System Reliability Thory
6. Common-Cause Failures

Marvin Rausand
marvin.rausand@ntnu.no

RAMS Group
Department of Production and Quality Engineering
NTNU

(Version 0.1)

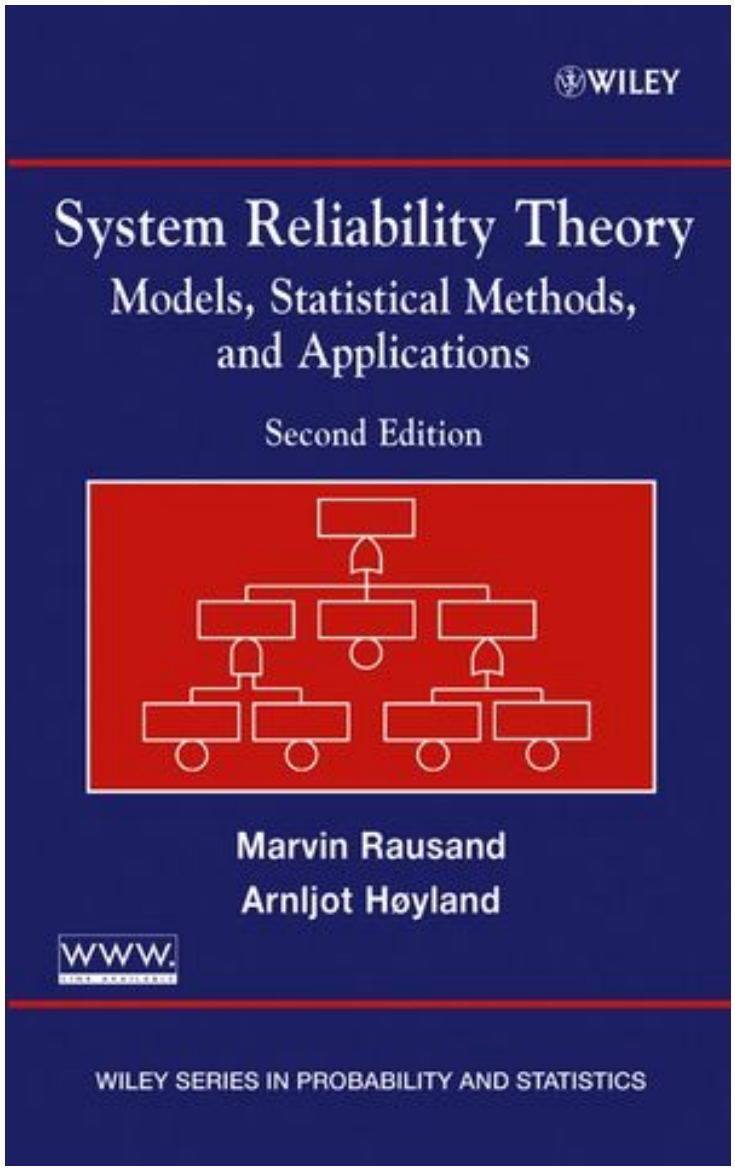
NTNU – Trondheim
Norwegian University of
Science and Technology

Slides related to the book

System Reliability Theory
Models, Statistical Methods, and Applications

Wiley, 2004

Homepage of the book:
http://www.ntnu.edu/ross/books/srt



Learning objectives

In this lecture, you will learn:

1. What is a CCF?
2. Why are they important?
3. How can we include CCFs in reliability analyses?
4. What are the main challenges?

What is a common-cause failure?

A common-cause failure (CCF) is a failure where:

- Two or more items fail within a specified time such that the success of the system mission would be uncertain.
- Item failures result from a single shared cause and coupling factor (or mechanism)

Importance of CCFs

CCFs are of concern because

- They may violate the effect of using redundancy to enhance the system reliability
- They may violate the effect of having several layers of protection

Independent failures - 1

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 events, E_1 and E_2 are said to be statistically independent if

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

$$\text{such that} \quad \Pr(E_1 \cap E_2) = \Pr(E_1) \cdot \Pr(E_2)$$

Note that when $E_1 \cap E_2 = \emptyset$, then $\Pr(E_1 \cap E_2) = 0$ and $\Pr(E_1 \mid E_2) = 0$. A set of events cannot be both mutually exclusive and independent.

