Chapter 10.
Common Cause Failures (CCFs)

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 become familiar with:

- What a CCF is
- The relationship between dependent failures and CCFs
- Key attributes of CCFs: Root causes and coupling factors
- Defence strategies to avoid introducing CCfs
- Some selected approaches for how model CCFs using some selected approaches
- Some selected approaches for how to determine “CCF parameter” beta (β)

Outline of Presentation

Background

Common cause failures (CCF) represent events where multiple failures occur due to a shared cause. They are important to consider because they can violate the effects of redundancy.

Nuclear industry has been in the forefront of developing knowledge and methods:

- First guideline on the modeling of CCF modeling was published by Nuclear Regulatory Agency in 1975 "Reactor Safety Study," WASH-1 400"
- Several other guidelines were published in period from 1989-2007 (NUREG/CR- 4780, NUREG/CR-5485, NUREG/CR-6268, NUREG/CR-6303)
- An International Common-cause Failure Data Exchange (ICDE) Project on CCF data collection and analysis was initiated in 1994 and is still on-going

Today, "all" standards on functional safety require that CCFs are taken into account - regardless of industry domain and application area

CCFs - a Sub-Category of Dependent Failures

CCFs are a sub-category of dependent failures.

What is a dependent failure?

- Consider two items, 1 and 2, and let E_i denote the event that item i is in a failed state. The probability that both items are in a failed state is:

$$\Pr(E_1 \cap E_2) = \Pr(E_1 \mid E_2) \cdot \Pr(E_2) = \Pr(E_2 \mid E_1) \cdot \Pr(E_1)$$

- The two items, 1 and 2, are dependent when

$$\Pr(E_1 \mid E_2) \neq \Pr(E_1) \quad \text{and} \quad \Pr(E_2 \mid E_1) \neq \Pr(E_2)$$

Positive and Negative Dependence

There are two types of dependencies: positive and negative dependence.

- Items 1 and 2 are said to have a positive dependence when $\Pr(E_1 \mid E_2) > \Pr(E_1)$ and $\Pr(E_2 \mid E_1) > \Pr(E_2)$, such that

$$\Pr(E_1 \cap E_2) > \Pr(E_1) \cdot \Pr(E_2)$$

- Items 1 and 2 are said to have a negative dependence when $\Pr(E_1 \mid E_2) < \Pr(E_1)$ and $\Pr(E_2 \mid E_1) < \Pr(E_2)$

$$\Pr(E_1 \cap E_2) < \Pr(E_1) \cdot \Pr(E_2)$$

where E_i is the event that item i is in a failed state. ‘

A CCF represents a positive dependence.

No Commonly Accepted Definition

- Despite being a topic for analysis for almost five decades, there is no generally accepted definition of CCFs.
- For this reason, may guidelines, standards, and textbooks have suggested their own, depending on the application and context.

The following slides give some samples of definitions.

Definition of CCFs - (I)

Nuclear industry (NEA, 2004):

☞ 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.

Space industry (NASA PRA guide, 2002):

☞ The failure (or unavailable state) of more than one component due to a shared cause during the system mission.

Functional safety standards (IEC 61508, 2010):

☞ Failure, that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to system failure.

SIS textbook suggests:

☞ Failure, that is the direct result of a shared cause, in which two or more separate channels in a multiple channel system are in fault state simultaneously, leading to system fault.

Definition of CCFs - (II)

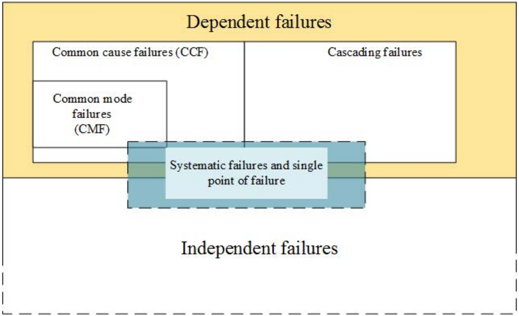
The definition of Smith and Watson (1980) is perhaps the most comprehensive one:

1. The items affected are unable to perform as required
2. Multiple failures exist within (but not limited to) redundant configurations
3. The failures are "first-in-line" type of failures and not the result of cascading failures
4. The failures occur within a defined critical time period (e.g., the time a plane is in the air during a flight)
5. The failures are due to a single underlying defect or physical phenomenon (the "common cause")
6. The effect of failures must lead to some major disabling of the system's ability to perfor as required

CCFs and Other Dependent Failure Types

Other Dependent Failure Types include:

- Common mode failures (CMFs), which are a subcategory of CCFs,
- Cascading failures.



Two Categories of CCFs

In general, we can distinguish between the following two categories of CCFs:

(a) CCFs that occur at the **same time** due to a **shock**, or

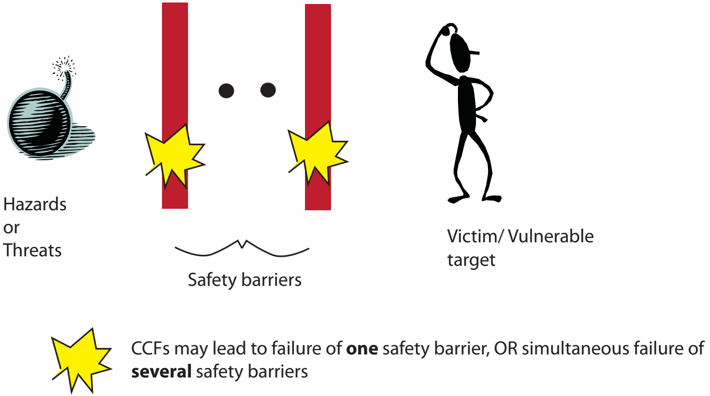
(b) CCFs that occur **over a certain time interval** due to an **increased stress** (e.g. temperature, humidity, vibrations)

It may be remarked that:

