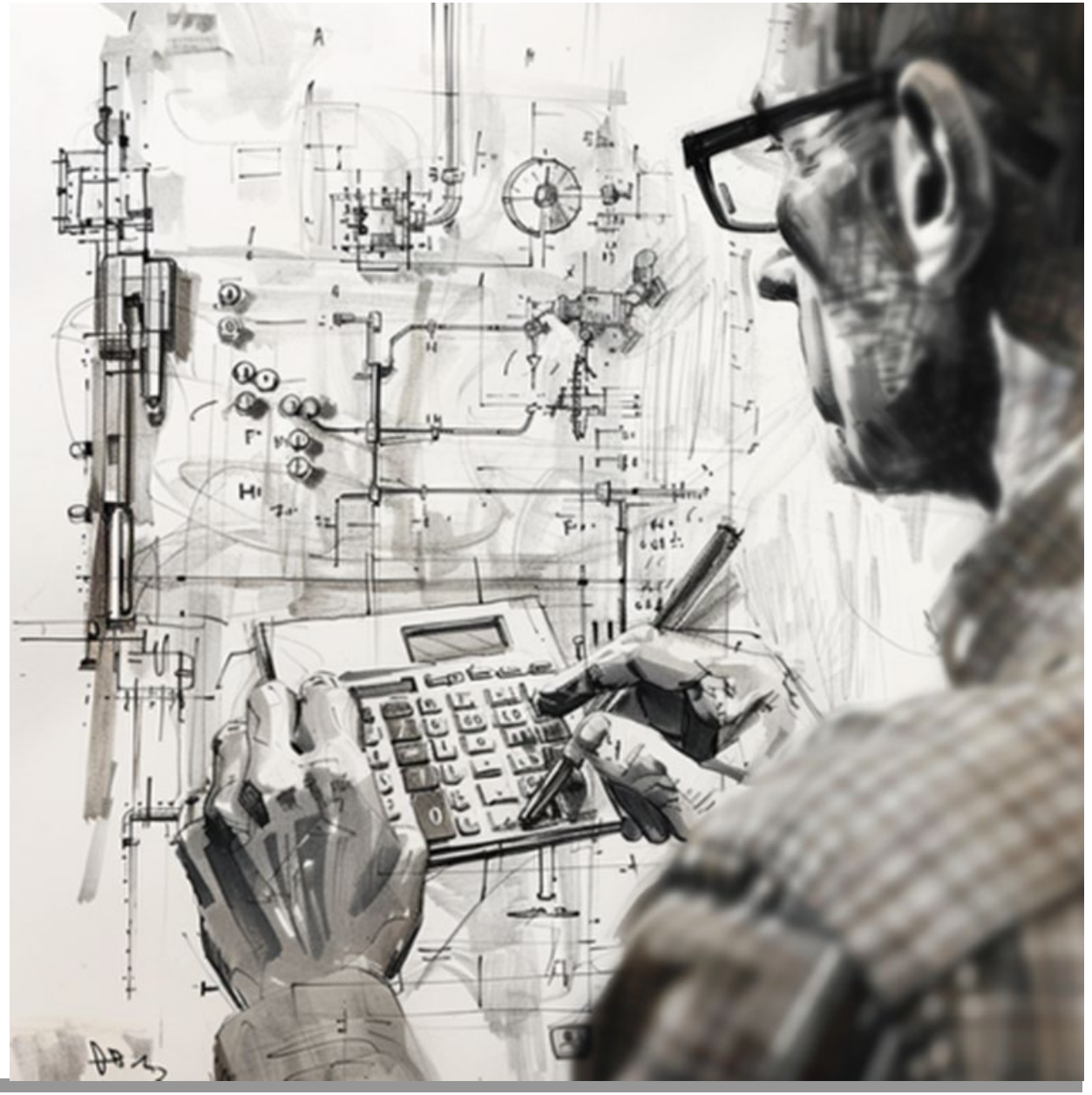
Image made with Midjourney v 6.0

# Do engineers really need calculators to estimate probability of safety function failure?



# IEC 61508-6 makes it look complicated

Even something as simple as 1oo2 voting:

$$PFD_G = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

# Overview

This presentation is based on generic MooN models developed in association with The 61508 Association (Working Group 15)

The main objective was to model the effect of staggered test intervals

The working group developed comprehensive MooN models:

We went all the way down the rabbit hole

…and out again

$$
\begin{aligned}
PFD_{AVG} \approx\ & \binom{N}{N-M+1}.\frac{((1-\beta).(\lambda_{DU}-\lambda_{DN}).T_1)^{N-M+1}}{N-M+2}+\frac{\beta.(\lambda_{DU}-\lambda_{DN}).T_1}{2} \\
& +\binom{N}{N-M+1}.\frac{((1-\beta).\lambda_{DN}.T_2)^{N-M+1}}{N-M+2}+\frac{\beta.\lambda_{DN}.T_2}{2} \\
& +\binom{N}{N-M+1}.((1-\beta_D).\lambda_{DD})^{N-M+1}.MTTR^{N-M+1}+\beta_D.\lambda_{DD}.MTTR \\
& +N.\lambda_{DD}.MTTR.\left(\binom{N-1}{N-M}.\frac{((1-\beta).(\lambda_{DU}-\lambda_{DN}).T_1)^{N-M}}{N-M+1}\right) \\
& +\left(N.\frac{(\lambda_{DU}-\lambda_{DN}).T_1}{2}\right).\left(\binom{N-1}{N-M}.((1-\beta_D).\lambda_{DD})^{N-M}.MTTR^{N-M}\right) \\
& +N.\lambda_{DD}.MTTR.\left(\binom{N-1}{N-M}.\frac{((1-\beta).\lambda_{DN}.T_2)^{N-M}}{N-M+1}\right) \\
& +\left(N.\frac{\lambda_{DN}.T_2}{2}\right).\left(\binom{N-1}{N-M}.((1-\beta_D).\lambda_{DD})^{N-M}.MTTR^{N-M}\right) \\
& +N.(\lambda_{DD}.MTTR).\left(\binom{N-1}{1}.\frac{\lambda_{DN}.T_2}{2}\right).\left(\binom{N-2}{N-M-1}.\frac{((1-\beta).(\lambda_{DU}-\lambda_{DN}).T_1)^{N-M-1}}{N-M+2}\right) \\
& +\left(N.\frac{(1-\beta).(\lambda_{DU}-\lambda_{DN}).T_1}{2}\right).\left(\binom{N-1}{1}.\frac{\lambda_{DN}.T_2}{2}\right).\left(\binom{N-2}{N-M-1}.((1-\beta_D).\lambda_{DD})^{N-M-1}.MTTR^{N-M-1}\right) \\
& +\left(N.\frac{\lambda_{DN}.T_2}{2}\right).\left(\binom{N-1}{1}.\frac{\lambda_{DU}.T_1}{2}\right).\left(\binom{N-2}{N-M-1}.((1-\beta_D).\lambda_{DD})^{N-M-1}.MTTR^{N-M-1}\right) \\
& +N.\frac{(\lambda_{DU}-\lambda_{DN}).T_1}{2}.\left(\binom{N-1}{N-M}.\frac{((1-\beta).\lambda_{DN}.T_2)^{N-M}}{N-M+1}\right) \\
& +N.\frac{\lambda_{DN}.T_2}{2}.\left(\binom{N-1}{N-M}.\frac{((1-\beta).(\lambda_{DU}-\lambda_{DN}).T_2)^{N-M}}{N-M+1}\right)
\end{aligned}
$$