Independent failures - 2

When the items of a system are independent, this implies that:

- The failure of an item has no functional influence on the other items of the system
- The failure of an item has a negligible physical effect on the other system items
- By adding redundant items to the system, the failure probability can be reduced as much as we like

Dependent failures

- Two items, 1 and 2, are dependent when

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

- 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.

Dependent failures

- In reliability and risk analyses, positive dependence is usually the most relevant.
- Negative dependency may also be relevant in some cases.

Example

Consider two items that influence each other by producing vibration or heat. When one item fails and is "down" for repair, the other item will have an improved operating environment, and its probability of failure is reduced.

Intrinsic dependency

From NUREG/CR-6268

☞ Intrinsic dependency: A situation where the functional status of a component is affected by the functional status of other components.

Sub-classes:

- Functional requirement dependency
- Functional input dependency
- Cascading failure

Extrinsic dependency

From NUREG/CR-6268

☞ Extrinsic dependency: A situation where the dependency or coupling is not inherent or intended in the functional characteristics of the system.

Extrinsic dependencies may be related to:

- Physical or environment stresses.
- Human intervention

Cascading failures

☞ Cascading failures: A sequence of item failures where the first failure shifts its load to one or more nearby items such that these fail and again shift their load to other item, and so on.

Cascading failures are sometimes referred to as a *Domino effect*.

Main CCF attributes

- A shared cause exists
- The shared cause has two elements, a root cause and a coupling factor:
  - Root cause: Why did the item fail? (i.e., linked to the item)
  - Coupling factor: Why were several items affected? (i.e., linked to the relationships between several items)

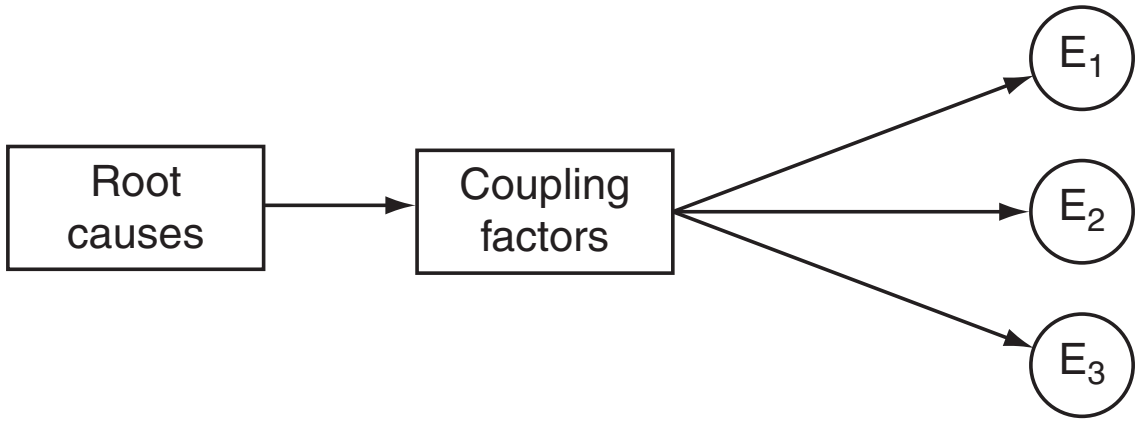
Root cause and coupling factor

☞ Root cause: Most basic cause of item failure that, if corrected, would prevent recurrence of this and similar failures.

☞ Coupling factor: Property that makes multiple items susceptible to the same root cause.

A coupling factor is also called a coupling mechanism.

Root cause and coupling factor



where E_i denotes that item i is in a failed state.

Typical root causes

We may distinguish between *pre-operational* and *operational* causes:

- Pre-operational root causes
  - Design, manufacturing, construction, installation, and commissioning errors.
- Operational root causes
  - Operation and maintenance-related: Inadequate maintenance and operational procedures, execution, competence and scheduling
  - Environmental stresses: Internal and external exposure outside the design envelope or energetic events such as earthquake, fire, flooding.

Typical coupling factors

To look for coupling factors is the same as to look for similarities ...

- 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

Common-cause component group

☞ Common-cause component group (CCCG): A group of (usually similar [in mission, manufacturer, maintenance, environment, etc.]) components that are considered to have a high potential for failure due to the same cause or causes.