- Shocks are often modeled by a homogeneous Poisson Process.
- The mean time a SIF has been unavailable due to a CCFs of category (a) is $\tau/2$ in case the CCF is revealed by a proof test
- The mean time that a SIF has been unavailable due to a CCFs of category (b) depends on the system architecture (voting) and the degradation processes

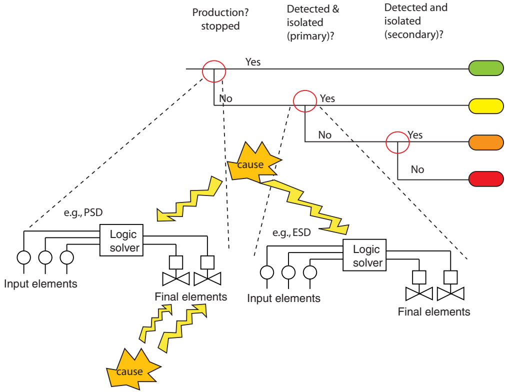
Impact of CCFs

CCFs may violate the performance of an individual safety barrier, or result in the simultaneous failure of several safety barriers.



Example 2: Impact of CCFs

CCFs may violate the performance of an individual safety barrier, or result in the simultaneous failure of several safety barriers.



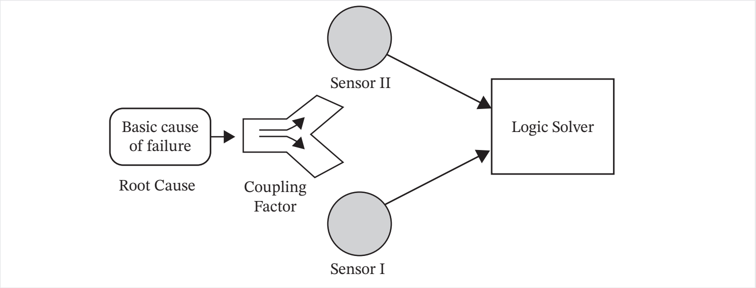
Attributes

Root Causes and Coupling Factors

The shared cause of a CCF may be split into two elements: the root cause and the coupling factor.

- Root cause: The most basic cause of failure of an item that, if corrected, would prevent the occurrence of this and similar faults.
- Coupling factor: A property (commonality) that make multiple items susceptible to failure from a shared cause.

A possible visualization is shown below.



Types of Root Causes

Root causes can be introduced already before the system is put into operation:

- Specification error: Lack of specification or improper specification
- Implementation error: Design errors (hardware, software, preparation of interaction)
- Installation error
- Commissioning and testing error

Failures not revealed are transferred to the operational phase. In operation, the system may also experience:

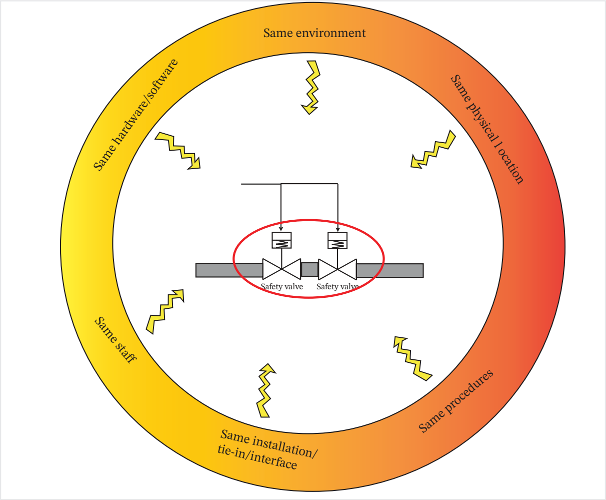
- Maintenance errors
- Operational errors
- Stress exposure beyond design limits

Examples of Coupling Factors

To look for coupling factors is the same as to look for commonalities, which in combination with root cases can result in failure of multiple items. Examples include:

- Same design (principles)
- Same hardware
- Same function
- Same software
- Same installation staff
- Same maintenance and operational staff
- Same procedures
- Same system/item interface
- Same environment
- Same (physical) location

Visualization



Defense Strategies

“ Defense strategies” is about reducing the probability of having CCFs. This include measures to:

- Reduce the occurrence of root causes
- Reduce existence of coupling factors
- A combination of both

Defense Strategies: Reduce Occurrence of Root Causes

The occurrence of root causes may be reduced by:

- Increase inherent reliability of each item: Installing more reliable and robust components
- Environmental control:
  - Ensuring that operating environment is within design constraints
  - Reduce shock-like exposures
  - Diagnostic testing and coverage
- Check for CCFs during at regular tests and maintenance

Strategies to reduce occurrence of root causes are effective for dependent *as well as for* independent failures.

Defense Strategies: Reduce Coupling Factors

Reducing coupling factors is about modifying properties of the design, installation or use.

Coupling factors may be reduced by:

- Introducing separation and segregation of redundant items (physical, functional, electrical)
- Introducing diversity in hardware and software
- Simplifying architecture and design, to avoid having undiscovered couplings
- Using analyses to detect design vulnerabilities, such as FMECA, zonal analysis*, particular risks analysis*, common mode analysis*

*CCF analysis methods suggested in aviation standards, like ARP4754A and ARP 4761.

