Chapter 8.
Calculation of PFD using RBD

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:

- Define and clarify the underlying assumptions of (the average) *probability of failure on demand* (PFD)
- Explain the derivation of simplified formulas for PFD using reliability block diagrams (RBDs)
- Introduce some extensions to the simplified formulas

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. Background
3. PFD_{avg}
4. Simplified formulas
5. CCFs
6. Repair&Test Time
7. Staggered

Application of $\mathrm{PFD}_{\mathrm{avg}}$

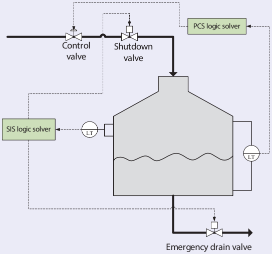
$\mathrm{PFD}_{\mathrm{avg}}$ is the preferred measure when:

- the SIF operates in the low-demand mode (with demands occuring less than once per year)
- the SIF operates independently of the EUC control system (and if relevant, any other SISs installed).

Example

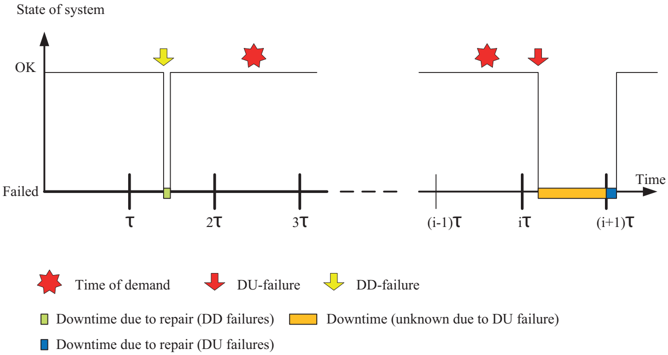
Consider a storage tank equipped with an EUC control system that controls the rate of filling:

- A failure of the EUC control system (e.g., a spurious opening of the control valve) may result in an overfilling
- A SIS may be installed to prevent overfilling. A dedicated level transmitter, logic solver and valve(s) are used for this purpose.



Consequences of SIS Failure

A failure of a SIS may not necessarily have any consequences, unless a demand occurs. The consequences of SIS failure is therefore conditional on the situation.


State of system
OK
Failed
Time
τ
2τ
3τ
(i-1)τ
iτ
(i+1)τ
Time of demand
DU-failure
DD-failure
Downtime due to repair (DD failures)
Downtime (unknown due to DU failure)
Downtime due to repair (DU failures)

It is thereforre important to regularly check (or test) if a DU failure is present, to reduce the risk of having unrevealed (DU) failures.

Possible Scenarious

In a time interval $(0, \tau)$, we may foresee the following scenarios:

- **No dangerous failure (DU or DD) in time interval:**
  Test time is main contributor to downtime.
- **A DD failure occurs in the time interval**:
  The SIS is in a failed state in a short period. Detection time is negligible, and main contributor to downtime is the restoration time, including start-up. Restoration time may, on the average, be a few hours if the access to the equipment is adequate and spare parts are available.
- **A DU failure occurs in the time interval:**
  The SIS may be in a failed state for a considerable time, as it may be unrevealed until the next demand or test (what ever comes first).

Known vs. Unknown Unavailability

The scenarios described can be used to distinguish between the following two contributors to unavailability:

- **Unknown** unavailability, meaning we are not aware of the unavailability:

  A DU failure has occurred, but it has not yet been revealed.

- **Known** unavailability, meaning that we *are* aware of the unavailability:

  A DD failure has occurred, or the SIS is down for repair or for scheduled testing.

How Often Does a DU Failure Occur?

Most tests will pass without any failure DU failure detected (if not, we do not have a reliable safety system). But how can we determine how many?

Consider a single component with failure rate $\lambda_{\text{DU}} = 2.0 \cdot 10^{-6}$ failures per hour, and that it is tested once a year (i.e. $\tau = 8760$ hours)

- The mean number of test intervals, E(Z), until a DU failure occurs is:

  $$E(Z) = \frac{R(\tau)}{F(\tau)}$$

  where $R(\tau) = e^{-\lambda_{\text{DU}}\tau} \approx 9.83 \cdot 10^{-2}$ and $F(\tau) = 1 - R(\tau)$.

This means that approximately 56 intervals (or 56 years when τ is 1 year) will past before the first DU failure occur.