- Identical components providing redundancy in the system should always be assigned to the same CCCG.
- Different redundant components that have parts that are identical, should always be assigned to a CCCG in spite of their diversity.
- Susceptibility of a group of components to CCFs not only depends on their degree of similarity, but also on the existence/lack of defensive measures (barriers) against CCFs.

Common-cause event

☞ Common-cause event (CCE): An event that represents the unavailability of a specific set of components because of shared causes that are not explicitly represented in the system logic model as other basic events.

Attributes of a CCF definition

Smith and Watson (1980) suggest that a definition of CCF should encompass:

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

Some different definitions - 1

- 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.
- Process industry (IEC 61511, 2003):
  - Failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to system failure.

Some different definitions - 2

- Lundteigen and Rausand (2007) - related to safety-instrumented systems:

1. The CCF event comprises complete failures of two or more redundant components or two or more safety instrumented functions (SIFs) due to a shared cause

2. The multiple failures occur within the same inspection or function test interval

3. The CCF event may lead to failure of a single SIF or loss of several SIFs

CCF event

☞ CCF event: An event involving failure of a specific set of components due to a common cause.

- A CCF event involves two or more item failures.
- The item failures of a CCF event can occur simultaneously or within a specified (short) time interval.
- Whether or not the item failures occur at the same time depends on the shared cause.
- The CCF event is sometimes called a common-cause basic event (CCBE).

CCF event

Example – Gas detection

Consider a system of m gas detectors that are installed in a production room. A shared cause of a potential CCF event is increased humidity in the room. This shared cause will lead to an increased probability of detector failure, but the failures will normally not occur at the same time. The time between detector failures may be rather long.

Modeling approach

1. Develop a system logic model (e.g., a fault tree or a reliability block diagram)
2. Identify relevant common-cause component groups (CCCG)
3. Identify relevant root causes and coupling factors/mechanisms
4. Assess the efficiency of CCF defenses
5. Establish explicit models
6. Include implicit models
7. Quantify the reliability and interpret the results

Explicit modeling

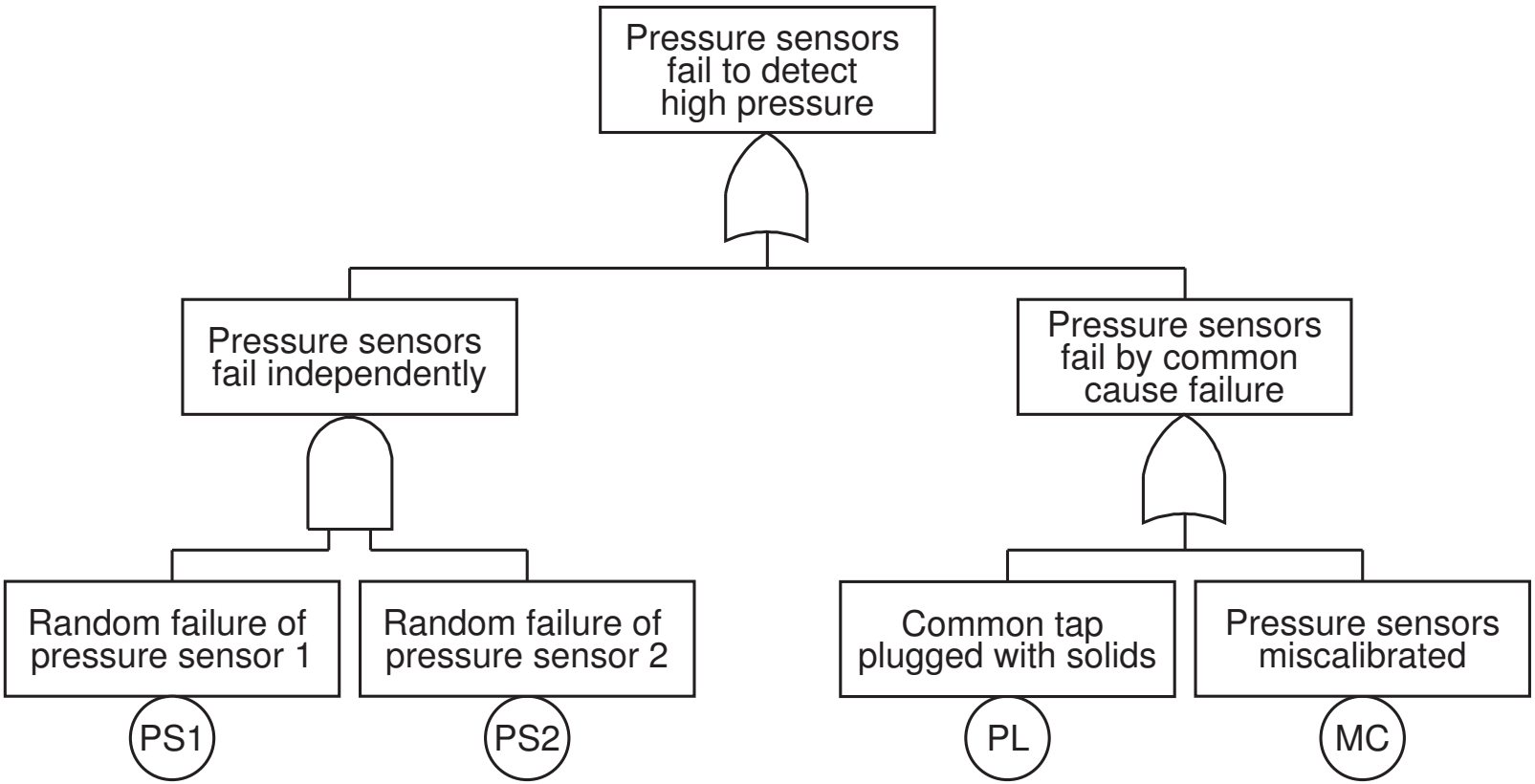
- The shared cause is identified as a separate basic event/element in the reliability model.