Typical Steps of Modeling

Modeling and analysis of CCFs can include:

1. Development of system logic models: Includes functional models, failure models, and reliability models
2. Identification of common cause component group (CCCG): Includes the identification of component groups that share some common vulnerability or dependency
3. Identification of root causes and coupling factors
4. Assessment of defense strategies (including updating the model in case of system being modified)
5. Explicit modeling of CCFs: Adding explicit causes of CCFs
6. Implicit modeling of CCFs: Adding implicit causes of CCFs
7. Quantification and interpretation of results

Explicit Modeling

Explicit modeling means to:

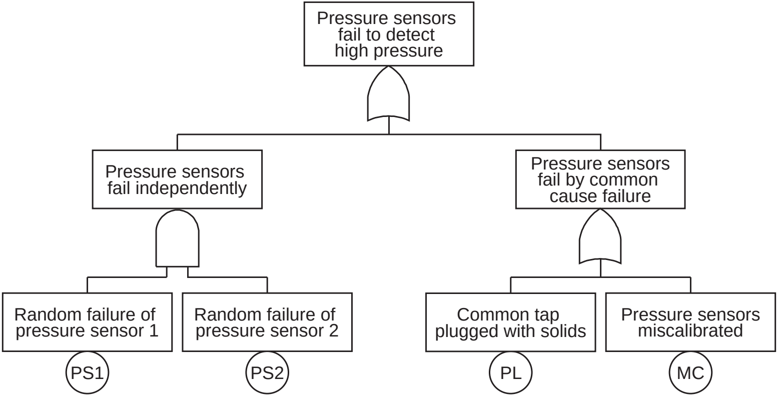
- Add each specific cause of CCF into the reliability model.

Specific causes include:

- Human errors
- Utility failures (e.g., power failure, cooling/heating failure, loss of hydraulic power)
- Shared equipment
- Environmental events (e.g., lightning, flooding, storm)

Explicit modeling may be chosen when data is available to support these basic events/elements.

Explicit Modeling: Illustrative Example



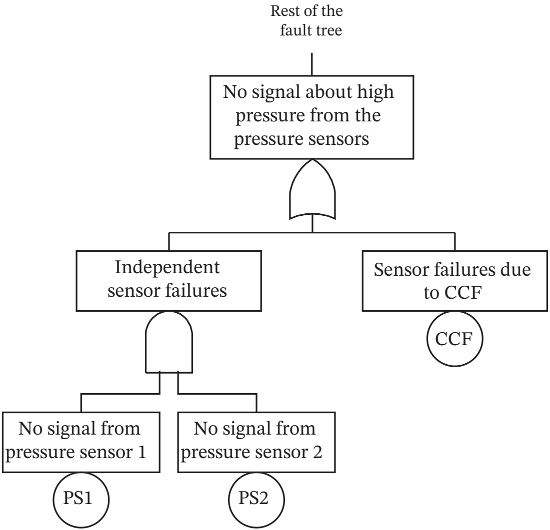
Implicit modeling

Implicit modeling means to:

- Add events that cover residual causes of CCFs

Implicit modeling may be chosen when data is not available to support explicit modeling.

Implicit Modeling: Illustrative Example



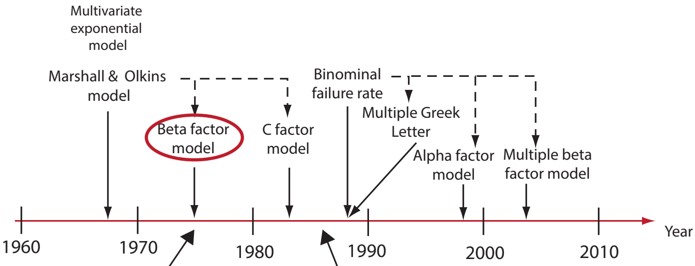
Overview of Implicit CCF models

There are several implicit models, and many of these have its origin in the Nuclear industry. Some examples are:

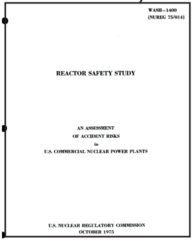
- C-factor model
- **Beta-factor model**
- Alpha-factor model
- Multiple Greek Letter model
- **Multiple beta-factor model**
- **Binomial failure rate model**

The models in **bold text** are focused here.

Implicit Modeling - In Historial Perspective



Key studies for including CCFs in reliability assessments

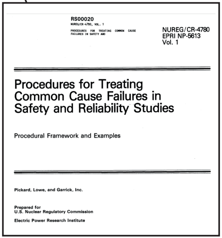


WASH–1400
(NUREG 75/014)

REACTOR SAFETY STUDY

AN ASSESSMENT
OF ACCIDENT RISKS
in
U.S. COMMERCIAL NUCLEAR POWER PLANTS

U.S. NUCLEAR REGULATORY COMMISSION
OCTOBER 1975



RS00020

NUREG/CR-4780
EPRI NP-5613
Vol. 1

Procedures for Treating Common Cause Failures in Safety and Reliability Studies

Procedural Framework and Examples

Pickard, Lowe, and Garrick, Inc.

Prepared for
U.S. Nuclear Regulatory Commission
Electric Power Research Institute

Beta-Factor Model: Most Widely Accepted

Beta-factor model was introduced by K.N Fleming in 1975. It is perhaps the most commonly used approach across industry sectors.

Basic assumption is that the failure rate λ is split into an independent part λ_I and a dependent part λ_c:

$$\lambda = \lambda^{(i)} + \lambda^{(c)}$$

In addition, a parameter beta-factor (β) is defined as

$$\beta = \frac{\lambda^{(c)}}{\lambda}$$

which means that:

$$\lambda = (1 - \beta)\lambda + \beta\lambda$$

Interpretation of β

There are two main interpretations of β:

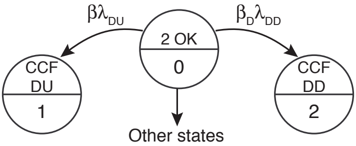
- β is the *fraction* all failures of a channel that are CCFs
- β is the *conditional probability* that a failure of a channel is a CCF:

$$\beta = \Pr(\text{CCF}|\text{Failure of a channel})$$

Beta-Factor Model and SIF

A SIS component may fail dangerously due to dangerous detected (DD) failures or dangerous undetected (DU) failures. We often introduce a separate β for the two; β for DU failures and β_D for DD failures.

A Markov model can be used to illustrate the difference between β and β_D in a system with redundant components, as shown below:



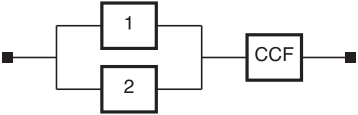
The overall rate of dangerous CCFs become:

$$\lambda^{(c)} = \beta\lambda_{DU} + \beta_D\lambda_{DD}$$

Illustrative Example for a 1oo2 Voted System

We consider a group of two identical channels voted 1oo2 with DU failure rate λ_{DU}. The system operated in the low-demand mode and is subject to regular perfect proof tests with interval τ.