# Overview

We discovered how the models can be simplified

Synchronised testing:

$$PFD_{\text{MooN }AVG} \approx \frac{2^{N-M+1}}{N-M+2}.\binom{N}{N-M+1}.\left((1-\beta_D).\lambda_{DD}.MTTR + \frac{(1-\beta).\lambda_{DU}.T}{2}\right)^{N-M+1} + \beta_D.\lambda_{DD}.MTTR + \beta.\frac{\lambda_{DU}.T}{2}$$

Staggered testing:

$$PFD_{\text{MooN }AVG} \approx St_{M,N}.\binom{N}{N-M+1}.\left((1-\beta_D).\lambda_{DD}.MTTR + \frac{(1-\beta).\lambda_{DU}.T}{2}\right)^{N-M+1} + \beta_D.\lambda_{DD}.MTTR + \beta.\frac{\lambda_{DU}.T/N}{2}$$

…but these models are never more accurate than very simple approximations such as

$$\boldsymbol{PFD_{AVG} \approx \frac{2}{3}.\beta.\lambda_{DU}.T} \quad \text{or} \quad \boldsymbol{RRF \approx \frac{3}{2}.\frac{MTBF_{DU}}{\beta.T}}$$

SYSTEMS

# In this presentation

Models for MooN independent channels covering:

1. Continuous mode and high demand mode
2. Synchronised testing
3. Proof test coverage
4. Evenly staggered testing
5. Examples

**Conclusion: Complex mathematics is not needed**

# Validating the simplified models

Results from the simplified MooN models were compared with:

- Longhand manual calculations
- Recursive algorithms coded in VBA
- Fully expanded spreadsheet models
- Discrete time-slice spreadsheet models
- Simple approximations

The evaluation covered all MooN combinations with N up to 7

The simplified models agreed with other calculations to within **1%**

**The approximation** $PFD_{AVG} \approx {}^{2}/_{3}.\beta.\lambda_{DU}.T$ **is within 30%**

SYSTEMS

# The models are based on **failure rates**

Derived from IEC 61508-6 and SINTEF PDS Method Handbook

The symbol $\lambda$ represents failure rate, estimated from frequency:
$n$ failures counted over time $\tau$ **$n/\tau$ is the historical frequency**

Units may be per hour, per $10^9$ hours, or per annum

**Future performance may vary significantly from past performance**

**Essential** to start with IEC 60812 *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

Failures always need to be considered **in context**

**Whether a failure is safe or dangerous depends on the application**

SYSTEMS

# The disclaimer: Expect uncertainty and variability

- Effects of failures may be uncertain
- When does degraded operation become a dangerous failure?
- Devices usually have multiple modes of failure
- Failure frequencies are always variable, depending on:
  - Environmental factors (refer to IEC 61709)
  - Human factors
  - Systematic factors
  - Equipment condition
- Expect failure rates to vary over **at least an order of magnitude**
  i.e. variation is usually wider than between 0.3 $\lambda$ and 3 $\lambda$

SYSTEMS

# No precision!

Don’t expect (or believe) any answers with 3 significant figures

**Even 1 significant figure of precision is optimistic**

Failure rate and probability estimates are never better than +/- 50%

An estimate within  +/- 30% is close enough

Risk estimates can never be better than within an order of magnitude

SYSTEMS

# Continuous mode and high demand mode functions

The overall dangerous failure rate of a safety function can be estimated as

$$\lambda_D^{SF} = \beta_D . \lambda_{DD} + \beta . \lambda_{DU} + \frac{N!}{(M-1)!} . \lambda_{DU}^{N-M} \left( (1-\beta_D) . \lambda_{DD} . MTTR + (1-\beta) . \lambda_{DU} . (T/2) \right)^{N-M}$$

> 99%

# Continuous mode and high demand mode functions

The overall dangerous failure rate of a safety function can be estimated as

$$\lambda_D^{SF} = \beta . \lambda_{DU} + \frac{N!}{(M-1)!} \cdot \lambda_{DU}^{N-M} \left( (1-\beta_D) \lambda_{DD} . MTTR + (1-\beta) . \lambda_{DU} . (T/2) \right)^{N-M}$$

> 99%

***Detected*** dangerous failures may be excluded in high demand mode if an **automatic fault reaction puts** the equipment into a safe state

# $\beta$ depends on M and N

***Typical*** values of $\beta$ for sensors and final elements:

| $\beta_{MooN}$ | | N | | | |
|---|---|---|---|---|---|
| | | 2 | 3 | 4 | 5 |
| M | 1 | 0.1 | 0.05 | 0.03 | 0.02 |
| | 2 | | 0.15 | 0.06 | 0.04 |
| | 3 | | | 0.18 | 0.08 |
| | 4 | | | | 0.2 |

$\beta$ is reduced with higher N-M, but increases with higher M

These values are derived from IEC 61508-6 Table D.5, different models give different values

**$\beta$ models are rule based, estimated values are always uncertain**

SINTEF Report A26922 (2015) reviewed operational experience:
$\beta_{1oo2}$ for sensors and valves is typically in the range **0.12 to 0.15**

SYSTEMS

# **Low demand**: basic 'average before product' model

The probability of N-M+1 concurrent dangerous failures in N ***completely independent*** channels can be approximated by raising the average $PFD$ of a single channel to the power N-M+1,

$$PFD_{\mathrm{MooN}\ AVG} \approx \binom{\mathrm{N}}{\mathrm{N-M+1}}.(PFD_{1oo1\ AVG})^{\mathrm{N-M+1}}$$

$$(1-\beta_D).\lambda_{DD}.MTTR + \frac{(1-\beta).(\lambda_{DU}-\lambda_{DN}).T_1}{2} + \frac{(1-\beta).\lambda_{DN}.T_2}{2}$$

Common cause failures are added to complete the model:

$$+ \beta_D.\lambda_{DD}.MTTR + \beta.\frac{(\lambda_{DU}-\lambda_{DN}).T_1}{2} + \beta.\frac{\lambda_{DN}.T_2}{2}$$

SYSTEMS

# Low demand mode with synchronised channel tests

**The average probability with synchronised testing is higher than estimated by the basic 'average before product' model**