Explicit causes may be:

- 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

Example: Two pressure sensors



– Adapted from Summers and Raney (1999)

Implicit modeling

- Where a set of items share a number of root causes and coupling factors, and where the explicit modeling would be unmanageable, the (residual) shared causes are modeled as a "combined" basic event/element.
- Implicit modeling implies using a CCF modeling approach.

Multiplicity of failures – 1

☞ Multiplicity: The number of items in a group that actually fails in the CCF event.

We may distinguish between:

- Complete (lethal) failure: All items in the group fail – this is usually associated with extreme environmental, human interactions, highly dependent requirements, or input interactions.

- Partial (non-lethal) failure: More than one, but not all items fail.

Multiplicity of failures – 2

Remarks:

- When the shared cause (e.g., a shock) occurs, the multiplicity of the CCF event will often be a random variable. Some risk analysts say that we have a CCF event also when the multiplicity is 1 (i.e., when the shared cause only leads to a single item failure). Other analysts may say that we have a CCF event even when the multiplicity is 0 (i.e., when the shared cause does not lead to any item failures).

- The above interpretation of CCF event is controversial – but may be beneficial in some CCF models.

Symmetry assumption

Consider a system of m identical items. In many CCF models, the following symmetry assumptions are made:

- There is a complete symmetry in the m items.
- All combinations where k items do not fail and $(m - k)$ items 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 $(m - j)$ items.

Multiplicity – 1

Example – three items

Consider a system of three components 1, 2, and 3, and let E_i be the event that item i is in a failed state and E_i^* that it is not.

A failure event can have 3 different multiplicities:

- A single failure, where only one item 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 – 2

Probability of a specific combination

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

For a system of 3 identical items:

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

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

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

Multiplicity – 3

Probability of a specific multiplicity

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

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

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

Multiplicity – 4

Example – 2-out-of-3 system

A 2-out-of-3 (2oo3) system functions as long as at least 2 of its 3 items function, and fails when 2 or more items fail. The probability of system failure is then

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

Multiplicity - 5

Probability when one failure has been observed

☞ $f_{k,m}$ = 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.

Example

Consider a safety-instrumented system that is tested periodically. If we, during the test, reveals that the first channel tested has failed, $f_{k,m}$ is the probability that this failure is, in fact, part of a CCF event with multiplicity$k$.