This result was calculated for only one component. At an installation, there may be several components of the same type. If there are e.g. 25 components, one may expect a failure in a test around once every second year.

Interpretations of PFD$_{\text{avg}}$

The average probability of failure on demand (PFD$_{\text{avg}}$) may be defined in two ways:

1. The average probability that a SIF is not able to respond if demanded
2. The mean fractional downtime of a SIF in a test interval

Some remarks:

- The PFD is not dependent on the demand rate as such, so the ”able to function on demand” is slightly misleading
- The PFD may include known as well as unknown unavailability. Known unavailability is only included if the EUC continues to operate while the repair is ongoing.

Basic Formulas

The calculation of PFD$_{\text{avg}}$ starts with the time dependent solution.

- PFD(t): The probability that a SIF, a SIF subsystem, or subsystem element is in the failed state at time t:

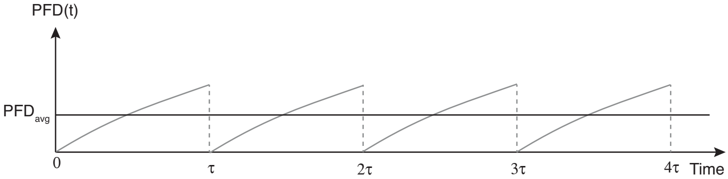
$$PFD(t) = \Pr(T \leq t) = F(t) = 1 - R(t)$$

- PFD$_{\text{avg}}$: The *average* probability of a SIF, SIF subsystem, or subsystem element not being able to perform as required in a time interval, usually the proof test interval (denoted τ).

$$PFD_{\text{avg}} = \frac{1}{\tau}\int_0^{\tau} PFD(t)\,dt = \frac{1}{\tau}\int_0^{\tau} F(t))\,dt = 1 - \frac{1}{\tau}\int_0^{\tau} R(t)\,dt$$

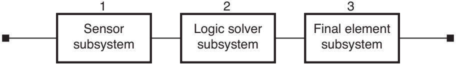
PFD$_{avg}$ of a SIF

- It is often assumed that (i) DU failures are the main contributor to PFD, (ii) that the time to a DU failure is exponentially distributed.
- If the test interval remains the same and the state of the system is returned to an “as good as new” state after each test, we may consider the PFD$_{avg}$ to be a long-run average value.



PFD_{avg} of a SIF

A SIF usually has three main subsystems:



Let E_i denote the event that subsystem i fails, for $i = 1, 2, 3$. The SIF fails if any of the subsystems fail, meaning that:

$$\begin{aligned} PFD^{SIF}_{\text{avg}} &= \Pr(E_1 \cup E_2 \cup E_3) = \Pr(E_1) + \Pr(E_2) + \Pr(E_3) \\ &- \Pr(E_1 \cap E_2) - \Pr(E_1 \cap E_3) - \Pr(E_2 \cap E_3) + \Pr(E_1 \cap E_2 \cap E_3) \end{aligned}$$

When the three subsystems are independent and have high reliability ($\Pr(E_i)$ is small), then:

$$PFD^{SIF}_{\text{avg}} \approx \Pr(E_1) + \Pr(E_2) + \Pr(E_3)$$

Remark: If the SIF may fail due to a single event, such as loss of utility system (e.g., power supply), it will be necesary to add this effect as a separate block in series with the other subsystems.

Mean Fractional Downtime

We may calculate the PFD$_{\text{avg}}$ as the mean fractional (i.e. in %) downtime as:

$$PFD_{\text{avg}} = \frac{E[D(0,\tau)]}{\tau}$$

where $E[D(0,\tau)]$ is the mean downtime in the proof test interval τ. The mean downtime in an interval t is then:

$$E[D(0,t)] = PFD_{\text{avg}} \cdot t$$

Example

Assume that the PFD$_{\text{avg}}$ has been calculated to be $2.7 \cdot 10^{-3}$. During a 5 years period (1 year is 8760 hours), the mean downtime is ≈ 118 hours.

Unconditional vs. Conditional Downtime

The (*unconditional*) mean downtime in a proof test interval is:

$$E[D(0,\tau)] = \tau \cdot PFD_{\text{avg}} = \tau \cdot \frac{1}{\tau}\int_0^{\tau} F(t)\,dt = \int_0^{\tau} F(t)\,dt$$

We do not know exactly when a hidden (DU) failure occurs, but once revealed during a proof test it may be of interest to know *for how long time (on the average) the system has been in a failed state due to this DU failure.*

- We then need to determine the *conditional downtime*, denoted $E[D(0,\tau|X(\tau)=0]$

where $X(\tau)=0)$ denotes that the system has been found to be in a failed state.