The $(PFD)^{\text{N-M+1}}$ product needs to be expanded before averaging

The **instantaneous** probability of N-M+1 failures can be estimated as:

$$\binom{\text{N}}{\text{N}-\text{M}+1}\left[(1-\beta_D).\lambda_{DD}.MTTR+\ (1-\beta).(\lambda_{DU}-\lambda_{DN}).t_1+(1-\beta).\lambda_{DN}.t_2\right]^{\text{N}-\text{M}+1}$$

$$+\ (\beta_D.\lambda_{DD}.MTTR+\ \beta.(\lambda_{DU}-\lambda_{DN}).t_1+\beta.\lambda_{DN}.t_2)$$

The expanded product is integrated over time to estimate the average

This is known as the '**product before average**' model

SYSTEMS

# Detailed low demand model with synchronised testing

$$PFD_{AVG} \approx \binom{N}{N-M+1} \cdot \frac{((1-\beta).(\lambda_{DU}-\lambda_{DN}).T_1)^{N-M+1}}{N-M+2} + \frac{\beta.(\lambda_{DU}-\lambda_{DN}).T_1}{2}$$
$$+ \binom{N}{N-M+1} \cdot \frac{((1-\beta).\lambda_{DN}.T_2)^{N-M+1}}{N-M+2} + \frac{\beta.\lambda_{DN}.T_2}{2}$$
$$+ \binom{N}{N-M+1} \cdot ((1-\beta_D).\lambda_{DD})^{N-M+1}.MTTR^{N-M+1} + \beta_D.\lambda_{DD}.MTTR$$
$$+ N.\lambda_{DD}.MTTR \cdot \left( \binom{N-1}{N-M} \cdot \frac{((1-\beta).(\lambda_{DU}-\lambda_{DN}).T_1)^{N-M}}{N-M+1} \right)$$
$$+ \left( N.\frac{(\lambda_{DU}-\lambda_{DN}).T_1}{2} \right) \cdot \left( \binom{N-1}{N-M} \cdot ((1-\beta_D).\lambda_{DD})^{N-M}.MTTR^{N-M} \right)$$
$$+ N.\lambda_{DD}.MTTR \cdot \left( \binom{N-1}{N-M} \cdot \frac{((1-\beta).\lambda_{DN}.T_2)^{N-M}}{N-M+1} \right)$$
$$+ \left( N.\frac{\lambda_{DN}.T_2}{2} \right) \cdot \left( \binom{N-1}{N-M} \cdot ((1-\beta_D).\lambda_{DD})^{N-M}.MTTR^{N-M} \right)$$
$$+ N.(\lambda_{DD}.MTTR) \cdot \left( \binom{N-1}{1} \cdot \frac{\lambda_{DN}.T_2}{2} \right) \cdot \left( \binom{N-2}{N-M-1} \cdot \frac{((1-\beta).(\lambda_{DU}-\lambda_{DN}).T_1)^{N-M-1}}{N-M+2} \right)$$
$$+ \left( N.\frac{(1-\beta).(\lambda_{DU}-\lambda_{DN}).T_1}{2} \right) \cdot \left( \binom{N-1}{1} \cdot \frac{\lambda_{DN}.T_2}{2} \right) \cdot \left( \binom{N-2}{N-M-1} \cdot ((1-\beta_D).\lambda_{DD})^{N-M-1}.MTTR^{N-M-1} \right)$$
$$+ \left( N.\frac{\lambda_{DN}.T_2}{2} \right) \cdot \left( \binom{N-1}{1} \cdot \frac{\lambda_{DU}.T_1}{2} \right) \cdot \left( \binom{N-2}{N-M-1} \cdot ((1-\beta_D).\lambda_{DD})^{N-M-1}.MTTR^{N-M-1} \right)$$
$$+ N.\frac{(\lambda_{DU}-\lambda_{DN}).T_1}{2} \cdot \left( \binom{N-1}{N-M} \cdot \frac{((1-\beta).\lambda_{DN}.T_2)^{N-M}}{N-M+1} \right)$$
$$+ N.\frac{\lambda_{DN}.T_2}{2} \cdot \left( \binom{N-1}{N-M} \cdot \frac{((1-\beta).(\lambda_{DU}-\lambda_{DN}).T_2)^{N-M}}{N-M+1} \right)$$

This model includes the averages of product terms for N-M ≤ 2

It seems complicated, but it can be modelled in a spreadsheet

…unless N-M > 2

The number of terms in the product increases with N-M

SYSTEMS

# Simplified model for synchronised testing

A correction factor can be included in the basic 'average before product' model to give the same results as the fully expanded model for synchronised tests

$$PFD_{\mathrm{MooN}\,AVG} \approx \frac{2^{\mathrm{N-M+1}}}{\mathrm{N-M+2}} \cdot \binom{\mathrm{N}}{\mathrm{N-M+1}} . (PFD_{1oo1\,AVG})^{\mathrm{N-M+1}}$$

$$+ \beta_D . \lambda_{DD} . MTTR + \beta . \frac{(\lambda_{DU} - \lambda_{DN}) . T_1}{2} + \beta . \frac{\lambda_{DN} . T_2}{2}$$

The model distinguishes between:

- Detected failures revealed by diagnostics
- Undetected failures revealed by inspection and test at intervals $T_1$
- The remaining undetected failures revealed at intervals $T_2$

SYSTEMS

# The simpler way to model limited proof test coverage

Limited test coverage increases the **average time** to reveal failures that remain undetected by diagnostics

$$T = PTC.T_1 + (1 - PTC).T_2$$

Interval between tests with partial coverage

Interval between tests with full coverage (or between demands)

# Partial stroke testing example

Annual partial stroke testing can typically achieve 60% test coverage
A full test might be carried at 6-yearly intervals:

$PTC$ = 60% $T_1$ = 1 y $T_2$ = 6 y

$$(PTC.T_1 + (1 - PTC).T_2). = 0.6 \times 1 + 0.4 \times 6 \approx 3$$

Limited test coverage typically increases $PFD$ by a factor of 2 or 3

SYSTEMS

# Simplified model with limited proof test coverage

$$PFD_{\text{MooN } AVG} \approx \frac{2^{\mathbf{N-M+1}}}{\mathbf{N-M+2}} \cdot \binom{\mathrm{N}}{\mathrm{N-M+1}} \cdot (PFD_{1oo1\ AVG})^{\mathrm{N-M+1}}$$

$$(1-\beta_D).\lambda_{DD}.MTTR + (1-\beta).\frac{\lambda_{DU}.T}{2}$$

$$+ \beta_D.\lambda_{DD}.MTTR + \beta.\frac{\lambda_{DU}.T}{2}$$

Where $T = PTC.T_1 + (1-PTC).T_2$

This model is mathematically identical to the model based on $(\lambda_{DU} - \lambda_{DN}).T_1$ and $\lambda_{DN}.T_2$