Multiplicity - 6

Example: 2-out-of-3 system (1)

Consider a 2oo3 system of 3 identical items, and assume that we have observed that item 1 is failed. The conditional probability that this, in fact, is a triple failure is:

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

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

where Q denotes the probability that item 1 fails, i.e., $\Pr(E_1)$.

Multiplicity - 7

Example: 2-out-of-3 system (2)

The conditional probability that the failure is a double failure is – following the same arguments:

$$f_{2,3} = \frac{g_{2,3}}{Q} + \frac{g_{2,3}}{Q} = \frac{2\,g_{2,3}}{Q}$$

where of the $g_{2,3}$'s correspond to the failure of items 1 and 2, and the other to failures of items 1 and 3.
The conditional probability that the failure is a single failure is

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

and we note that $f_{1,3} + f_{2,3} + f_{3,3} = 1$

Beta-factor model - 1

The beta-factor model for CCFs was proposed by Karl N. Fleming in 1975. It is a very simple model with the following properties:

- The item failure rate λ is split into an independent part λ_I and a dependent part λ_c, such that $\lambda = \lambda_I + \lambda_c$.
- The beta-factor (β) is the fraction of all item failures that are common-cause failures (CFF), i.e., $\beta = \lambda_c/\lambda$
- The failure rates are therefore

Karl N. Fleming

$$\lambda_c = \beta\lambda$$
$$\lambda_I = (1-\beta)\lambda$$

The beta-factor can also be interpreted as the conditional probability that the failure is a CCF, given that the item has failed.

Beta-factor model - 2

Limitations

Consider a system of m identical items.

- Each item failure can have two distinct causes: (i) an independent cause (i.e., a cause that only affects the specific item), and (ii) a shared cause that will affect all the m items – and cause all m to fail at the same time.
- This means that the multiplicity of each CCF event must be either 1 or m. It is not possible to have CCF events with intermediate multiplicities.

Beta-factor model - 3

Multiplicity of failures

Consider a system of m identical channels and assume that we have observed that a channel has failed. The conditional probability that this is, in fact, a CCF of multiplicity k is

$$\begin{aligned} f_{1,m} &= 1-\beta \\ f_{k,m} &= 0 \\ f_{m,m} &= \beta \end{aligned}$$

for $k = 2, 3, \ldots, m-1$

Beta-factor model - 4

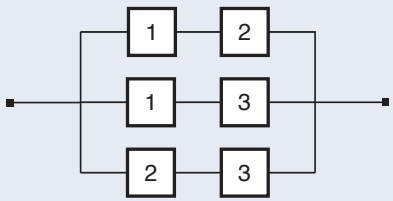
Example: 2oo3 structure

Consider a 2oo3 structure of 3 identical items with failure rate λ. The dependency between the items can be modeled by a beta-factor model with parameter β.

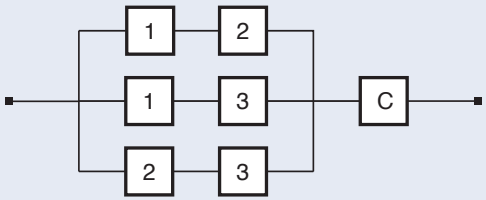
Because the common-cause event (with rate $\lambda_c = \beta\lambda$) will affect all the three items, it can be modeled as a virtual item in series with the real items.

The survivor function of the 2oo3 structure is

$$\begin{aligned} R(t) &= \left(3e^{-2(1-\beta)\lambda t} - 2e^{-3(1-\beta)\lambda t}\right) e^{-\beta\lambda t} \\ &= 3e^{-(2-\beta)\lambda t} - 2e^{-(3-2\beta)\lambda t} \end{aligned}$$



2oo3 structure



2oo3 structure with CCF virtual item

Beta-factor model - 5

- The beta-factor model is simple and easy to understand and use – since it has only one extra parameter (β), and it is easy to understand the meaning of this parameter.
- The beta-factor model is the most commonly used CCF model.
- The beta-factor model is a preferred CCF model in IEC 61508.

Beta-factor model - 6

A criticism

An effort to reduce an item's susceptibility to CCFs will reduce the parameter β, but will at the same time increase the rate of independent failures λ_I since λ_I is defined as

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

When using the beta-factor model, the total failure rate λ is kept constant. It is obviously possible to compensate for this strange behavior, but this is often forgotten in practice.

