Chapter 8.
Calculation of PFH

Marvin Rausand   Mary Ann Lundteigen

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 the alternative failure measure used with SIS, called *average frequency of dangerous failures* in key standards like IEC 61508 and IEC 61511.
- More specifically, we will address:
  - When this measure is more suited than the average probability of failure on demand, PFD_{avg}.
  - The underlying theory and assumptions for this failure measure.
  - Some of the analytical formulas developed for this purpose.

Other methods may be presented in other slides series, such as the use of Markov methods and PetriNets.

Motivation and clarifications

- average frequency of dangerous failure is *frequency measure*
- The measure is used for many applications, such as for railway signaling systems and for machinery systems.
- For railway industry, it is sometimes referred to as the hazard rate, as the result of a SIS failure (e.g., setting a green light signal when it should be red) is likely to be hazardous.
- The main attribute of systems using a failure frequency measure is that they operate in the **continuous demand** or **high-demand**, according to the classification in IEC 61508.
- The measure is often abbreviated **PFH**, even if the “old” term "Probability of having a dangerous failure per hour” has been removed from IEC 61508.

Characteristics of a high-/continuous demand system

What characterizes a high-demand vs continuous demand system (SIS)?

- The SIS is subject to **frequent demands**, either more often than once per year (high-demand) or always (continuous demand)
- The system may be repairable or non-repairable
- In case of a repairable system: The system may or may not be subject to regular proof testing
    - If never tested, there is a possibility that a redundant system is down, even if the response to the demand is successful

Frequency is not “just a frequency”

The failure frequency can be “different things”, and a starting point is to distinguish frequency measures for **non-repairable** and for **repairable** systems.

For repairable systems, we often refer to the following “types” of frequency measures:

- Probability density function
- Failure rate function
- Average failure rate

For repairable systems, we may use:

- Rate of occurrence of failures (ROCOF)
- Average ROCOF
- Vesely Failure Rate

Frequency measure for non-repairable systems

Detailed about the frequency measures for repairable systems are:

- **Probability density function**, $f(t)$, which is the *unconditional* probability that the item fails in a small interval Δt per Δt time units.
- **Failure rate function**, $z(t)$, which is the *conditional* probability that the item fails in a small test interval Δt given that the item has survived til the starting point of the interval, t, per Δt time units.
- **Average failure rate**, which is

$$\bar{z}(0, \tau) = \frac{1}{\tau} \int_0^\tau z(t) dt \approx \frac{F(\tau)}{\tau}$$

Note that the approximation above only applies to rather short intervals. For large values of τ, we note that the average failure rate tends towards zero, which is not realistic (even if desired...).

Frequency measure for non-repairable systems

Which measure would be PFH for non-repairable systems?

- The failure rate function would perhaps be the best alternative (?)
- Once the distribution of z(t) or F(t) is selected, we may calculate the PFH
- Consider a *single* item. We then get for:
  - Exponentially distributed time to failure, with parameter λ:

$$\bar{z}(0,\tau) = \frac{1}{\tau}\int_0^\tau z(t)\,dt = \frac{1}{\tau}\int_0^\tau \lambda dt = \lambda$$

  - Weilbul distributed time to failure, with parameters λ and α

$$\bar{z}(0,\tau) = \frac{1}{\tau}\int_0^\tau z(t)\,dt = \frac{1}{\tau}\int_0^\tau \alpha\lambda^\alpha t^{\alpha-1} dt = \lambda^\alpha \tau^{\alpha-1}$$

What would be such a non-repairable system?

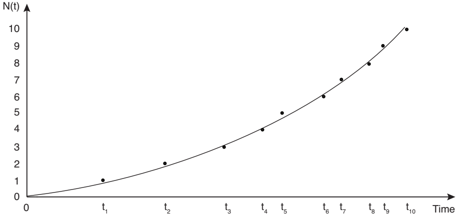
Most safety-critical systems in our context are repairable. Non-repairable systems are less common. One example could be a space mission system (never to return to earth) or a destructive system (destroye, once used).

- We will not spend more time on non-repairable systems in this lecture.

Frequency measure for repairable systems

Suitable frequency measure for a repairable system is ROCOF, $w(t)$

- ROCOF can be estimated on the basis of the following curve.
- Note that the curve may be linear, convex or concave, depending on whether the ROCOF is constant, increasing or decreasing with time.