SYSTEMS

# Correction factor example – 1oo2 architecture

The basic 'average before product' model gives:

$$PFD_{1oo2\,AVG} \approx \left((1-\beta).\lambda_{DU}.T\right)^2/4 + \beta_D.\lambda_{DD}.MTTR + \beta.\lambda_{DU}.T/2$$

The 'product before average' model for synchronised tests gives:

$$PFD_{1oo2\,AVG} \approx ((1-\beta).\lambda_{DU}.T)^2/3 + \beta_D.\lambda_{DD}.MTTR + \beta.\lambda_{DU}.T/2$$

The correction factor is: $\dfrac{2^{N-M+1}}{N-M+2} = \dfrac{2^2}{3} = \dfrac{4}{3}$

SYSTEMS

# The corrected model was validated for all MooN

$$PFD_{\text{MooN } AVG} \approx \frac{2^{N-M+1}}{N-M+2} \cdot \binom{N}{N-M+1} \cdot (PFD_{1oo1\ AVG})^{N-M+1} \quad < 25\%$$

$$+ \beta_D . \lambda_{DD} . MTTR + \beta . \frac{\lambda_{DU} . T}{2} \quad > 75\%$$

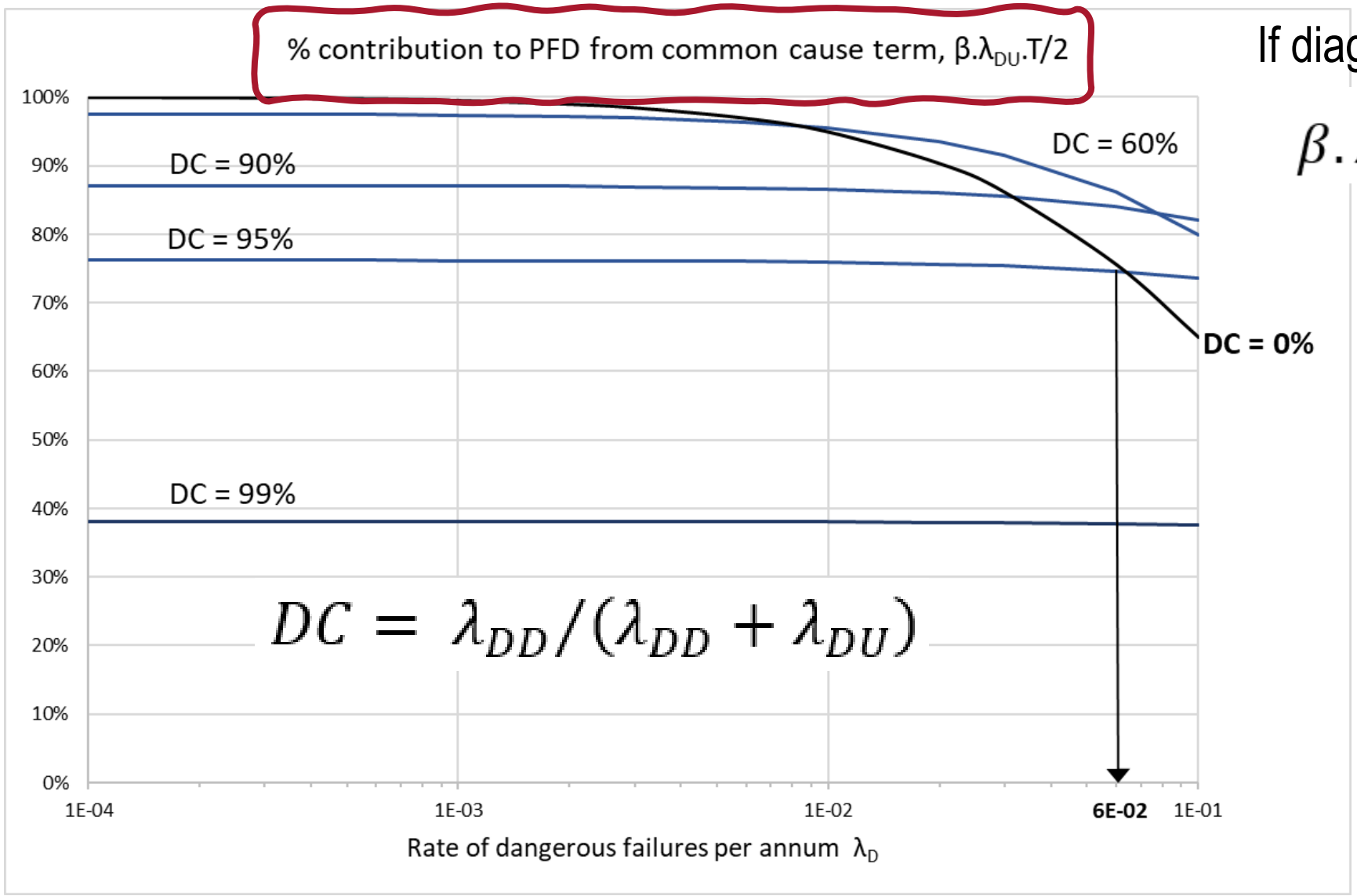
**The simplified model is within +/- 1% of the expanded model**

Analysis using these models showed that the **common cause failures** almost always account for > 75% of the $PFD$