Determination of the beta-factor

The beta-factor may be determined by

- Expert judgment
- Checklists
- Estimation based on observed data

Humphrey's method - 1

An approach to determining a plant-specific β was proposed by Humphreys (1987).

- Eight factors are important for the value of β (grouped as *design*, *operation*, and *environment*)
- Each factor is classified as $a, b, \ldots, e$ and given scores according to a specific table (see next slide), where a is the best state and e is the worst state.
- The application-specific β is determined by adding the scores and dividing by 50 000.

Humphrey's method - 2

Humphrey's method is based on the following table of scores:

Factor	Subfactor	Scores				
		a	b	c	d	e
Design	Separation	2 400	580	140	35	8
	Similarity	1 750	425	100	25	6
	Complexity	1 750	425	100	25	6
	Analysis	1 750	425	100	25	6
Operation	Procedures	3 000	720	175	40	10
	Training	1 500	360	90	20	5
Environment	Control	1 750	425	100	25	6
	Tests	1 200	290	70	15	4

IEC 61508 method

IEC 61508, Part 6, Annex D presents a checklist of about 40 questions that can be used to determine a plant-specific value of the beta-factor for safety-instrumented systems:

- Each question is answered by "yes" or "no"
- X and Y scores are given for each question
- For all questions with answer "yes"; the corresponding X values and Y values are summed up.
- A table is used to determine the beta-factor based on $\sum(X_i + Y_i)$
- Provides a beta-factor between 0.5% and 5% (for logic solvers) and between 1% and 10% for sensors and final elements.

IEC 61508 method

The 40 questions cover the following issues:

1. Degree of physical separation/segregation
2. Diversity/redundancy (e.g., different technology, design, different maintenance personnel)
3. Complexity/maturity of design/experience
4. Use of assessments/analyses and feedback data
5. Procedures/human interface (e.g., maintenance/testing)
6. Competence/training/safety culture
7. Environmental control (e.g., temperature, humidity, personnel access)
8. Environmental testing

IEC 62061 method

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

Unified partial method

- The unified partial method (UPM) was proposed by Brand (1996) and further developed by Zitrou and Bedford in 2003
- UPM is the standard approach in the UK nuclear industry
- UPM assumes that the beta-factor is influenced by eight underlying factors $(s_1, s_2, \ldots, s_8)$
- Each underlying factor s_i is associated with a weight and a score
- A mathematical relationship is established between some underlying factors and the beta-factor

Unified partial method

The eight underlying factors are:

1. Environmental control
2. Environmental tests
3. Analysis
4. Safety culture
5. Separation
6. Redundancy and diversity
7. Understanding
8. Operator interaction

The factors are not independent of each other.

Unified partial method

A lineral relationship is assumed between the beta-factor and the "status" for each factor:

$$\beta \approx \sum_{i=1}^{8} w_i \cdot x_i$$

In practice:

- It is difficult to obtain statistically significant results for the correlation because CCF events are rare
- It is not obvious that a linear relationship exists

To overcome this problem, Zitrou and Bedford have proposed to use multi-attribute value theory.

C-factor model

- The C-factor model is mainly the same model as the beta-factor model, but the rate of dependent failures, λ_c is defined as a fraction (C) of the independent failure rate , λ_I instead of as a fraction of the total failure rate (as is done in the beta-factor model), such that

$$\lambda = \lambda_I + C \cdot \lambda_I$$

- This means that an effort to reduce the item's susceptibility to CCFs will reduce the total failure rate λ, and not as in the beta-factor model to increase the independent failure rate.

Binomial failure rate model - 1

The binomial failure rate (BFR) model was proposed by William E. Vesely in 1977. The main principles of the BFR model are:

- The items in the CCCG are exposed to two types of impacts, called lethal and non-lethal shocks. It is assumed that the shocks will hit all items in the CCCG.
- The lethal shocks occurs with constant rate $\lambda^{(i)}$ and the non-lethal shocks occur with constant rate ν.
- When a lethal shock occurs, all the items of the CCCG fail at the same time.
- When a non-lethal shock occurs, the items in the CCCG will fail independently, each with (conditional) probability p.