- The question is then: How can this conditional downtime be determined?

Conditional Mean Downtime

The conditional downtime may be found by using double expectations:

$$\begin{aligned} E[D(0,\tau)] &= E(E[D(0,\tau)|X(\tau)]) \\ &= E[D(0,\tau)|X(\tau)=1]\cdot\Pr(X(\tau=1)) + E[D(0,\tau)|X(\tau)=0]\cdot\Pr(X(\tau \\ &= E[D(0,\tau)|X(\tau)=0]\cdot\Pr(X(\tau=0) \end{aligned}$$

Note that we assume that $E[D(0,\tau)|X(\tau)=1]$ is zero, meaning that the mean downtime if we *know* that the system is functioning at time τ is zero (which is a reasonable assumption). We further assume that:

$$\begin{aligned} \Pr(X(\tau)=0) &= F(\tau) \\ E[D(0,\tau)] &= \int_0^\tau F(t)\,dt = PFD_{\text{avg}}\cdot\tau \end{aligned}$$

This means that:

$$E[D(0,\tau)|X(\tau)=0] = \frac{\tau}{F(\tau)}PFD_{\text{avg}}$$

Conditional Mean Downtime: Example

Consider a 2oo3 system of identical and indpendent components with exponentially distributed time to a (DU) failure. In this case:

$$\begin{aligned} F(t) &= 1 - 3e^{-2\lambda_{DU}\tau} + 2e^{-3\lambda_{DU}\tau} \\ &\approx 3(\lambda_{DU}\tau)^2 \end{aligned}$$

when using the Taylor series. We also know that:

$$PFD_{\text{avg}} \approx (\lambda_{DU}\tau)^2$$

$$E[D(0,\tau)|X(\tau)=0] = \frac{\tau}{F(\tau)} PFD_{\text{avg}} = \frac{\tau}{3(\lambda_{DU}\tau)^2}(\lambda_{DU}\tau)^2 = \frac{\tau}{3}$$

What does this say? A 2oo3 system fails when two of the three components have failed. If the two DU failures are distributed evenly over the test interval, we see that the system is in the failed state in the last third of the interval.

Using RBDs

Simplified formulas may be determined by the following steps:

1. Set up the structure function, $R_{S,i}(t)$ for SIF subsystem i, i is typically input elements (IE), logic solver (LS) and final elements (FE)
2. Calculate PFD$_{\text{avg}}$ using the formula:

$$PFD_{\text{avg,i}} = 1 - \frac{1}{\tau} \int R_{S,i}(t)\,dt$$

3. Add the contribution of PFD from each subsystem:

$$PFD_{\text{avg}} \approx PFD_{IE} + PFD_{LS} + PFD_{FE}$$

We focus from now on one sub-system only, and remove the notation i.

Assumptions

At this stage we consider a $koon$ voted structure where:

- All channels are identical and independent
- The channels are tested at the same time
- DU failures are the main contributors to PFD, and the impact of other failures and downtime may be neglected
- The time to a DU failure is exponential distributed

Approach (Simplified)

Instead of calculating $PFD_{\text{avg}} = 1 - \frac{1}{\tau}\int R_S(t)dt$, we can use upper bound approximation for fault tree analysis:

The upper found approximation states that the probability of TOP event (i.e. SIF failure) is the sum of the probability of failure of each minimal cutset.

- Recall that a $koon$ system fails if $n - k + 1$ components fail. For example, a 2oo4 system fails if $4 - 2 + 1 = 3$ components fail.
- Each minimal cutset j can be represented as a $1oo(n - k + 1)$ system:

$$PFD_{\text{avg,j}}^{(1oo(n-k+1))} = \frac{(\lambda_{\text{DU}}\tau)^{n-k+1}}{n-k+2}$$

- There are $\kappa = \binom{n}{n-k+1}$ minimal cutsets. This means that the PFD$_{avg}$ of a $koon$ system becomes:

$$PFD_{\text{avg}}^{(koon)} = \kappa \cdot \frac{(\lambda_{\text{DU}}\tau)^{n-k+1}}{n-k+2}$$