**Undetected failures** dominate unless diagnostic coverage > 95%

SYSTEMS

# Varying diagnostic coverage




$$DC = \lambda_{DD}/(\lambda_{DD} + \lambda_{DU})$$

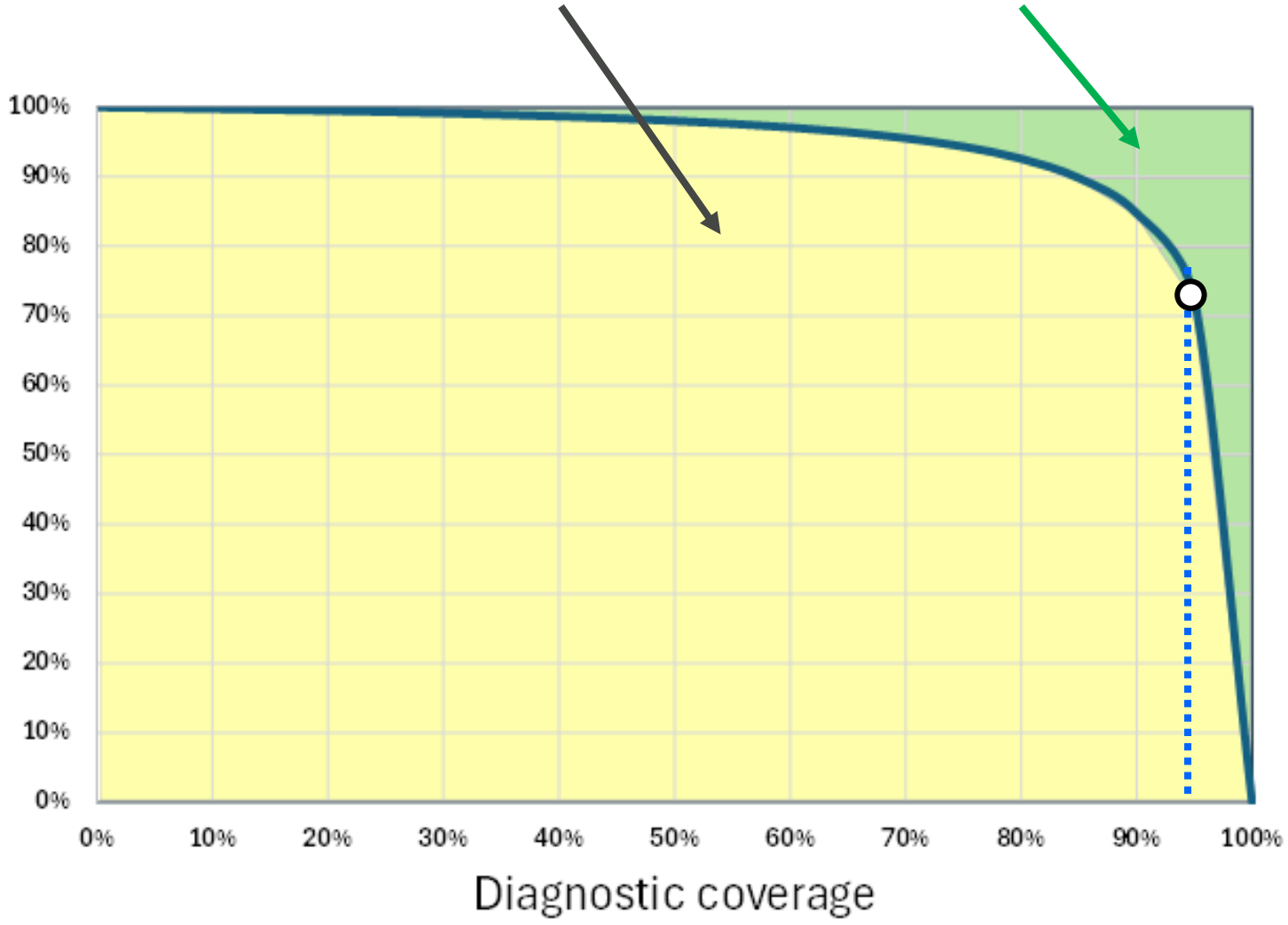
If diagnostic coverage ≤ 95%, then

$$\beta.\lambda_{DU}.T/2 > 3/4.PFD$$

# Undetected faults dominate unless $DC$ > 95 %

% contributions to $PFD_{1oo1}$ from $\lambda_{DU}.T/2$ and $\lambda_{DD}.MTTR$

$T$ = 1 y and
$MTTR$ = 0.01 y




SYSTEMS

# Simple approximations are just as accurate

If diagnostic coverage > 95% , then

$$PFD_{AVG} \approx \beta_D . \lambda_{DD} . MTTR + \beta . \lambda_{DU} . T/2$$

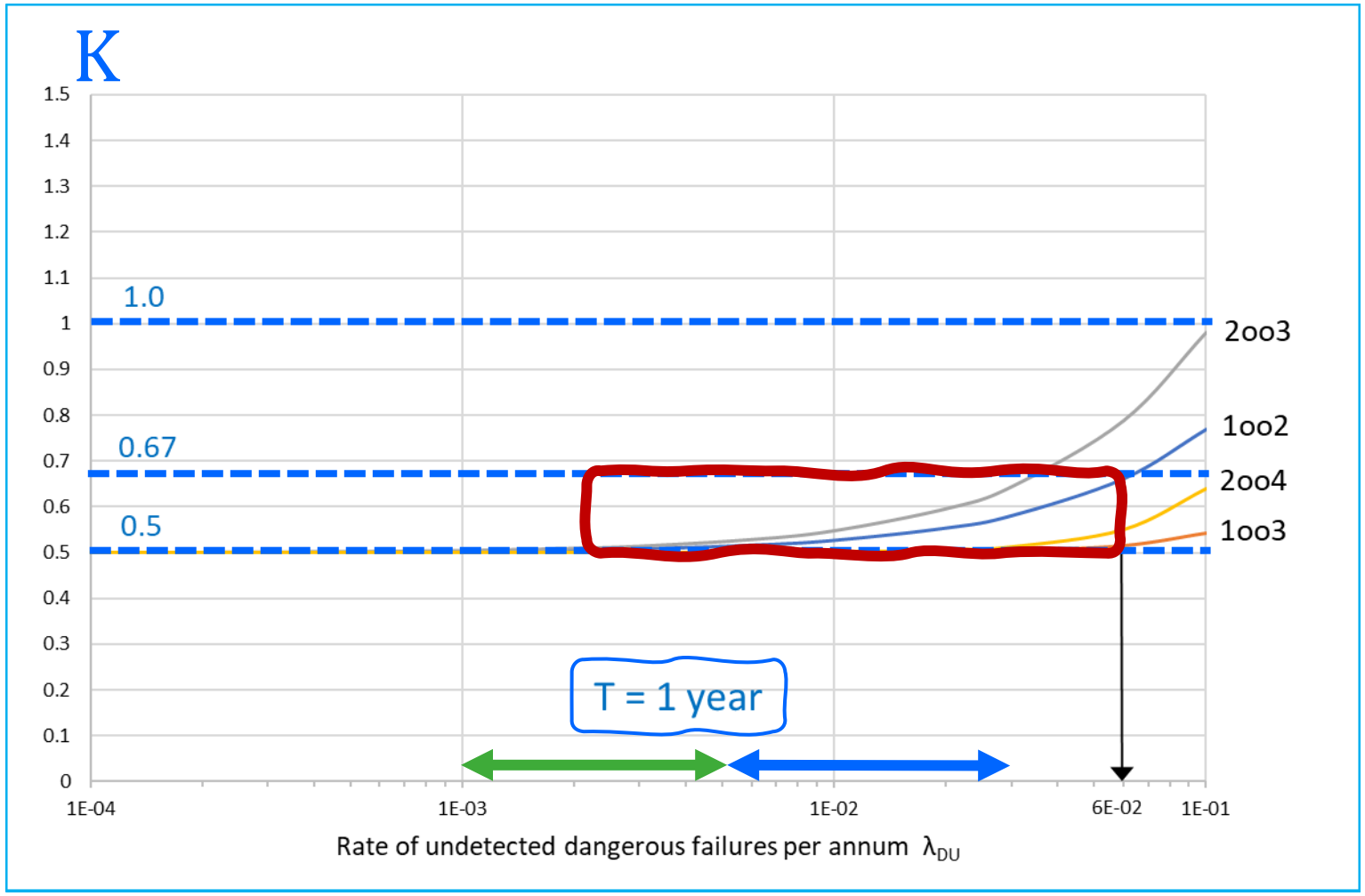
With diagnostic coverage ≤ 95%, $\beta . \lambda_{DU} . T/2 > 3/4 . PFD$

and $\beta . \lambda_{DU} . T/2 < PFD < 2/3 . \beta . \lambda_{DU} . T$

So…. $\boldsymbol{PFD < 2/3 . \beta . \lambda_{DU} . T}$ …but within what limits?