Binomial failure rate model - 2

- In the BFR model, each item in the CCCG has total (dependent) failure rate $\lambda_c = \lambda^{(i)} + pv$
- Let Z denote the number of items, among the n items in the CCCG, that fail in a non-lethal shock. The probability distribution of Z is

$$\Pr(Z = z) = \binom{n}{z} p^z (1-p)^{n-z} \quad \text{for } z = 0, 1, 2, \ldots, n$$

- The rate of dependent total failures of the CCCG (i.e., that n-out-of-n items fail) is hence $\lambda^{(i)} + vp^n$
- The rate of dependent failures of the CCCG of multiplicity k is

$$\lambda_{G,c} = v \Pr(Z = k) = v \binom{n}{k} p^k (1-p)^{n-k}$$

Binomial failure rate model - 3

- It is problematic to estimate the rate ν of non-lethal shocks from observed data. This is because a non-lethal shock may not give any item failures (i.e., $Z = 0$) and thus may be unnoticed.
- We may also assume that each item may fail due to individual deterioration with rate λ_{I} such that the total failure rate of an item is $\lambda = \lambda_{\mathrm{I}} + \lambda_{\mathrm{c}}$

Binomial failure rate model - 4

Example: 2oo4 structure (CCCG)

Consider a voted group (CCCG) that is functioning if at least 2 of its four identical items are functioning. Lethal shocks are assumed to occur with rate $\lambda^{(i)} = 5 \cdot 10^{-7}$ per hour. Non-lethal shocks are assumed to occur with rate $\nu = 8 \cdot 10^{-6}$ per hour. When a non-lethal shock occurs, each item will fail (independently) with probability $p = 0.40$.
The failure rate of each component is then $\lambda_c = \lambda^{(i)} + \nu p = 3.7 \cdot 10^{-6}$ per hour.
The rate $\lambda_{G,c}$ of dependent group failures is:

$$\begin{aligned}\lambda_{G,c} &= \lambda^{(i)} + \nu \Pr(Z > 2) \\ &= \lambda^{(i)} + \nu \left[\binom{4}{3} p^3 (1-p) + p^4 \right] \approx 1.93 \cdot 10^{-6} \quad \text{per hour}\end{aligned}$$

Basic parameter model

Introductory example

Consider a system of 3 items, and let E_i denote the event that item i is in a failed state. Item 1 will fail (from all causes) with probability

$$\Pr(E_1) = \Pr\left[E_1^i \cup (E_1^c \cap E_2^c) \cup (E_1^c \cap E_3^c) \cup (E_1^c \cap E_2^c \cap E_3^c)\right] \tag{1}$$

where E_1^i denotes an independent failure of item 1, and E_i^c denotes a CCF of item i, for $i = 1, 2, 3$.
This means that a failure of item 1 can be a single independent failure or a CCF with multiplicity 2 or 3.

Similar formulas can easily be established for $\Pr(E_2)$ and $\Pr(E_3)$.

Basic parameter model

Basic notation

For a system of 3 identical items, the basic parameter model (BPM) is usually assumed to fulfill:

$$\begin{aligned} Q_{1:3} &= \Pr(E_1^i) = \Pr(E_2^i) = \Pr(E_3^i) \\ Q_{2:3} &= \Pr(E_1^c \cap E_2^c) = \Pr(E_1^c \cap E_3^c) = \Pr(E_2^c \cap E_3^c) \\ Q_{3:3} &= \Pr(E_1^c \cap E_2^c \cap E_3^c) \end{aligned}$$

where $Q_{i:3}$ is the probability of a failure with multiplicity i in a system with three items.

Basic parameter model

Symmetry assumption

- The symmetry assumption implies that the probability of failure of any given basic event involving similar items depends only on the number and not on the specific attributes of the items in that basic event.

Basic parameter model

The total probability of failure (of all types) of a specified item in a system of 3 items is

$$Q_t = Q_{1:3} + 2 \cdot Q_{2:3} + Q_{3:3}$$

For a system of m identical items, this formula can be written

$$Q_t = \sum_{k=1}^{m} \binom{m-1}{k-1} Q_{k:m}$$

where $\binom{m-1}{k-1}$ is the number of different ways a specified item can fail with $(k-1)$ other items in a group of m items.

