5.1 Introduction to Dependent and Common Cause Failures

5.1.1 Identification of the Problem

Achieving a high reliable system \( S \) can be done in two ways:

1. Selection of a high reliable single item \( I \).
2. Use of redundant items \( I_i \).

Unfortunately, the first solution is often not tractable because such items do not exist or are highly expensive. Therefore, the second solution is generally implemented in industry.

For example, the probability of failure, \( P_r(\bar{S}) \), of a system \( S \) comprising 2 independent redundant items \( I_1 \) and \( I_2 \) can be calculated from the probabilities of failure, \( P_r(\bar{I}_1) \) and \( P_r(\bar{I}_2) \), by the following formula:

\[
P_r(\bar{S}) = P_r(\bar{I}_1 \cap \bar{I}_2) = P_r(\bar{I}_1) \times P_r(\bar{I}_2) \tag{5.1}
\]

If it is required that \( P_r(\bar{S}, T) \leq 10^{-6} \) over a given time interval \([0, T]\), applying formula (5.1) shows that the use of two identical redundant items having a failure probability \( P_r(\bar{I}_1, T) = P_r(\bar{I}_2, T) \leq 10^{-3} \) would allow to reach the target. Formula 5.1 can be extended to any number of redundant items and it seems that reaching a high level of success (i.e. a low probability of failure) is just a matter of adding up a sufficient number of redundant items.

Unfortunately, this is an illusion as the items are not necessarily fully independent and in this case formula 5.1 is no longer valid. For example, when \( \bar{I}_1 \) and \( \bar{I}_2 \) are not independent, the following formula 5.2 has to be used instead:
In this formula, $\text{Pr}(\overline{I}_1 | \overline{I}_2)$ denotes the conditional probability of $\overline{I}_1$ given that $\overline{I}_2$ has occurred. This implies:

$$\text{Pr}(\overline{I}_1 | \overline{I}_2) = \frac{\text{Pr}(\overline{I}_1 \cap \overline{I}_2)}{\text{Pr}(\overline{I}_2)} \quad (5.3)$$

When $\overline{I}_1$ and $\overline{I}_2$ are independent, formula 5.3 leads to $\text{Pr}(\overline{I}_1 | \overline{I}_2) = \text{Pr}(\overline{I}_1)$. This result constitutes a criterion of independency between $\overline{I}_1$ and $\overline{I}_2$.

In another way, $\text{Pr}(\overline{I}_2 | \overline{I}_1)$ can be calculated by the following formula:

$$\text{Pr}(\overline{I}_2 | \overline{I}_1) = \frac{\text{Pr}(\overline{I}_1 \cap \overline{I}_2)}{\text{Pr}(\overline{I}_1)} = \text{Pr}(\overline{I}_1 | \overline{I}_2) \times \frac{\text{Pr}(\overline{I}_2)}{\text{Pr}(\overline{I}_1)} \quad (5.4)$$

Then, when $\overline{I}_1$ and $\overline{I}_2$ are dependent, the dependency exists on both sides: the occurrence of $\overline{I}_1$ depends on the occurrence of $\overline{I}_2$ and vice versa.

Therefore, dependencies described by conditional probabilities such as $\text{Pr}(\overline{I}_1 | \overline{I}_2) \neq \text{Pr}(\overline{I}_1)$ or $\text{Pr}(\overline{I}_2 | \overline{I}_1) \neq \text{Pr}(\overline{I}_2)$ do not imply any link of causality between the events $\overline{I}_1$ and $\overline{I}_2$, but rather implies a positive or a negative mutual influence between them. These dependencies are the symptom of underlying (or root) causes affecting both items. When the impact is detrimental, these underlying causes are called common cause failures.

However, an underlying cause is often considered to be a “true” common cause failure (CCF) only if the failures of two or more individual items impacted by this cause occur within a limited interval of time.

Let us consider that $I_1$ and $I_2$ are two bulbs which fail to light. This can be due to a loss of the electrical power supply, $\overline{E}$, which obviously is a common cause leading to $\overline{I}_1$ and $\overline{I}_2$. Therefore, $\overline{E}$ is a cause of $\overline{I}_1$ and a cause of $\overline{I}_2$ and this is because $\overline{I}_1$ and $\overline{I}_2$ share this common cause that they are not independent.