Simplified formulas

Considering the above assumptions, we may derive at the following table:

k/n	1	2	3	4
1	$\frac{\lambda_{\text{DU}}\tau}{2}$	$\frac{(\lambda_{\text{DU}}\tau)^2}{3}$	$\frac{(\lambda_{\text{DU}}\tau)^3}{4}$	$\frac{(\lambda_{\text{DU}}\tau)^4}{5}$
2	–	$\lambda_{\text{DU}}\tau$	$(\lambda_{\text{DU}}\tau)^2$	$(\lambda_{\text{DU}}\tau)^3$
3	–	–	$\frac{2\lambda_{\text{DU}}\tau}{2}$	$2(\lambda_{\text{DU}}\tau)^2$
4	–	–	–	$2\lambda_{\text{DU}}\tau$

Non-identical components

What happens if the channels are not identical? We demonstrate with a 1oo2 system:

- The reliability function will look slightly different:

$$R_S(t) = e^{-\lambda_{\mathrm{DU},1}\tau} + e^{-\lambda_{\mathrm{DU},2}\tau} - e^{-(\lambda_{\mathrm{DU},1}+\lambda_{\mathrm{DU},2})\tau}$$

- Integrating and using Taylor series give:

$$PFD_{\mathrm{avg}}^{(1oo2)} = \frac{(\lambda_{\mathrm{DU},1}\lambda_{\mathrm{DU},2})\tau^2}{3}$$

Non-identical components

We demonstrate also for a 2oo3 system:

- Recall that the reliability function of a 2oo3 system of *identical* components is:

  $$PFD_{\text{avg}}^{(2oo3)} = (\lambda_{\text{DU}}\tau)^2$$

  This is really the sum of *three* 1oo2 systems, consituting the possible combinations of the three components $\{1,2\}$, $\{1,3\}$, and $\{2,3\}$, meaning (if the three components were identical with the same DU failure rate):

  $$PFD_{\text{avg}}^{(2oo3)} = 3\frac{(\lambda_{\text{DU}}\tau)^2}{3} = (\lambda_{\text{DU}}\tau)^2$$

- If the three components are *not* identical, we get:

$$\begin{aligned} PFD_{\text{avg}}^{(2oo3)} &= \frac{(\lambda_{\text{DU},1}\lambda_{\text{DU},2})\tau^2}{3} + \frac{(\lambda_{\text{DU},1}\lambda_{\text{DU},3})\tau^2}{3} + \frac{(\lambda_{\text{DU},2}\lambda_{\text{DU},3})\tau^2}{3} \\ &= \frac{(\lambda_{\text{DU},1}\lambda_{\text{DU},2} + \lambda_{\text{DU},1}\lambda_{\text{DU},3} + \lambda_{\text{DU},2}\lambda_{\text{DU},3})\tau^2}{3} \end{aligned}$$

Non-identical components

General for $koon$:

- The PFD of each minimal cutset C_i becomes (note that this system becomes a 1oo$(n-k+1)$ sub-system):

$$PFD_{\text{avg}C_i}^{(1oo(n-k+1))} = \frac{(\prod_{j\in C_i} \lambda_{\text{DU,j}})\tau^{n-k+1}}{n-k+2}$$

  where C$_i$, $i = 1, 2, ..\kappa$ represents a specific minimal cutset, and j represents each of the components that belong to this one.

- The number of minimal cutsets, κ, is $\binom{n}{n-k+1}$. We need to add the contribution from each of these, giving:

$$PFD_{\text{avg}}^{(koon)} = \sum_{i=1}^{\kappa} \frac{(\prod_{j\in C_i} \lambda_{\text{DU,j}})\tau^{n-k+1}}{n-k+2}$$

Non-identical components

Consider a 3oo4 system of non-identical components:

- The number of minmial cutsets are $\binom{4}{2} = 6$. The six cutsets are $\{1, 2\}$, $\{1, 3\}$, $\{1, 4\}$, $\{2, 3\}$, $\{2, 4\}$, $\{3, 4\}$.
- The PFD$_{\text{avg}}$ becomes:

$$PFD^{(1oo2)}_{\text{avg}, C_i} = \frac{(\prod_{j \in C_i} \lambda_{\text{DU,j}})\tau^2}{3}$$

where C$_i$, $i = 1, 2, ..6$.