Basic parameter model

When $Q_{k:m}$ is demand-based, Mosleh et al. (1988) have shown that the maximum likelihood estimate for $Q_{k:m}$ is given by

$$\hat{Q}_{k:m} = \frac{n_k}{N_k}$$

where n_k is the number of failure events involving failure of k items , and N_k is the number of demands on any k items in the CCCG.

- To estimate $Q_{k:m}$, we need to count the number of events n_k with k failures, and the number of demands N_k on all groups of k items.

Basic parameter model

- If all m items are demanded each time the system is operated, and this number of demands is N_D, then

$$N_k = \binom{m}{k} N_D$$

- The term $\binom{m}{k}$ is the number of groups of k items that can be formed from m items. We therefore have:

$$\hat{Q}_{k:m} = \frac{n_k}{\binom{m}{k} \cdot N_D}$$

Alpha-factor model (1)

☞ Alpha-factor ($\alpha_{k:m}$): The fraction of failure events that occur in a group of m items and involve failure of exactly k items due to a common cause.

Remark:

If, for example, $\alpha_{2:m} = 0.05$, this means that 5% of all failure events in a group of m items is a CCF with multiplicity equal to 2.

Alpha-factor model

The alpha-factor can be calculated as:

$$\alpha_{k:m} = \frac{\binom{m}{k} \cdot Q_{k:m}}{\sum_{j=1}^{m} \binom{m}{j} \cdot Q_{j:m}}$$

where $\binom{m}{k} \cdot Q_{k:m}$ is the probability of a failure events involving exactly k items, and the denominator is the sum of such probabilities.

Remark:

$\alpha_{k:m}$ is therefore the conditional probability of a CCF with multiplicity k, given that a failure event has occurred in a group of m items.

Alpha-factor model

Example

For a group of 3 similar items, we have:

$$\alpha_{1:3} = \frac{3 \cdot Q_{1:3}}{3 \cdot Q_{1:3} + 3 \cdot Q_{2:3} + Q_{3:3}}$$

$$\alpha_{2:3} = \frac{3 \cdot Q_{2:3}}{3 \cdot Q_{1:3} + 3 \cdot Q_{2:3} + Q_{3:3}}$$

$$\alpha_{3:3} = \frac{Q_{3:3}}{3 \cdot Q_{1:3} + 3 \cdot Q_{2:3} + Q_{3:3}}$$

and $\alpha_{1:3} + \alpha_{2:3} + \alpha_{3:3} = 1$, as expected.

Alpha-factor model (2)

Let:

- Q_t = the total failure probability of a specific item due to all independent and CCF events.

The probability of a CCF involving k items will depend on how the items are tested. For simultaneous testing, the probability is

$$Q_{k:m} = \frac{k}{\binom{m-1}{k-1}} \cdot \frac{\alpha_{k:m}}{\alpha_t} \cdot Q_t = \frac{m}{\binom{m}{k}} \cdot \frac{\alpha_{k:m}}{\alpha_t} \cdot Q_t$$

where $\alpha_t = \sum_{k=1}^{m} k \cdot \alpha_{k:m}$

Alpha-factor model

- Since the alpha-factor $\alpha_{k:m}$ is the fraction of all failure events that involve exactly k items, the factor can be estimated as

$$\hat{\alpha}_{k:m} = \frac{n_k}{\sum_{j=1}^{m} n_j}$$

To determine the CCF contribution, it is therefore only necessary to estimate Q_t and determine n_k for $k = 1, 2, \ldots, m$.

Defenses against CCFs

Relevant defense strategies include:

- Item diversity
- Item isolation
  - Physical shielding
  - Physical containment
  - Physical separation
- Item design margin
- Human error prevention

CCF data sources

ICDE – The OECD/NEA International Common-cause Failure Data Exchange Project

Objectives:

- Collect and analyze CCF events over a long term to understand such events, their causes, and their prevention
- Generate qualitative insights into the root causes of CCF events that can then be used to derive approaches or mechanisms for their prevention or for mitigating their consequences
- Establish a mechanism for efficient feedback of experience gained in connection with CCF phenomena, including the development of defenses against their occurrence, such as indicators for risk-based inspections
- Generate quantitative insights and record event attributes to facilitate quantification of CCF frequencies in member countries
- Use the ICDE data to estimate CCF parameters