SYSTEMS

# For ***any*** MooN: $PFD \approx \mathrm{K}.\ \beta.\lambda_{DU}.T$




Typical range of $\lambda_{DU}$ Sensors Final elements

For most common applications K is between 0.5 and 0.67

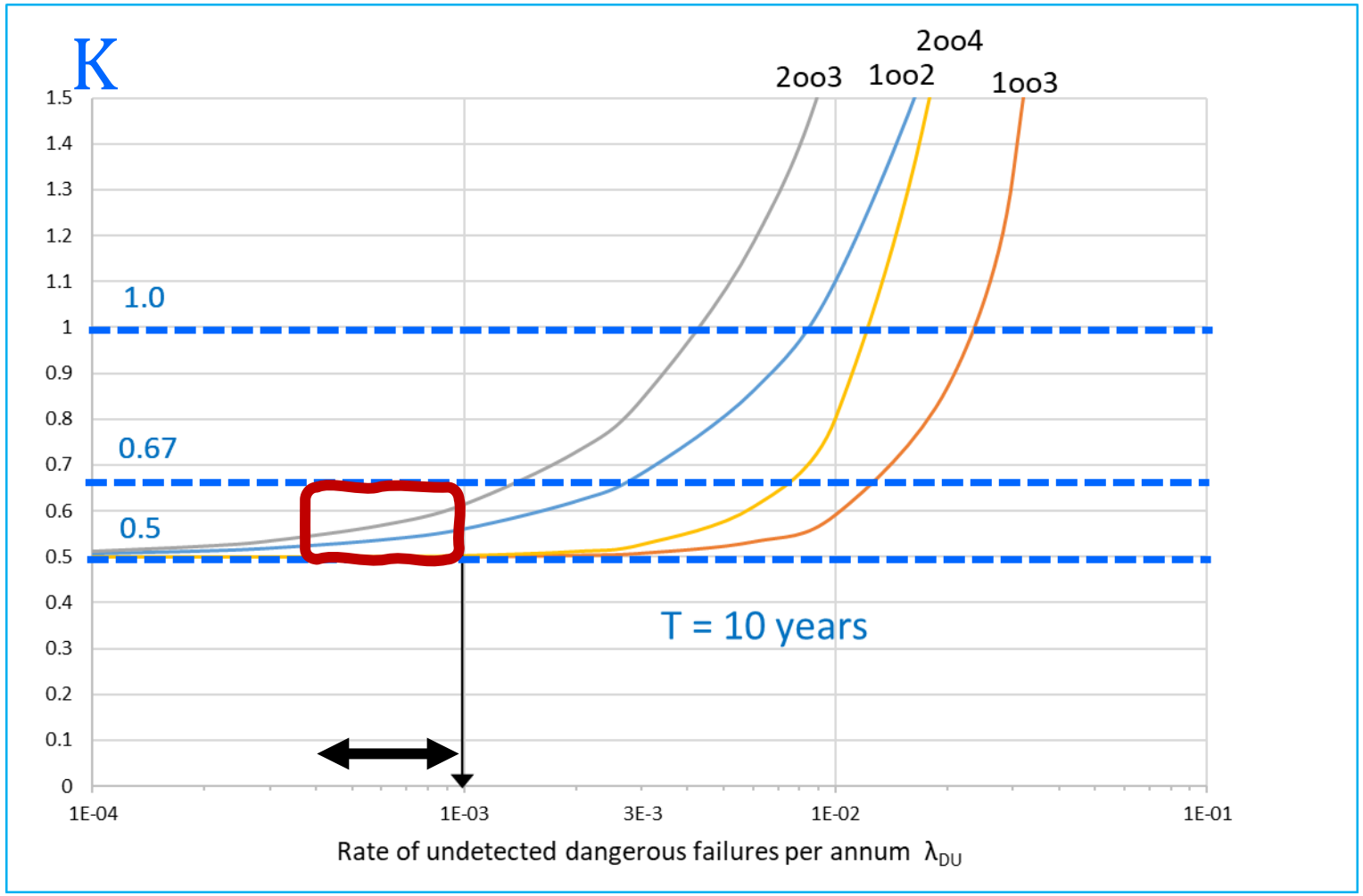
K increases with $T$, but

2oo3 and higher order architectures usually have enough diagnostic coverage to achieve $\lambda_{DU}$ < 0.01 pa

$T$ > 3 y might be used if $\lambda_{DU}$ < 0.01 pa, so is the approximation still valid?

SYSTEMS

# What about logic solvers with $T$ = 10 years?




Logic solvers may have $T$ > 10 years

but usually have $DC$ > 95% and $\lambda_{DU}$ < 0.001 pa

(about 100 FITS or $10^{-7}$ $h^{-1}$)

Logic solvers (assuming $\beta_{INT}$ = 0.05)

# Logic solvers usually have $DC > 90\%$ and $\beta_{INT} < 0.05$

For logic solvers we could use

$$PFD_{AVG} \approx \beta_D . \lambda_{DD} . MTTR + \beta . \lambda_{DU} . T/2$$

Is this realistic, or purely academic? What will the fault reaction be?