Frequency measure for repairable systems

- ROCOF may be calculated as:

$$\begin{aligned} w(t) &= \frac{d}{dt}E[N(t)] = \lim_{\Delta t \to 0} \frac{E[N(t+\Delta t) - N(t)]}{\Delta t} \\ &\approx \frac{E[N(t+\Delta t) - N(t)]}{\Delta t} \text{ (for small } \Delta t\text{)} \\ &= \frac{\text{Pr[Failure in (t,t+}\Delta\text{t)]}}{\Delta t} \text{ (Assuming} \leq \text{1 failure in } \Delta\text{t)} \end{aligned}$$

- Note that the ROCOF is *unconditional* failure frequency, as it does not consider what happened before t.
- Any further calculation requires that we make an assumption about the *distribution* of the occurrence of failures.

Frequency measure for repairable systems

- For small values of Δt, we get:

$$w(t) \quad \approx \quad \frac{\text{Mean (or observed) number of failures in } (t, t+\Delta t)}{\Delta t}$$

(Assuming ≤ 1 failure in Δt)

- This result is useful if we want to estimate the ROCOF on the basis of a given curve (N(t) or E(N(t)).

Frequency measure for repairable systems

We now assume that the failure rate, λ, of an item is constant (i.e., exponentially distributed time to failure for each item)

- In this case, the failures occur according to a homogeneous Poisson process with distribution:

$$\Pr(N(t) = n) \quad = \quad \frac{(\lambda t)^n}{n!} e^{-\lambda t} \text{ for n } = 0, 1 \dots$$

- The mean number of failures in an interval $(0, t)$ is:

$$E[N(t)] = \sum_{n=0}^{\infty} n \Pr(N(t) = n) = \lambda t$$

- The ROCOF then becomes (for not too large values of t):

$$w(t) = \frac{E[N(t)]}{t} = \lambda$$

Frequency measure for repairable systems

Assuming the homogeneous Poisson process results in a ROCOF that *has the same value* as the rate λ, however the concepts have different meaning!

Frequency measure for repairable systems

Vesely Failure Rate, here denoted $\lambda^V(t)$, is an alternative to the ROCOF failure frequency measure. It is defind as:

$$\begin{aligned}\lambda^V(t) &\approx \frac{\Pr(\text{Failure in } (t, t+\Delta t] | X(t)=1)}{\Delta t} \\ &= \frac{\Pr(\text{Failure in } (t, t+\Delta t])}{\Pr(X(t)=1)} \cdot \frac{1}{\Delta t} = \frac{w(t)}{A(t)}\end{aligned}$$

This failure rate has the following attributes:

- It is a conditional probability of a failure in $(t, t+\Delta t]$, given that the item is functioning at time t.
- It is not considered how many times the item has failed prior to t, *just* with what probability the item is functioning at time t.
- The ROCOF is therefore a *fraction* of the Vesely Failure Rate.

PFH as a frequency measure

PFH has a meaning that partly overlap with ROCOF:

- PFH may be regarded as ROCOF *with respect to dangerous failures*

It is suggested in the textbook that the term PFH can be used as as a time dependent parameter *as well as* an average value, just as we have for ROCOF.

IEC 61508 defines PFH as a frequency *per hour*. In principle, we could decide to use PFH per minute, per second, per year and so on, however tables in IEC 61508 is set up using “per hour”.

The meaning of dangerous in PFH

PFH is the (average) failure rate of *dangerous* failures per hour. But what is meant by dangerous in this context.

- Interpretation 1: It considers *all* failures that terminates the ability of a SIS to carry out its safety functions
- Interpretation 2: It considers those dangerous failures that results in a hazardous event within the EUC

Confused?

- In the second option, we disregard certain types of dangerous failures, the dangerous detected (DD) failures *IF* the EUC is brought to a safe state as a response to the failures.
- This may be implemented for sensors and logic solvers, but now always applicable to final elements.