- The total PFD$_{\text{avg}}$ becomes:

$$\begin{aligned} PFD^{3oo4}_{\text{avg}} &= (\lambda_{\text{DU},1}\lambda_{\text{DU},2} + \lambda_{\text{DU},1}\lambda_{\text{DU},3} + \lambda_{\text{DU},1}\lambda_{\text{DU},4} \\ &+ \lambda_{\text{DU},2}\lambda_{\text{DU},3} + \lambda_{\text{DU},2}\lambda_{\text{DU},4} + \lambda_{\text{DU},3}\lambda_{\text{DU},4})\tau^2/3 \end{aligned}$$

Inclusion of CCFs

The effect of CCFs should be considered in case of redundancy.

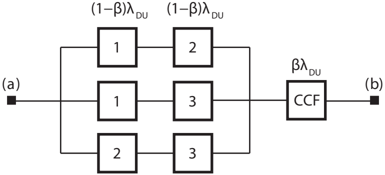
- Here, it is assumed first that the (standard) beta factor model is used as basis
- This model assumes that a *fraction* β of the total (in our context, the DU) failure rate is CCF, while the remaining fraction of failures $(1 - \beta)$ are independent failures:

  $$\lambda_{\mathrm{DU,tot}} = (1 - \beta)\lambda_{\mathrm{DU,tot}} + \beta\lambda_{\mathrm{DU,tot}}$$

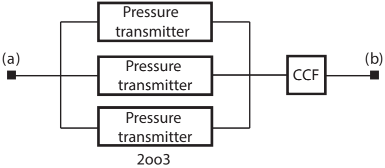
CCF is regarded as an failiure event that is independent from event of multiple independentfailures. In a RBD, the contribution of CCFs are added as a new functional block in series with the parallel structure.

Inclusion of CCFs

For a 2oo3 system, the RBD may look like:



If we know that the components are identical, for example, consisting of three pressure transmitters, the RBD is sometimes made as follows:



Inclusion of CCFs

The contribution from CCFs is treated as a single virtual component with failure rate $\beta\lambda_{\mathrm{DU}}$. For a 2oo3 system, the $\mathrm{PFD}_{\mathrm{avg}}$ becomes:

$$\begin{aligned} PFD_{\mathrm{avg}} &= PFD_{\mathrm{avg,\,ind.}} + PFD_{\mathrm{avg,\,ccf}} \\ &\approx ((1-\beta)\lambda_{DU}\tau)^2 + \frac{\beta\lambda_{DU}\tau}{2} \end{aligned}$$

It may be remarked that the contribution from CCFs is dominating.

Example

Consider a 2oo3 system with DU failure rate $1 \cdot 10^{-6}$ failures per hour, proof test interval $\tau = 8760$ hours and $\beta = 1 + 0\%$. Check that the contribution from CCFs is approximately 87% and about 13% from the independent failures.

Non-Negligible Repair Time

- In some cases, it is more reasonable to assume that the repair time is significant. For example if the system is installed subsea. The failure may be revealed during operation or found in relation to a proof test.
- The contribution from downtime due to repair can be disregarded if the EUC is in a safe state while repair is ongoing.

The contribution to PFD due to repair time is:

$$PFD_{\text{avg},2} = \frac{\Pr(T_{DU} \leq \tau) \cdot \text{MRT}}{\tau} = \frac{F(t) \cdot \text{MRT}}{\tau}$$

where MRT is the *mean repair time*, and index 2 donotes the known unavailability (as opposed to unknown unavailability, with index 1 in the textbook).

Non-Negligible Repair Time: Single System

Consider a SIS constituting a single component that may fail due to a DU failure with $F(\tau) = 1 - e^{\lambda_{DU}\tau} \approx \lambda_{DU}\tau$. When a DU failure occurs, the SIS will be unavailable as long as the repair is ongoing. The contribution to unavailability is in this situation:

$$PFD_{\text{avg},2} = \frac{F(t) \cdot \text{MRT}}{\tau} \approx \frac{\lambda_{DU}\tau\text{MRT}}{\tau} = \lambda_{DU}\text{MRT}$$

Example

Assume that the failure rate of a downhole safety valve (DHSV) installed in subsea well is $8 \cdot 10^{-6}$ failures/hour. Assume that it is tested every 6 months (1 month is 730 hours), and that the repair time if a failure occurs is 1 month (assuming that a intervention rig needs to be hired to do the job). The contribution from known unavailability then becomes $5.8 \cdot 10^{-3}$. The result is a low value, but not in comparison with the unknown unavailability.