The corresponding reliability block diagram is:



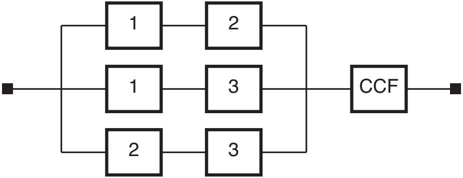
The corresponding formula for the average probability of failure on demand (PFD) becomes:

$$\text{PFD}_{\text{avg}} \approx \underbrace{\frac{[(1-\beta)\lambda_{\text{DU}}\tau]^2}{3}}_{\text{Indvidual}} + \underbrace{\frac{\beta\lambda_{\text{DU}}\tau}{2}}_{\text{CCF}}$$

Illustrative Example for a 2oo3 Voted System

We consider a group of two identical channels voted 2oo3 with DU failure rate λ_{DU}. The system operated in the low-demand mode and is subject to regular perfect proof tests with interval τ.

The corresponding reliability block diagram is:



The corresponding formula for the average probability of failure on demand (PFD) becomes:

$$\text{PFD}_{\text{avg}} \approx \underbrace{((1-\beta)\lambda_{\text{DU}}\tau)^2}_{\text{Individual}} + \underbrace{\frac{\beta\lambda_{\text{DU}}\tau}{2}}_{\text{CCF}}$$

An Observation from the Two Examples

The two previous examples show that the CCF part is the same regardless of how a system with redundant channels is voted.

This is shown here:

$$\begin{aligned}
\mathrm{PFD}_{\mathrm{avg,a}} &\approx \frac{[(1-\beta)\lambda_{\mathrm{DU}}\tau]^2}{3} + \frac{\beta\lambda_{\mathrm{DU}}\tau}{2} \\
\mathrm{PFD}_{\mathrm{avg,b}} &\approx [(1-\beta)\lambda_{\mathrm{DU}}\tau]^2 + \frac{\beta\lambda_{\mathrm{DU}}\tau}{2}
\end{aligned}$$

This comparison shows that the beta-factor model always assumes that *all* channels fail if a CCF occurs.

Beta-Factor Model for Nonidentifical Channels

The original beta-factor was defined for *identical* channels with the same constant failure rate. In many practical cases, one may find that redundant channels are non-identical. For example, a subsystem to detect gas in a process area may comprise different types of gas detectors.

In order to apply the beta-factor model, we introduce a "representative" failure rate for the channels, assuming geometric mean of the DU failure rates. We demonstrate for a system of two redundant channels voted1oo*n*:

$$\lambda_{\mathrm{DU}} = \left(\prod_{i=1}^{n} \lambda_{\mathrm{DU},\,i} \right)^{1/n}$$

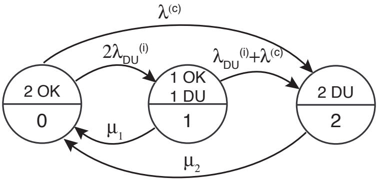
This failure rate is then used in formulas for e.g. PFD_{avg}.

This approach may be adequate when all the DU failure rates are in the same order of magnitude. Otherwise, the result may be unrealistic. See examples in SIS textbook.

Beta-Factor Model with Markov Approach

The Markov approach is a flexible approach to model also the effect of degradation and repairs.

The following model represents the states and transitions of a 1oo2 system subject to DU failures and CCFs:



The attention should be made to the transition μ_2:

- Without CCF included in the model, the transition from state 2 to 1 is $\frac{\tau}{3}$
- With CCFs transition included, the same transition becomes $\frac{\tau}{2}$

How to Determine the Value of β

β may be determined by:

- Expert judgment
- Checklists developed for the purpose
- Estimation based real data from use

Humphreys Checklist

Humphreys proposed already in 1987 a checklist for determining β. The checklist is also part of the Unified partial method (UPM).

Factor	Subfactor	Weights				
		a	b	c	d	e
Design	Separation	2400	580	140	35	8
	Similarity	1750	425	100	25	6
	Complexity	1750	425	100	25	6
	Analysis	1750	425	100	25	6
Operation	Procedures	3000	720	175	40	10
	Training	1500	360	90	20	5
Environment	Control	1750	425	100	25	6
	Tests	1200	290	70	15	4

Humphreys Checklist

Some remarks about the checklist:

- It is assumed that β is influenced by three main factors: design, operation, and environment.
- A set of sub-factors is defined for each of these.
- Each sub-factor is judged, and a level "a" (worst) to "e" (best) is assigned.
- Each combination of a letter and a subfactor is assigned as score score as seen in the table
- The score, when summed up for all subfactors, is divided by 50000. The extremes (or anchoring points) are:
  - If all sub-factors are assigned level "a", then $\beta = 0.30$.
  - If all sub-factors are assigned level "b", then $\beta = 0.001$
- All selections of entry points are based on expert judgments

Checklist in IEC 61508

IEC 61508, Part 6, Annex D presents a checklist of 37 questions to be used in relation to SIS devices. The questions are grouped into the following categories:

1. Physical design (20 questions)
    - Separation/segregation (5)
    - Diversity/redundancy (9)
    - Complexity/design/application/maturity/experience (6)
2. Analysis (3 questions)
    - Assessment/analysis and feedback of data
3. Human/operator issues (10 questions)
    - Procedures/human interface (8)
    - Competence/training/safety culture (2)
4. Environmental issues (4 questions)
    - Environmental control (3)
    - Environmental testing (1)

Application of Checklist in IEC 61508

The checklist is used as follows:

- Each question asks whether a specific measure is available
- For each question, there is a corresponding score X_{SF} and Y_{SF}.
- If the question has a positive answer ("yes"), the score is added, otherwise the score is zero.
- After all questions have been answered, the sum of each column X_{SF} and Y_{SF} is calculated
- A gives a value of β based on the calculated $\sum X_{SF} + \sum Y_{SF}$. Values ranges between 0.5% and 5% (for logic solvers) and between 1% and 10% for sensors and final elements
- Additional formula available to determine β_D for DD failures: $\sum X_{SF}(Z+1) + \sum Y_{SF}$. Value of Z is selected from a table.