The meaning of dangerous in PFH

Why are DD failures a concern:

- In high-demand mode, demands occur so often that it may not be time to initiate or complete repair in before
- The probability that a demand with constant rate λ_{de} occurs before the DD failure has been repaired, with mean time to restoration (MTTR), is:

$$\Pr(t < \text{MTTR}) \approx \lambda_{de}\text{MTTR}$$

- If the MTTR is 24 hours and λ_{DE} is once every week, the probability that a demand occurs before restoration is approximately 14%.

PFH of a SIF

The PFH of a SIF is the sum of the PFH calculated for each subsystem in the same time interval, often $(0, \tau)$ where τ is the proof test interval:

$$PFH_{\text{SIF}}(0, \tau) = PFH_S(0, \tau) + PFH_{LS}(0, \tau) + PFH_{FE}(0, \tau)$$

Where the notation “S” means sensors, “LS” means logic solver and “FE” means final element.

Even with constant failure rate of items, the PFH at the subsystem level (and thereby also the SIF level) may be time dependent if one or more of the subsystems are redundant.

Simplified formulas: PFH for a single system

A single system may enter either a DD or DU failure state. In a time interval DD, we may experience first one (that is repaired) and then the other.

Assumption: Only one failure can occur during a period of in the magnitude of the proof test interval. Since the system is a single system, we will shut down/stop the EUC upon a DD failure.

The assumption means that we only consider the contribution from DU failrues:

$$PFH_G^{1oo1} = \frac{E[N_G(\tau)]}{\tau}$$

where

$$E[N_G(\tau) = 0 \cdot \Pr(N(\tau) = 0) + 1 \cdot \Pr(N(\tau) = 1) = (1 - e^{-\lambda_{DU}\tau}) \approx \lambda_{DU}\tau$$

which results in:

$$PFH_G^{1oo1} = \frac{1 - e^{-\lambda_{DU}\tau}}{\tau} \approx \lambda_{DU}$$

Simplified formulas: PFH for a series structure

The failure rate of a series structure is the sum of the failure rates:

$$PFH_G^{noon} = \sum_{i=1}^{n} \lambda_{DU,i}$$

Simplified formulas: PFH for a 1oo2 system

Assumption: We maintain focus on DU failures only. No more than one DANGEROUS GROUP FAILURE during a period of a proof test interval, or another defined time interval of a magnitude of a year or so:

$$PFH_G^{1oo2} = \frac{E[N_G(\tau)]}{\tau}$$

where:

$$E[N_G(\tau) = 0 \cdot \Pr(N(\tau) = 0) + 1 \cdot \Pr(N(\tau) = 1) = (1 - e^{-\lambda_{DU}\tau})^2 \approx (\lambda_{DU}\tau)^2$$

This results in:

$$PFH_G^{1oo2} = \lambda_{DU}^2 \tau$$

Simplified formulas: PFH of a *koon* system

Assumption: We maintain focus on DU failures only. No more than one DANGEROUS GROUP FAILURE during a period of a proof test interval, or another defined time interval of a magnitude of a year or so:

$$PFH_G^{koon} = \frac{E[N_G(\tau)]}{\tau}$$

where:

$$\begin{aligned} E[N_G(\tau)] &= 0 \cdot \Pr(N(\tau) = 0) + 1 \cdot \Pr(N(\tau) = 1) = \Pr(M \geq n - k + 1) \\ &\approx \sum_{j=n-k+1}^{n} \binom{n}{j} (\lambda_{DU}\tau)^j \\ &\approx \Pr(M = n - k + 1) \end{aligned}$$

This results in:

$$PFH_G^{koon} = \frac{\Pr(M = n - k + 1)}{\tau} = \binom{n}{n-k+1} \lambda_{DU}^{n-k+1} \tau^{n-k}$$

Inclusion of DD failures

Assumption: We study a 1oo2 system. Two possible situations for the first failure:

(a) A DU failure occurs first, OR

(b) A DD failure occurs first.

The next (second) failure will result in a group failure. We assume that (n-k+1) DD failures always results in an automatic transition to the safe state.