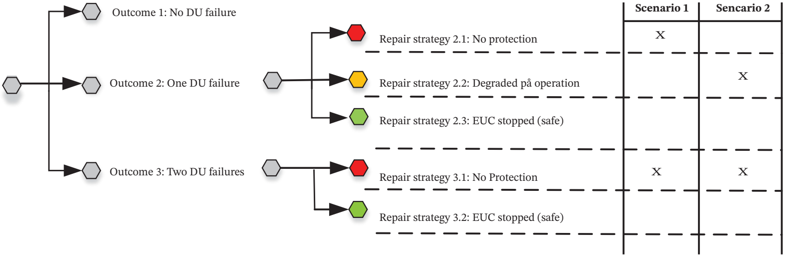
Non-negligible Repair Time: 1oo2 System

A 1oo2 system may experience ONE of the following three outcomes in a time period $(0, \tau)$:

- **Outcome 1**: No DU failure occurs with probability $p_1(\tau)$
- **Outcome 2**: One DU failure occurs with probability $p_2(\tau)$. Under this state, there are two credible options (see illustration on next slide):
  - **Repair strategy 2.1**: We repair without any protection. The whole system (both the failed and the remaining component) are disconnected while the repair is ongoing. The whole subsystem is unavailable in whole repair period.
  - **Repair strategy 2.2**: We repair with some protection. Only the failed component is isolated. The system is therefore degraded to 1oo1 whilethe repair is ongoiong. The subsystem becomes unavailable only if the other component fails repair is ongoing.
  - **Repair strategy 2.3**: We stop the EUC while repair is ongoing. This strategy would not give any contribution to the PFD of course, since the EUC is in the safe state.
- **Outcome 3**: Two DU failures occur with probability $p_3(\tau)$. There are two repair strategies (see illustration on next slide):
  - **Repair strategy 3.1**: We repair without any protection. The whole subsystem is unavailable in whole repair period.
  - **Repair strategy 3.2**: We stop the EUC while repair is ongoing. This strategy would not give any contribution to the PFD of course, since the EUC is in the safe state.

Remark: Notations deviate from printed textbook.

Non-negligible repair time: 1oo2 systems



	Scenario 1	Sencario 2
Repair strategy 2.1: No protection	X	
Repair strategy 2.2: Degraded på operation		X
Repair strategy 2.3: EUC stopped (safe)		
Repair strategy 3.1: No Protection	X	X
Repair strategy 3.2: EUC stopped (safe)		

Non-negligible repair time: 1oo2 systems

The probability for having each of the three outcomes is:

- **Outcome 1:**

$$p_1(\tau) \quad = \quad \Pr(T_{DU} \geq \tau) = (e^{-\lambda_{DU}\tau})^2$$

- **Outcome 2:**

$$\begin{aligned} p_2(\tau) &= \Pr(T_{DU} \leq \tau) = e^{-\lambda_{DU}\tau}(1 - e^{-\lambda_{DU}\tau}) + (1 - e^{-\lambda_{DU}\tau})e^{-\lambda_{DU}\tau} \\ &= 2e^{-\lambda_{DU}\tau}(1 - e^{-\lambda_{DU}\tau}) \end{aligned}$$

- **Outcome 3:**

$$p_3(\tau) \quad = \quad \Pr(T_{DU} \leq \tau) = (1 - e^{-\lambda_{DU}\tau})^2$$

Non-negligible repair time: 1oo2 systems

The mean downtime for each of the outcomes is:

- **Outcome 1:** Not relevant, as this state involves no DU failures.
- **Outcome 2:**
  - Repair strategy 2.1 (no protection - NP):

$$E(D)_{2,NP} = p_2(\tau) \cdot \mathrm{MRT} = 2e^{-\lambda_{DU}\tau}(1 - e^{-\lambda_{DU}\tau})\mathrm{MRT}$$

  - Repair strategy 2.2 (degraded mode - DM):

$$\begin{aligned} E(D)_{2,DM} &= p_2(\tau) \cdot E(D_r) \\ E(D_r) &= \int_0^{MRT} (1 - e^{-\lambda_{DU} t})dt \approx \int_0^{MRT} \lambda_{DU} t dt = \frac{\lambda_{DU}\mathrm{MRT}^2}{2} \\ E(D)_{2,DM} &= p_2(\tau) \cdot E(D_r) \end{aligned}$$