Challenges with the IEC 61508 checklist

Some critique have been raised against the checklist in IEC 61508:

- Many of the questions are ambiguous and difficult to answer, even by those that are designers
  Example: "Are all devices /components conservatively rated (e.g. by a factor of 2 or more)?
- Some questions ask for practices that are uncommon in some industries
  Example: Diversity is given high credit, but in some sectors it is not a desired strategy due to e.g. complexity and possibility of human errors during maintenance.
- The scores seem a bit arbitrary and they are not explained.
- It is not advocating improvement. No change in the value of β is seen from improving according to one or a few questions.

Checklist in IEC 62061

IEC 62061 has suggested their own checklist for machinery. Questions or statements are evaluated, and scores are assigned to the following factors:

1. Separation/segregation
2. Diversity/redundancy
3. Complexity/design/application
4. Assessment/analysis
5. Competence/training
6. Environmental control

The result gives a β in the same range as with the approach in IEC 61508 (double check). Many users may find that this checklist is simpler to use than the checklist in IEC 61508.

Binomial failure rate (BFR) model

- The binomial failure rate (BFR) model is suggested in IEC 61508 as an alternative approach to the standard beta-factor model
- BFR model was Vesely in 1977, using the following assumptions:
  - A system is a voted group of identical channels
  - The channels are exposed to randomly occurring shocks according to a homogeneous Poisson process with rate ν.
  - Each of the individual channels is assumed to fail with probability p, independent of the states of the other channels.
  - The number of channels failing, Z, is binomial distributed with parameter (n,p).

Binomial failure rate (BFR) model

- The *channel* failure rate can be split into two parts,:

$$\lambda = \lambda_i + p \cdot v$$

where λ_i is the individual failure rate caused by internal failure causes and $p \cdot v$ is the additional failure rate caused by shocks. Here, v is the degree of stress (in terms of a stress frequency) and p is the built in resistance against shocks.

Binomial failure rate (BFR) model

Consider a system consisting of n channels. The probability of having exactly z of the channels failing due to the shock is:

$$\Pr(Z = z) = \binom{n}{z} p^z (1 - p)^{n-z}$$

for $z = 0, 1, \ldots, n$.

Assume that the system is voted $k$oo$n$ system. In this case the system fails if there are $n - k + 1$ or more failures. The CCF failure rate (due to shocks) $\lambda^{(c)}$ becomes:

$$\lambda^{(c)} = p_s \nu$$

where p_s is the probability of having $n - k + 1$ or more faults, i.e.

$$p_s = \sum_{i=n-k+1}^{n} \Pr(Z = i)$$

Illustrative Example of a 1oo3 System

Consider a 1oo3 system of identical channels, where each failure has an independent DU-failure rate $\lambda_{DU}^{(i)} = 5.0 \cdot 10^{-6}$ per hour. The group is tested every year (i.e. $\tau = 8760$ hours), and the test is assumed perfect. Assume that the group is exposed to random shocks with rate $1 \cdot 10^{-5}$ per hour, and each time a shock occurs the probability of channel failure is 0.20.

The system has a CCF only when all three channels fail. In this case, $\lambda^{(c)}$ becomes:

$$\lambda^{(c)} = \Pr(Z = 3)\nu$$

where $p_s = \Pr(Z = 3) = p^3 = 0.0080$. The PFD_{avg} becomes:

$$PFD_{avg} = \frac{(\lambda_{DU}^{(i)}\tau)^3}{4} + \frac{\lambda_c \tau}{2}$$

Inserted with values, we get:

$$PFD_{avg} = 2.1 \cdot 10^{-5} + 3.5 \cdot 10^{-4} = 3.71 \cdot 10^{-4}$$

Illustrative Example of a 2oo3 System

Consider a 2oo3 system of identical channels. We assume the same data in the previous example for the 1oo3 system.

The system has a CCF when *two and three* channels fail. In this case, $\lambda^{(c)}$ becomes:

$$\lambda^{(c)} = (\Pr(Z = 2) + \Pr(Z = 3))\nu$$

where $p_s = \Pr(Z = 2) + \Pr(Z = 3) = 0.1040$. The PFD$_{avg}$ becomes:

$$PFD_{avg} = (\lambda_{DU}^{(i)}\tau)^2 + \frac{\lambda^{(c)}\tau}{2}$$

Inserted with values, we get:

$$PFD_{avg} = 1.92 \cdot 10^{-3} + 4.55 \cdot 10^{-3} = 6.47 \cdot 10^{-3}$$

Challenges in Using BFR Model

- The difficulty of BFR model is the parameter v
- To determine the value of nu it is necessary to record all outcomes of shocks, also those without any failure (i.e. $Z = 0$)
- If a reasonable estimate of nu can be provided, it is rather straight forward to use the model

Why Study Multiplicity of Faults

Practical experience indicate many situations where only some, and not all, channels fail due to a shared cause within the time frame of interest. The time frame may e.g. be a proof test interval.

The situation is then:

- It can be overly conservative to use standard beta-factor model (which assumes always that all channels fail if a CCF occurs)
- We may use BFR model to determine Z, the number of failed channels, but we may have the problem of determining reasonable value of ν (the shock rate)
- An alternative is to use a more general distribution of Z for multiplicity of failures

Symmetry Assumption

Modeling multiplicity can be complicated. A way to simplify is to make an assumption about symmetry.