The approach is as before:

- First determine Pr(DGF in $(0,\tau)$) (which under our assumptions is the same as E[($\mathrm{N}_G\tau$)]).
- Then determine:

$$PFH_G = \frac{\Pr(\text{DGF in}(0,\tau)}{\tau}$$

Inclusion of DD failures: Option (a)

Option (a) - (approximation found using Maple):

$$
\begin{aligned}
&\Pr(\text{DGF in}(0,\tau)) \\
&\quad = \int_0^\tau 2\lambda_{DU} e^{-2\lambda_{DU} t}(1 - e^{-(\lambda_{DU}+\lambda_{DD})(\tau - t)})\,dt \\
&\quad \approx (\lambda_{DU}\tau)^2 + \lambda_{DU}\lambda_{DD}\tau^2
\end{aligned}
$$

Inclusion of DD failures: Option (b)

Option (b) - approach 1 (approximation found using Maple):

$$\begin{aligned} \Pr(\text{DGF in}(0,\tau)) &= \int_0^\tau 2\lambda_{DD} e^{-2\lambda_{DD} t}\left[1 - e^{-\lambda_{DU}\cdot MTTR}\right] dt \\ &\approx 2\lambda_{DU}\lambda_{DD}\tau MTTR \end{aligned}$$

Option (b) - approach 2:

$$\begin{aligned} \Pr(\text{DGF in}(0,\tau)) &= (1 - e^{-2\lambda_{DD}\tau})(1 - e^{-\lambda_{DU} MTTR}) \\ &\approx 2\lambda_{DU}\lambda_{DD}\tau MTTR \end{aligned}$$

Note the assumption that the second failure of interest is a DU failure only (as a double DD failure is assumed to result a commanded transition to the safe state)

Inclusion of DD failures: Options (a) AND (b)

A DGF occurs if option (a) or option (b) occurs. This means that:

$$\Pr(\text{DGF in}(0,\tau)) \quad = \quad (\lambda_{DU}\tau)^2 + \lambda_{DU}\lambda_{DD}\tau^2 + 2\lambda_{DU}\lambda_{DD}\tau MTTR$$

The PFH becomes then:

$$PFH_G = \frac{\Pr(\text{DGF in}(0,\tau)}{\tau} = \lambda_{DU}^2\tau + \lambda_{DU}\lambda_{DD}\tau + 2\lambda_{DU}\lambda_{DD}MTTR$$

Section 9.4.2 - “low” high-demand mode

When the demand rate is just slightly higher than one demand per year (e.g., once every 7-10 months), it is likely that any detected (DD) failure is repaired before the next demand. In this case, we may disregard the DD-failures in the PFH formulas.

$$\Pr(\text{DGF in}(0,\tau)) \quad = \quad (\lambda_{DU}\tau)^2$$

The PFH becomes then:

$$PFH_G = \frac{\Pr(\text{DGF in}(0,\tau)}{\tau} = \lambda_{DU}^2\tau$$

Section 9.4.2 - inclusion of CCFs

The inclusion of CCFs is rather straight forward with the standard beta factor model:

$$PFH_{G}^{koon} = PFH_{G,i}^{koon} + PFH_{G,c}^{koon}$$

PFH$_{G,i}$ corresponds to the equation(s) developed on previous slides, but with λ_{DU} replaced by $(1-\beta)\lambda_{DU}$ and λ_{DD} replaced by $(1-\beta_D)\lambda_{DD}$, and:

$$PFH_{G,c} = \beta\lambda_{DU}$$

You may notice that $\beta_D\lambda_{DD}$ was omitted. The main reason is that a double DD failure is assumed to result in a commanded transition to the safe state.

IEC 61508 formulas: Assumptions

The main assumption in IEC 61508 is that a group failure (DGF) occurs if a D (DU or DD) failure occurs first (independent failure), and then a DU failure.

If a DD failure occurs as the last failure (independent or CCF), it results in a transition to the safe state. This last assumptions is questionable since it is impossible to know *when* the DD failure is the last of n failures, if one or more of the previous failures are (hidden) DU failures.

IEC 61508 formulas: Basic approach

- The basic idea is to find what we previously have referred to as *dangerous group failure (DGF)*.
- DGF is however not exactly the same as we determined it with PFD-formulas, because of the assumption that the the contribution DD-failure as the last failure is disregarded.