- **Outcome 3:**
  - Repair strategy 3.1 (no protection):

$$E(D)_{3,NP} = p_3(\tau) \cdot \mathrm{MRT}$$

Non-negligible repair time: 1oo2 systems

The PFD for the Scenario 1 (Outcome 2/No protection OR Outcome3/No Protection):

$$\begin{aligned} PFD_{\text{avg2}} &= \frac{(p_2(\tau)+p_3(\tau))\text{MRT}}{\tau} = \frac{\text{MRT}(1-e^{-2\lambda_{DU}\tau})}{\tau} \\ &\approx \frac{2\lambda_{DU}\tau\text{MRT}}{\tau} = 2\lambda_{DU}\text{MRT} \end{aligned}$$

PFDavg for Scenario 2 (Outcome 2/Degraded mode OR Outcome 3/No Protection):

$$\begin{aligned} PFD_{\text{avg2}} &= \frac{p_2(\tau)\cdot E(D_r)+p_3(\tau)\text{MRT}}{\tau} \\ &\approx p_2\frac{\lambda_{DU}\text{MRT}^2}{2\tau} + \text{MRT}(\lambda_{DU})^2 \end{aligned}$$

Note that the notations here may deviate slightly from the *printed* text book. There is an error in formula for $\text{MDT}_{2(b)}$ in textbook ($\text{p}_2(\tau)$ has been forgotten).

Case study: 1oo2 systems

Do the two approaches give very different results? Consider a 1oo2 system with DU failure rate $1 \cdot 10^{-6}$ per hour, $\tau = 8760$ hours, and MRT = 730 hours (one month).

	Equations		Results	
Formula*	**PFD unknown**	**PFD known**	**PFD unknown**	**PFD known**
Scenario 1	$\frac{(\lambda_{DU}\tau)^2}{3}$	$2\lambda_{DU}\text{MRT}$	$2.56 \cdot 10^{-5}$	$1.46 \cdot 10^{-3}$
Scenario 2	$\frac{(\lambda_{DU}\tau)^2}{3}$	$\frac{\lambda_{DU}MRT^2}{2\tau} + \lambda_{DU}^2\tau\text{MRT}$	$2.56 \cdot 10^{-5}$	$3.68 \cdot 10^{-5}$

As expected, we see that the contribution to PFD for scenario 1 has a significant impact on the PFD, and is the dominating part. Repairing while having no protection is therefore not a good idea when the repair time is significant as in this example.

Non-Negligible Repair Time: A Simple Approach

A more simplified approach to include non-negligible repair time of DU failures and which may be used for *koon* is:

- **Repair strategy 1:**
  - Repair is initiated after first failure (always)
  - We isolate the whole subsystem while repair is ongoing, i.e. there is no protection provided by SIS in this period.
- **Repair strategy 2:**
  - Repair is initiated after $n - k + 1$ DU failures.
  - We accept operation in degraded mode until the $n - k + 1$th failure (but do not calculate its contribution)
  - We isolate the whole subsystem while repair is ongoing, i.e. there is no protection provided by SIS in this period.

Non-negligible repair time: *koon* systems

PFDavg when considering repair strategy 1:

$$PFD_{\text{avg},2}^{koon} = \frac{\Pr(M \geq 1) \cdot \text{MRT}}{\tau} \approx n\lambda_{DU} \cdot \text{MRT}$$

PFDavg when considering repair strategy 2:

$$PFD_{\text{avg},2}^{koon} = \frac{\Pr(M \geq n-k+1) \cdot \text{MRT}}{\tau} \approx \binom{n}{n-k+1} \lambda_{DU}^{n-k+1} \tau^{n-k} \cdot \text{MRT}$$

It may be remarked that we get the same equations as we previously set up for a 1oo2 system, except that the contribution from a second component failing, while repairing the first one.

Non-negligible repair time: *koon* systems and CCF

PFDavg when considering repair strategy 1 - and also including CCFs is:

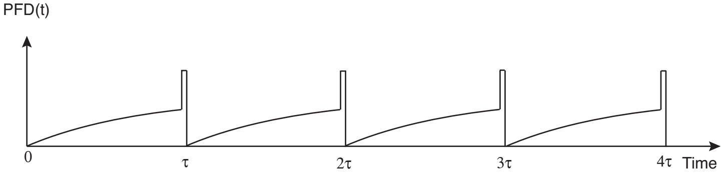
$$PFD_{\text{avg},2}^{koon} = \frac{\Pr(M \geq 1) \cdot \text{MRT}}{\tau} \approx (n(1-\beta)\lambda_{DU} + \beta\lambda_{DU}) \cdot \text{MRT}$$