Consider a system of m channels. The symmetry assumption implies that:

- There is a complete symmetry in the m channels, and each channel has the same constant failure rate.
- All combinations where k channels do not fail and $(m - k)$ channels fail have the same probability of occurrence.
- Removing j of the m channels will have no effect on the probabilities of failure of the remaining $(m - j)$ channels.

Application for Three Channels

The implementation of the symmetry is difficult to visualize beyond three channels. We therefore focus on three channels onley 1, 2, and 3, and let E_i be the event where channel i is in a failed state.

A failure event can have 3 different outcomes, or multiplicities:

- A single failure, where only one component fails, can occur in 3 different ways as: $(E_1 \cap E_2^* \cap E_3^*)$, $(E_1^* \cap E_2 \cap E_3^*)$, or $(E_1^* \cap E_2^* \cap E_3)$
- A double failure can also occur in three different ways as: $(E_1 \cap E_2 \cap E_3 *)$, $(E_1 \cap E_2 * \cap E_3)$, or $(E_1^* \cap E_2 \cap E_3)$
- A triple failure occurs when $(E_1 \cap E_2 \cap E_3)$

Multiplicity Parameters

In relation to multiplicities, we will introduce three terms:

- $g_{k,m}$ =: Probability of having a SPECIFIC combination of failed (k) and functioning (m) channels.
- $Q_{k:m}$ =: Probability that a CCF involves the failure of k out of m channels
- $f_{k,m}$ =: Conditional probability that a CCF has multiplicity k when we know that a SPECIFIC channel has failed.

$g_{k,m}$

$g_{k,m}$ focuses on each channel:

☞ $g_{k,m}$ = The probability of a *specific* combination of functioning and failed channels such that exactly k channels are in failed state and $(m-k)$ channels are functioning.

For a system of 3 identical channels, using the assumption of symmetry, we get:

$$
\begin{aligned}
g_{1,3} &= \Pr(E_1 \cap E_2^* \cap E_3^*) = \Pr(E_1^* \cap E_2 \cap E_3^*) \\
&= \Pr(E_1^* \cap E_2^* \cap E_3)
\end{aligned}
$$

$$
\begin{aligned}
g_{2,3} &= \Pr(E_1 \cap E_2 \cap E_3*) = \Pr(E_1 \cap E_2 * \cap E_3) \\
&= \Pr(E_1^* \cap E_2 \cap E_3)
\end{aligned}
$$

$$
g_{3,3} = \Pr(E_1 \cap E_2 \cap E_3)
$$

$Q_{k,m}$

$Q_{k,m}$ focuses on the system:

☞ $Q_{k:m}$ = The probability that a (CCF) event in a system of m channels has multiplicity k, for $1 \leq k \leq m$.

For a system of $m = 3$ channels, we have

$$
\begin{aligned}
Q_{1:3} &= \binom{3}{1} \cdot g_{1,3} = 3 \cdot g_{1,3} \\
Q_{2:3} &= \binom{3}{2} \cdot g_{2,3} = 3 \cdot g_{2,3} \\
Q_{3:3} &= \binom{3}{3} \cdot g_{3,3} = g_{3,3}
\end{aligned}
$$

Illustrative Example: A 2oo3 system

A 2oo3 system fails when two or three channels fail. The probability of system failure becomes:

$$\begin{aligned}\Pr(\text{System failure}) &= Q_{2:3} + Q_{3:3} \\ &= 3 \cdot g_{2,3} + g_{3,3}\end{aligned}$$

$f_{k,m}$

$f_{k,\,m}$ is focusing on the fraction of failures for each multiplicity of failure:

☞ $f_{k,\,m}$ = The *conditional* probability that a CCF event in a system of m channels has multiplicity k, when we know that a specific channel has failed.

We now focus on channel 1 (as the results are the same for the other channels, due to symmetry assumption).

The fraction of failures for multiplicity 3 becomes:

$$f_{3,3} = \Pr(E_1 \cap E_2 \cap E_3 \mid E_1) = \frac{\Pr(E_1 \cap E_2 \cap E_3)}{\Pr(E_1)} = \frac{g_{3,3}}{Q}$$

The fraction of failures for multiplicity 2 becomes:

$$\begin{aligned} f_{2,3}^{(1,2)} &= \Pr(E_1 \cap E_2 \cap E_3^* \mid E_1) = \frac{g_{2,3}}{Q}, f_{2,3}^{(1,3)} = \Pr(E_1 \cap E_2^* \cap E_3 \mid E_1) = \frac{g_{2,3}}{Q} \\ f_{2,3} &= f_{2,3}^{(1,2)} + f_{2,3}^{(1,3)} = \frac{2g_{2,3}}{Q} \end{aligned}$$

The fraction of failures for multiplicity 1 becomes:

$$f_{1,3} = \Pr(E_1 \cap E_2^* \cap E_3^* \mid E_1) = \frac{g_{1,3}}{Q}$$

Attributes of MBF Model

The multiple beta-factor (MBF) model is a practical way to implement some of the results from the discussion about multiplicity. It was developed as part of the PDS-method (`www.sintef.no/pds` by Per Hokstad.

Some key attributes of the model are:

- Parameters are introduced to solve $f_{k,m}$ for multiplicity $2, 3, \ldots n$
- Values associated with these parameters are based on expert judgments
- A modification factor is based on MBF for $k$oo$n$ systems, called C_{MooN} (M represents k and N represents n)

MBF model parameter

A set of new β_k parameters are introduced:

$$\beta_k = \Pr(\text{(k+1) comp. fails}|\text{ Comp. 1..k have already failed})$$

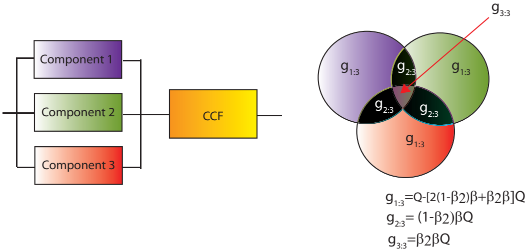
β_1 is called β, but the meaning is not the same as in the standard beta factor model. While β in the standard beta-factor model applies to any multiplicity of failures, we see that β in MBF model applies only for multiplicity 2.

