\mathrm{PFD}_{\mathrm{avg}}$ becomes:

$$
\begin{aligned}
PFD_{\mathrm{avg}} &= 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^3 t_{CE}^{(i)} t_{GE2}^{(i)} t_{GE}^{(i)} \\
&+ \beta_D \lambda_{DD} \mathrm{MTTR} + \beta \lambda_{DU}\left(\frac{\tau}{2} + MRT\right)
\end{aligned}
$$

IEC formulas using Markov approach

The same formulas may be derived using Markov methods, (or more precisely using approximate Markov steady state models based on multiphase Markov models).

Consider figure 3.19 in Fares Innal master thesis. This diagram can be modified for different architectures, but this one is used to illustrate derivation of formula for a $x$oo3 system.

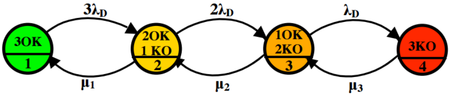


Figure 3.19: Approached Markov model relating to 1oo3 architecture

Figure: Source: F. Innal PhD thesis (2008)

Note: The repair/restoration rates (μ_i) are not all going back to state 1. For the approximations on the next slide, the result would be the same once truncated.

IEC formulas using Markov approach

For a 1oo3 system, the PFDavg corresponds to the steady state probability of state 4:

$$PFD_{avg} = P_4(\infty) = \frac{6{\lambda_D}^3}{6\,{\lambda_D}^3 + 6\,{\lambda_D}^2\mu_3 + 3\,\lambda_D\mu_2\mu_3 + \mu_1\mu_2\mu_3} \approx \frac{6{\lambda_D}^3}{\mu_1\mu_2\mu_3}$$

For a 2oo3 system, the PFDavg corresponds to the steady state probability of state 3 and 4 (but probability of state 3 is the dominating):

$$PFD_{avg} \approx P_3(\infty) = \frac{6{\lambda_D}^2\mu_3}{6\,{\lambda_D}^3 + 6\,{\lambda_D}^2\mu_3 + 3\,\lambda_D\mu_2\mu_3 + \mu_1\mu_2\mu_3} \approx \frac{6{\lambda_D}^2}{\mu_1\mu_2}$$

Note: These equations may be time consuming to derive by hand. Here, the software *Maple* was used to derive symbolic equations.

Meaning of μ_i

The meaning of μ_i is identical to the meaning of t_{GEi}:

- $\mu_1 = t_{G1E} = t_{CE}$
- $\mu_2 = t_{G2E}$ (which is t_{GE} for 2oo3 system)
- $\mu_3 = t_{G3E}$(which is t_{GE} for 1oo3 system)

Remarks:

- t_{CE} is always used when the equivalent mean downtime concerns a single channel
- t_{GE} is always used when the equivalent mean downtime concerns the whole group (at (n-k+1)th failure)
- t_{GjE} is otherwise used to represent multiple failures up to the (n-k)th failures.