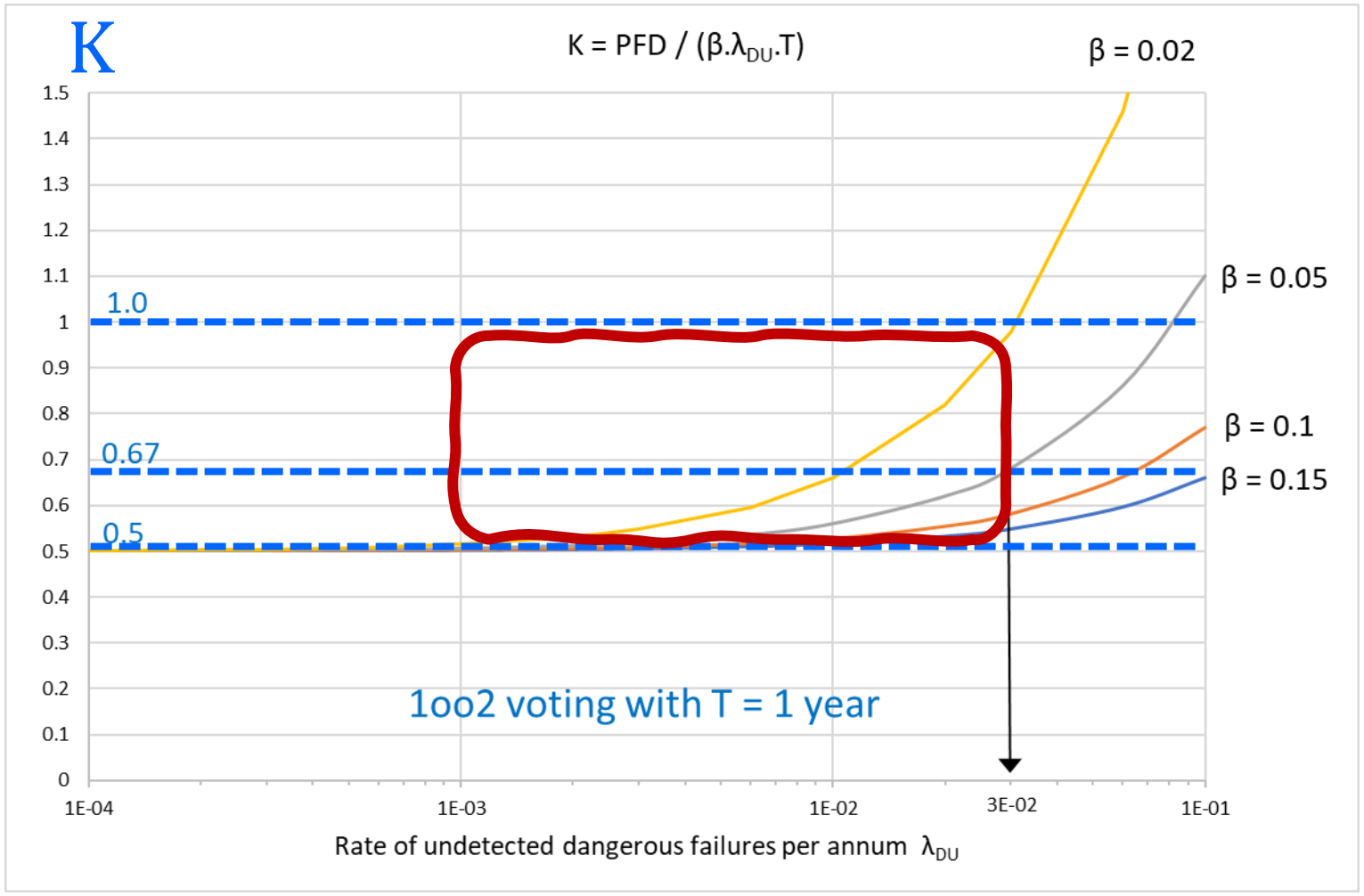
The approximation $PFD_{AVG} \approx {}^{2}/_{3} . \beta . \lambda_{DU} . T$ is still close enough

Logic solver $PFD$ is typically in the order of $10^{-6}$ to $10^{-5}$

Precise estimates cannot be expected

SYSTEMS

# Diverse channels may have $\beta_{INT} < 0.02$




$PFD < \beta.\lambda_{DU}.T$ is usually valid for $\beta_{INT} > 0.02$

$\beta_{INT} < 0.02$ may be needed for $RRF \geq 10{,}000$

Carry out detailed analysis with FMEA for $\beta_{INT} < 0.02$

$PFD_{AVG} \approx \beta.\lambda_{DU}.T$ could be used with $\beta_{INT} < 0.02$

# Precision can never be justified

- The validity of $\beta$ models is questionable for diverse channels
- Uncertainty in the $\beta$ for any MooN is typically +/- 50%
- ***All*** failure rates usually vary ***more*** than between 0.3 $\lambda$ and 3 $\lambda$
- Failure rates > 0.01 pa (MTBF 100 years) are mostly dependent on service conditions and human actions (systematic factors); even wider variation can be expected
- Detailed models are **not more accurate** than simple approximations

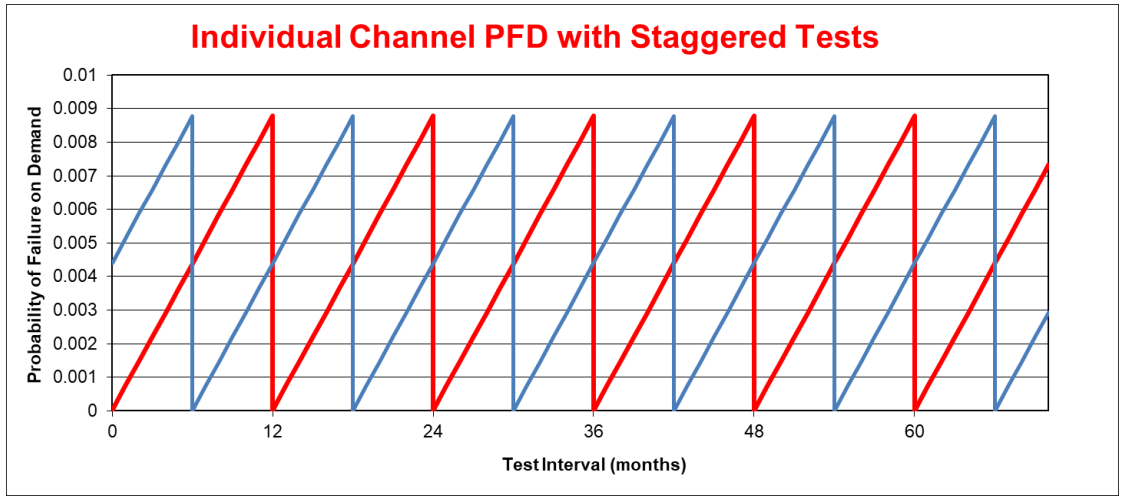
SYSTEMS

# Perfectly staggered testing **reduces** *PFD*

Refer to The 61508 Association paper T6A 042 for detailed analysis

For 1oo2 architecture

$$PFD_{AVG} \approx \frac{5}{6} \cdot \left(\frac{\lambda_{DU} \cdot T_1}{2}\right)^2 \quad \text{instead of} \quad \left(\frac{\lambda_{DU} \cdot T_1}{2}\right)^2$$




Correction factors $\mathbf{St_{M,N}}$ for different N and M, based on T6A 042

| $St_{M,N}$ | N | | | | | |
|---|---|---|---|---|---|---|
| M | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 0.83 | 0.67 | 0.52 | 0.41 | 0.31 | 0.24 |
| 2 | | 0.89 | 0.75 | 0.61 | 0.49 | 0.39 |
| 3 | | | 0.92 | 0.8 | 0.68 | 0.56 |
| 4 | | | | 0.93 | 0.83 | 0.72 |
| 5 | | | | | 0.94 | 0.86 |
| 6 | | | | | | 0.95 |

$$PFD_{\mathrm{MooN}\,AVG} \approx \mathrm{St_{M,N}} \cdot \binom{\mathrm{N}}{\mathrm{N-M+1}} \cdot \left(\frac{\lambda_{DU} \cdot T}{2}\right)^{\mathrm{N-M+1}}$$