For a system of three channels, we get two CCF parameters:

- β, that applies for the situation where exactly two channels have failed
- β_2, that applies for the situation where exactly three channels have failed

Illustrative Example for Three Channels

The parameters β_k can be used to set up $g_{k,m}$ (and similarly, $f_{k,m}$, as shown below



How to Determine $g_{k,m}$

The probability of a triple failure is calculated as follows:

$$\begin{aligned} g_{3,3} &= \Pr(E_1 \cap E_2 \cap E_3) \\ &= \Pr(E_3 \mid E_1 \cap E_2) \cdot \Pr(E_2 \mid E_1) \cdot \Pr(E_1) \\ &= \beta_2 \beta \cdot Q \end{aligned}$$

The probability of a *specific* double fault (e.g., fault of channels 1 and 2) becomes:

$$\begin{aligned} g_{2,3} &= \Pr(E_1 \cap E_2 \cap E_3^*) \\ &= \Pr(E_3^* \mid E_1 \cap E_2) \cdot \Pr(E_2 \mid E_1) \cdot \Pr(E_1) \\ &= (1 - \beta_2)\beta Q \end{aligned}$$

Because the channels are of the same type, we get the same result for all three combinations of double faults.
The probability of a *specific* single fault (e.g., fault of channels 1) becomes:

$$\begin{aligned} g_{1,3} &= \Pr(E_1 \cap E_2^* \cap E_3^*) \\ &= Q - 2g_{2,3} - g_{3,3} = Q[1 - (2 - \beta_2)\beta] \end{aligned}$$

Application for CCFs Modeling

Consider a 2oo3 system. The system fails upon two and three failures. The CCF part becomes:

- $Q_{\text{CCF}}^{(2oo3)} = 3g_{2,3} + g_{3,3} = (3 - 2\beta_2)\beta Q$

Consider now instead a 1oo3 system. This system fails only upon three failures. The CCF part becomes:

- $Q_{\text{CCF}}^{(1oo3)} = g_{3,3} = \beta_2 \beta Q.$

Note that Q has the same meaning in the two cases, $\frac{\lambda_{DU}\tau}{2}$ when using the simplified formulas.

From MBF model to C_{MooN}

The PDS method has proposed correction factors, called C_{MooN}, with basis in the MBF model:

- C_{MooN} is used to replace the term "in-front of" β
- For a 2oo3 system this means that $Q_{\text{CCF}} = (3 - 2\beta_2)\beta Q$ becomes $C_{2oo3}\beta Q$.
- For a 1oo3 system, this means that $Q_{\text{CCF}} = \beta_2 \beta Q$ becomes $C_{1oo3}\beta Q$
- The value of C_{MooN} is found by assigning a value to β_k. In the 2013 version of the PDS-method, β_2 is, for example $= 0.5$.
- Inserting these values give $C_{1oo3} = 0.5$ and $C_{2oo3} = 2.0$
- Note that "Q" here may be PFD. In the case of a CCF this means $\frac{\lambda_{DU}\tau}{2}$

C_{MooN} table

M/N	N=2	N=3	N=4	N=5	N=6
M=1	$C_{1oo2} = 1.0$	$C_{1oo3} = 0.5$	$C_{1oo4} = 0.3$	$C_{1oo5} = 0.2$	$C_{1oo6} = 0.15$
M=2	–	$C_{2oo3} = 2.0$	$C_{2oo4} = 1.1$	$C_{2oo5} = 0.8$	$C_{2oo6} = 0.6$
M=3	–	–	$C_{3oo4} = 2.8$	$C_{3oo5} = 1.6$	$C_{3oo6} = 1.2$
M=4	–	–	–	$C_{4oo5} = 3.6$	$C_{4oo6} = 1.9$
M=5	–	–	–	–	$C_{5oo6} = 4.5$

Remark: More detailed formulas and underlying assumptions are described in PDS method book that can be ordered from `www.sintef.no/pds`

Illustrative Example for a 1oo2 Voted System

We consider a group of two identical channels voted 1oo2 with DU failure rate λ_{DU}. The system operated in the low-demand mode and is subject to regular perfect proof tests with interval τ.

The corresponding reliability block diagram is: The corresponding formula for the average probability of failure on demand (PFD) becomes:

$$\mathrm{PFD}_{\mathrm{avg}} \approx \underbrace{\frac{[\lambda_{\mathrm{DU}}\tau]^2}{3}}_{\text{Indvidual}} + \underbrace{C_{1oo3}\frac{\beta\lambda_{\mathrm{DU}}\tau}{2}}_{\text{CCF}}$$

Remark: The total failure rate is used instead of independent failure rate, as this error is usually very small.

Illustrative Example for a 2oo3 Voted System

We consider a group of two identical channels voted 2oo3 with DU failure rate λ_{DU}. The system operated in the low-demand mode and is subject to regular perfect proof tests with interval τ.

The corresponding formula for the average probability of failure on demand (PFD) becomes:

$$\mathrm{PFD}_{\mathrm{avg}} \approx \underbrace{(\lambda_{\mathrm{DU}}\tau)^2}_{\text{Individual}} + \underbrace{C_{2oo3}\frac{\beta\lambda_{\mathrm{DU}}\tau}{2}}_{\text{CCF}}$$

Remark: The total failure rate is used instead of independent failure rate, as this error is usually very small.

An Observation from the Two Examples

The two previous examples show that the CCF part is the same regardless of how a system with redundant channels is voted.

This is shown here:

$$
\begin{aligned}
\mathrm{PFD}_{\mathrm{avg,\,a}} &\approx \frac{[\lambda_{\mathrm{DU}}\tau]^2}{3} + C_{1oo3}\frac{\beta\lambda_{\mathrm{DU}}\tau}{2} \\
\mathrm{PFD}_{\mathrm{avg,\,b}} &\approx [\lambda_{\mathrm{DU}}\tau]^2 + C_{2oo3}\frac{\beta\lambda_{\mathrm{DU}}\tau}{2}
\end{aligned}
$$

This comparison shows that the PDS approach, based on MBF model, gives different CCF contribution depending on how the channels are voted.