IEC 61508 formulas: Examples

Consider a 1oo2 system (without including CCFs):

$$PFH_G^{1oo2} = 2 \cdot \lambda_D(1 - e^{-\lambda_{DU} t_{CE}}) \approx 2\lambda_D\lambda_{DU} t_{CE}$$

where $t_{CE} = \frac{\lambda DU}{\lambda D}(\frac{\tau}{2} + MRT) + \frac{\lambda DD}{\lambda D} MTTR$. With CCFs included, we get:

$$PFH_G^{1oo2} = 2 \cdot \lambda_D(1 - e^{-(1-\beta)\lambda_{DU} t_{CE}}) + \beta\lambda DU \approx 2\lambda_D^{(I)}\lambda_{DU} t_{CE} + \beta\lambda_{DU}$$

where and $\lambda_D^{(i)} = (1 - \beta)\lambda_{DU} + (1 - \beta_D)\lambda_{DD}$. Note again that CCF contribution from DD failures are disregarded due to the initial assumption.

IEC 61508 formulas

We may use the same assumptions to derive the formula for 2oo3 system:

$$PFH_G^{2oo3} = 3 \cdot \lambda_D^{(I)}(1 - e^{-2(1-\beta)\lambda_{DU} t_{CE}}) + \beta\lambda DU \approx 6\lambda_D\lambda_{DU} t_{CE} + \beta\lambda DU$$

For a 1003 system, the system fails when the third failure occurs. This must happen in the mean downtime after two failures, which is:

$$t_{GE2} = \frac{\lambda_{DU}}{\lambda_D}(\frac{\tau}{3} + MRT) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

The equation becomes:

$$\begin{aligned} PFH_G^{1oo3} &= 3 \cdot \lambda_D^{(I)}(1 - e^{-2\lambda_D^{(I)} t_{CE}})(1 - e^{-(1-\beta)\lambda_{DU} t_{GE2}}) + \beta\lambda DU \\ &= 6\lambda_D^2(1-\beta)\lambda_{DU} t_{CE} t_{GE2} + \beta\lambda DU \end{aligned}$$

Note that the group equivalent mean downtime is never part of PFH formulas (therefore no t_{GE} which is previously used to denote this special case.

IEC 61508 formula- alternatives

We can also use an alternative approach to derive the IEC 61508 formulas, using the relationship:

$$PFH_G = \frac{PFD_{avg}}{t_{GE}}$$

However, it should be noted the assumption about DD failure to be disregarded as the last failure is not captured here.

IEC 61508 formula- alternatives

For a *koon* system, we get:

$$PFH_G = (\prod_{i=1}^{n-k+1}(n-i+1))(\lambda_D^{(I)})^{n-k}(1-\beta)\lambda_{DU}(\prod_{i=2}^{n-k} t_{GEi})t_{CE} + \beta\lambda_{DU}$$

Note that there is an error in formula (9.59) in the SIS book, so the one above has been developed for the purpose of the slides. It is in line with the new version of section 8.4, formula 8.48, found under errata for the textbook.

Markov methods

The use of Markov approach to solve for PFH is very similar to what we did for PFD.

1. Define the system states
2. Set up the state transition diagram
3. Calculate the steady state probabilities[1]
4. Determine PFH by considering all "jumps" into the dangerous states[2]

[1] Alternatively, one can calculate the time dependent probabilities .

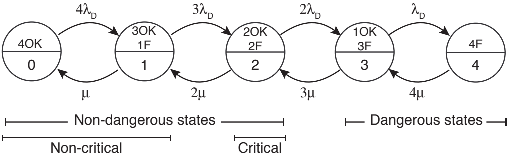
[2] Alternatively, if time dependent probabilities have been calculated: Integrate and average the "jumps" into the dangerous states during a defined time interval

Example

Consider a 2oo4 system of independent channels that may fail with a dangerous failure rate λ_D.

State	State description
0	Four channels are functioning
1	Three channels are functioning, one has failed
2	Two channels are functioning, two have failed
3	One channel is functioning and three are failed

The state transition diagram becomes:



Example continued

PFH becomes:

$$PFH_G = P_2 \cdot 2\lambda_D$$

where P_2 is (by using MAPLE) is:

$$P_2 = \frac{6\lambda_D^2\mu^2}{\mu^2 + \mu^3\lambda_D + 6\mu^2\lambda_D^2 + 4\mu\lambda_D^3 + \lambda_D^4}$$