(note that T6A 042 uses different definitions of M and N)

# Low-demand mode with staggered tests

Systems with evenly staggered testing may be modelled in detail by:

$$PFD_{\mathrm{MooN}\,AVG} \approx \mathrm{St}_{\mathrm{M,N}} \cdot \binom{\mathrm{N}}{\mathrm{N-M+1}} \cdot (PFD_{1oo1\,AVG})^{\mathrm{N-M+1}} + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \frac{\lambda_{DU} \cdot T}{2}$$

where $T = PTC \cdot {}^{T_1}/_{\mathrm{N}} + (1 - PTC) \cdot {}^{T_2}/_{\mathrm{N}}$

The main benefit of staggered testing is in **reducing the average time to reveal undetected common cause failures**

This simple approximation is still valid, and just as accurate:

$$PFD_{AVG} \approx {}^{2}/_{3} \cdot \beta \cdot \lambda_{DU} \cdot T$$

# Summary - for any low demand application

Simple approximations can be used to estimate failure probability for any low-demand mode safety functions

for MooN $$PFD_{AVG} \approx {}^{2}/_{3}.\beta.\lambda_{DU}.T$$

for NooN $$PFD_{AVG} \approx \mathrm{N}.\lambda_{DU}.T/2$$ (zero fault tolerance)

With diagnostic coverage >95 % we *could* use:

for MooN $$PFD_{AVG} \approx \beta_D.\lambda_{DD}.MTTR + \beta.\lambda_{DU}.T/2$$

for NooN $$PFD_{AVG} \approx \mathrm{N}.\lambda_{DD}.MTTR + \mathrm{N}.\lambda_{DU}.T/2$$

… but only if we are sure that normal operation will continue for $MTTR$

SYSTEMS

# Risk reduction factor estimates

Reciprocal formulas can be used to quickly estimate $RRF$ from the overall $MTBF_{DU}$ of a single channel:

For NooN $RRF \approx 2.\frac{MTBF_{DU}}{\mathrm{N}.T}$ and for MooN $RRF \approx \frac{3}{2}.\frac{MTBF_{DU}}{\beta.T}$

For example, with $\beta_{\mathrm{int}}$ = 0.1 and $T$ = 1 y:

| $MTBF_{DU}$ | $RRF$ with 1oo1 | $RRF$ with 1oo2 | $RRF$ with 1oo3 |
|---|---|---|---|
| 30 y | 60 | 500 | 1,000 |
| 100 y | 200 | 1,500 | 3,000 |
| 300 y | 600 | 5,000 | 10,000 |

SYSTEMS

# Low demand example: Typical values for $MTBF$ and $\lambda$

What $PFD$ can be achieved?

**Refer to silsafedata.com for failure rates that are feasible**

- Sensors:
  $MTBF_{DU}$ range 100 to 300 years, $\lambda_{DU} \approx 0.003$ to 0.01 pa
  $MTBF_{DD}$ range 30 to 100 years, $\lambda_{DD} \approx 0.01$ to 0.03 pa

- Actuated valve assemblies:
  $MTBF_{DU}$ range 30 to 100 years, $\lambda_{DU} \approx 0.01$ to 0.03 pa
  usually no diagnostics, $\lambda_{DD} = 0$

**Assume $\lambda_{DU} \approx 0.02$ pa**

- Contactors or relays:
  $MTBF_{DU}$ range 100 to 300 years, $\lambda_{DU} \approx 0.003$ to 0.01 pa
  usually no diagnostics, $\lambda_{DD} = 0$

SYSTEMS

# Example dual channel SIF with 1oo2 voting

$$PFD_{AVG} \approx \frac{\lambda_{DU}^{2}.T^{2}}{3} + \frac{\beta.\lambda_{DU}.T}{2} + \beta_D.\lambda_{DD}.MTTR$$

Sensor $PFD \approx$ (0.003 pa x 1 y)$^2$ / 3 + 0.1 x 0.003 pa x 1 y / 2 + 0.1 x 0.01 pa x 0.01 y

$\approx$ 0.00003 + **0.00015** + 0.00001 $\approx$ 0.00019

Valve $PFD \approx$ (0.02 pa x 1 y)$^2$ / 3 + 0.1 x 0.02 pa x 1 y / 2

$\approx$ 0.00013 + **0.001** $\approx$ 0.0011

SIF $PFD \approx$ 0.0002 + **0.0011** $\approx$ 0.0013

$RRF \approx$ 750, SIL 2 range

Obviously: $PFD > \beta.\lambda_{DU}.T/2$

# 1oo2 voting example with simple approximation

$$PFD_{AVG} \approx \frac{\lambda_{DU}^{2}.T^{2}}{3} + \frac{\beta.\lambda_{DU}.T}{2} + \beta_{D}.\lambda_{DD}.MTTR$$

$$PFD_{AVG} \approx \frac{2}{3}.\beta.\lambda_{DU}.T$$

Sensor $PFD \approx$ 2/3 x 0.1 x 0.003 pa x 1 y

$\approx$ 0.0002

Valve $PFD \approx$ 2/3 x 0.1 x 0.02 pa x 1 y

$\approx$ 0.0013

SIF $PFD \approx$ 0.0002 + 0.0013 ≈ 0.0015

$RRF \approx$ 650 (compared with 750 from the detailed estimate)

The 15% difference is academic given the uncertainty in failure rates

SYSTEMS

# Using the reciprocal form:

$$RRF \approx \frac{3}{2} . \frac{MTBF_{DU}}{\beta . T}$$

$\lambda_{DU}$ ≈ 0.003 pa + 0.02 pa

$MTBF_{DU}$ ≈ 1/0.023 ≈ 44 y

$RRF$ ≈ 3/2 x 44 y /(0.1 x 1) ≈ 650

SYSTEMS

# Continuous mode and high demand mode functions

For MooN $\lambda_D^{SF} \approx \beta . \lambda_D$

For NooN $\lambda_D^{SF} \approx \mathrm{N} . \lambda_D$

Detected failures may be excluded if there is an appropriate fault reaction

# Conclusions

Safety function performance is always **variable**; it depends primarily on:

- The rate of undetected failures
- Time taken to reveal undetected failures
- Common cause failure fraction

Simple approximations are just as accurate as the fully detailed models

SYSTEMS

# Conclusions

Failure probability can be reduced by orders of magnitude through:

- Selection of equipment suitable for the service and environment
- Reliability centered maintenance
- Automatic diagnostics
- Proof test and inspection
- Staggered testing
- Diversity between voted channels

**Conclusions:**
**FMEA is useful**

**Complicated mathematics is not necessary**

**The 'informative' formulas in IEC 61508-6 need to be clarified in Ed. 3**

…and no, we should not usually need a calculator

SYSTEMS