PFDavg when considering repair strategy 2 - and also including CCFs is:

$$\begin{aligned} PFD_{\text{avg},2}^{koon} &= \frac{\left[\Pr(M_{ind} \geq n-k+1) + \Pr(\text{CCF})\right] \cdot \text{MRT}}{\tau} \\ &\approx \frac{\left[\binom{n}{n-k+1}(1-\beta)\lambda_{DU}\tau^{n-k+1} + \beta\lambda_{DU}\tau\right] \cdot \text{MRT}}{\tau} \\ &= \left[\binom{n}{n-k+1}(1-\beta)\lambda_{DU}^{n-k+1}\tau^{n-k} + \beta\lambda_{DU}\right] \cdot \text{MRT} \end{aligned}$$

Non-negligible test time (proof tests)

- Proof tests are, unlike repairs, carried out at regular intervals for DU failures.
- The unavailability of the SIS while testing may follow the same strategies as for repair. If whole subsystem is isolated during the test, we have $PFD_{avg,3} = \mathrm{MTT}/\tau$ where MTT is the mean test time.
- The downtime may be illustrated as below:



Effect of non-negligible MTTR of DD failures

Considering a 1oo1 system:

- Mean number of DD failures occurring in a test interval may be calculated as $E(N_{DD}(0,\tau)) = \lambda_{DD}\tau$
- The downtime from these DD failures are then $E(D_{DD}(0,\tau)) = E(N_{DD}(0,\tau)) \cdot \text{MTTR} = \lambda_{DD}\tau\text{MTTR}$
- The mean fractional downtime, or contribution to PFD$_{avg}$ becomes:

$$PFD_{\text{avg},4,\text{DD}}^{koon} = \frac{E(D_{DD}(0,\tau)}{\tau} = \lambda_{DD}\text{MTTR}$$

We may use similar approach as for non-negligible repair time of DU failures for *koon*. However, for DU as well as for DD it may be better to use formulas in IEC 61508-6 (due to the limitations of the simplified formulas).

Staggered testing

☞ Staggered testing: A proof test strategy where redundant channels are tested with the same test interval but not at the same time.

Why may this be a useful strategy?

- The level of dependency between the channels *caused by the testing* is reduced, leading to an overall reduction in the PFD_{avg} of the system.

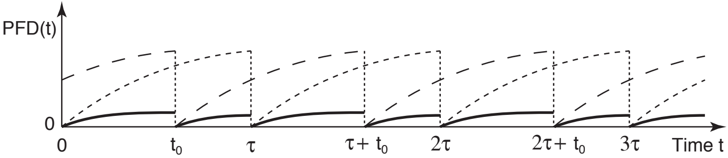


Figure: PFD(t) of a parallel system of two channels with staggered proof testing

Staggered testing

The PFD(t) for channel 1 is continuous in the interval from 0 to τ, whereas this is not the case for channel 2. Let's denote the unavailability function of channel 1 as $q_1(t)$, and for channel 2 as $q_2(t)$ and $q_3(t)$. This gives the following equations:

$$\begin{aligned}
q_1(t) &= 1 - e^{-\lambda_{DU} t} \text{ for } 0 < t \leq \tau \\
q_2(t) &= 1 - e^{-\lambda_{DU,2}(t+\tau-t_0}) \text{ for } 0 < t \leq t_0 \\
q_3(t) &= 1 - e^{-\lambda_{DU,2}(t+\tau-t_0}) \text{ for } t_0 < t \leq \tau
\end{aligned}$$

Consequently, the resulting unavailability in the two intervals become:

$$\begin{aligned}
q_s(t) &= q_1(t) \cdot q_2(t) \text{ for } 0 < t \leq t_0 \\
&= q_1(t) \cdot q_3(t) \text{ for } t_0 < t \leq \tau
\end{aligned}$$

Staggered testing

The PFD$_{\text{avg}}$ may now be calculated as:

$$PFD_{\text{avg}}(t_0) \quad = \quad \frac{1}{\tau}\Big[\int_0^{t_0} q_1(t)\cdot q_2(t)\,dt + \int_{t_0}^{\tau} q_1(t)\cdot q_3(t)\,dt\Big]$$

The full equation may be found by using e.g. MAPLE®.