C_{MooN} in Markov Model

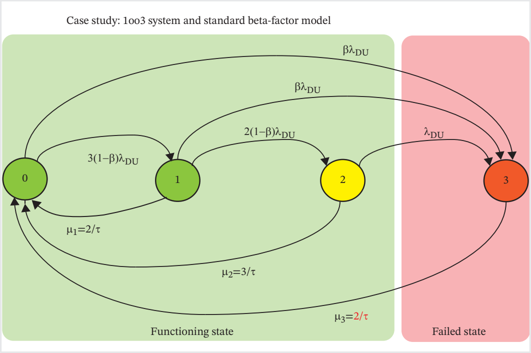
Introducing C_{MooN} means that new transitions are introduced into the Markov model

The following slides give some illustrative examples. When reading the Markov models, have in mind that:

- C_{MooN} means the correction factor consider $(M - N - 1)$ to N faults
- This means that:
  - C_{1oo3} means correction for exactly 3 faults among three channels
  - C_{2oo3} means correction of 2 and 3 faults among three channels
  - C_{2oo3} - C_{1oo3} means correction of exactly two faults among three channels
  - C_{1oo4} means correction for exactly 4 faults among four channels
  - C_{2oo4} means correction of 3 and 4 faults among four channels
  - C_{3oo4} means correction of 2, 3 and 4 faults among four channels
  - C_{3oo4} - C_{2oo4} means correction of exactly two faults among four channels
  - C_{2oo4} - C_{1oo4} means correction of exactly three faults among four channels

Illustrative Example: 1oo3 system

First, we recall that the Markov model for a 1oo3 system with standard beta-factor model is as shown below, assuming only DU-failures and that the system is subject to regular testing.

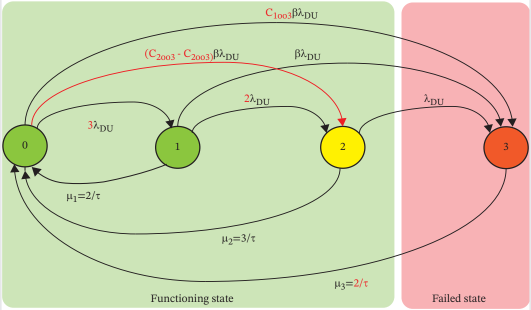


Note that state two becomes a "critical state" (marked yellow) while state three represents the failed state (marked red).

Illustrative Example: 1oo3 system

Now, we adjust the Markov model for the 1oo3 system with C_{MooN}-factors, see illustration below. One new transition is introduced and some other transition rates have been modified.

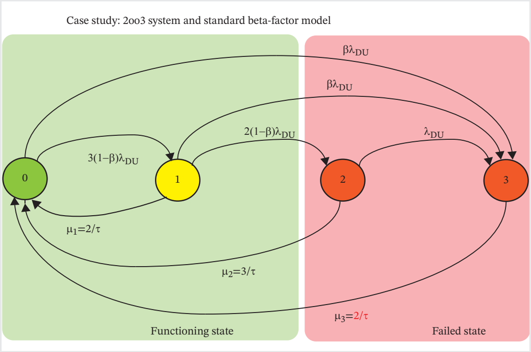
Case study: 1oo3 system and standard beta-factor model



Note that state two becomes a “critical state” (marked yellow) while state three represents the failed state (marked red).

Illustrative Example: 2oo3 system

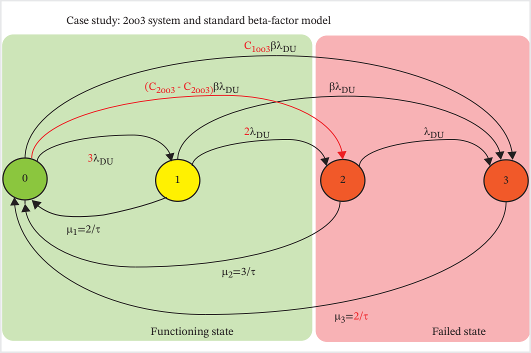
First, we recall that the Markov model for a 2oo3 system with standard beta-factor model is as shown below, assuming only DU-failures and that the system is subject to regular testing.



Note that state one becomes a "critical state" (marked yellow) while state two and three represent the failed state (marked red).

Illustrative Example: 1oo3 system

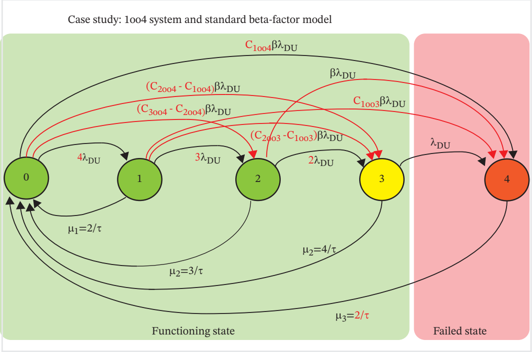
Now, we adjust the Markov model for the 2oo3 system with C_{MooN}-factors, see illustration below. Transitions are the same as for the 1oo3 system, but what are critical and failed states have been changed.



Note that state one becomes a “critical state” (marked yellow) while state two and three represent the failed state (marked red).

Illustrative Example: 1oo4 system

Now, we consider a Markov model for a 1oo4 system with C_{MooN}-factors, see illustration below. We see that several new transitions are added, compared to a model where standard beta-factor model is used. Some transitions are also modified.



Illustrative Example: 1oo4 system

Now, we consider a Markov model for a 2oo4 system with C_{MooN}-factors, see illustration below. Transitions are the same as for the 1oo4 system, but what are critical and failed states have been changed.