$\text{Pr}(\overline{I}_1 | \overline{I}_2)$ being greater than $\text{Pr}(\overline{I}_1)$ most of the time (positive dependency), using formula 5.1 instead of formula 5.2 leads to non-conservative results. Of course, the more dependent the events, the most optimistic formula 5.1. This is the core of the dependent/common cause failures difficulties: as soon as the items are linked by any
dependency, the system failure probability cannot be assessed just by multiplying
the item failure probabilities: conditional probabilities have to be considered instead.

As already described in Chap. 4 (see Fig. 4.6), the item failures being never
completely independent, decreasing the probability of failure of a system just by
increasing the redundancy is limited by existing dependencies due to common cause
failures (CCFs). That means that the impact of CCFs increases when the probability
of the system failure decreases. At the limit, a CCF negligible for an individual item
can become the topmost contributor when redundancy is high. Then, the dependent
failures and their underlying common causes often constitute the weak points of
redundant systems.

Therefore, it is important to take CCFs into account but, except in explicit
tangible cases (e.g. the loss of electrical power supply analysed above), assessing
conditional probabilities is usually difficult. This is why approximated models have
been developed to take them into account to some extent and to provide safeguards
against non-conservative results.

### 5.1.2 Definition

As pointed out by Modarres Modarres et al. (2017), “there is no unique and universal
definition for CCFs”. However, a fairly general definition of CCF is given by Mosley
Mosley et al. (1988) as “a subset of dependent events in which two or more component
fault states exist at the same time or in a short time interval, and are direct results
of a shared cause”.

In the absence of generally accepted definition of CCF, as already mentioned,
many information media such as standards, guidelines and textbooks have proposed
their own more or less equivalent definition often depending on their application
domain and context (Rausand 2014). Among them are the theses cited in Chap. 4 in
accordance with the IEV 192 standard IEC 60050-192 (2015) as follows:

**Common cause failures (CCFs): failures of multiple items, which would otherwise
be considered independent of one another, resulting from a single cause** (IEV 192-03-18).

Some other publications define the CCFs by the mechanism leading to them. For
example, in Mosley et al. (1988):

**Common cause failures (CCFs): result of the coexistence of two main factors:**

- A susceptibility for items to fail because of a particular root cause.
- A coupling mechanism (or factor).

The root cause is the most basic cause of the failure that, if corrected, would prevent its
occurrence (e.g. abnormal environmental stress, design inadequacy, human actions,
procedure inadequacy).
The coupling factor characterizes components susceptible to the same causal mechanism which creates the condition for multiple items to fail (e.g. shared hardware design, shared maintenance/test schedule).

In addition, it is expected that the failures of two or more individual items due to CCFs occur within a limited interval of time.

It has to be noted that common cause failures can lead to common mode failures which are defined as follows in the IEV 192:

**Common mode failures (CMFs): failures of different items characterized by the same failure mode** (IEV 192-03-19).

Moreover, the distinction between common cause and common mode failure may be difficult and some sources do not hesitate to consider CMFs as a sub-category of CCFs.

### 5.1.3 Dependency Classifications

Dependencies can be classified in many ways with regards to the type of failures. This is analysed hereafter where useful classifications are identified.

#### 5.1.3.1 Intrinsic Versus Extrinsic Dependencies

The first classical dependency classification consists to split them as follows:

- **Dependencies intrinsic** to the system. These dependencies find their roots in the design of the system. There are two classes:
  - *Functional dependencies*: the functional status of an item depends on the functional status of another one. Failures due to functional dependencies are often due to design errors.
  - *Cascade failures or propagating failures*: the failure of one item is the cause of the failure of another item which, in turn, can be the cause of failure of another item, etc. The cascading effect is often identified and taken into account by designers and operators.

- **Dependencies extrinsic** to the system. Typical extrinsic dependencies are:
  - Loss of support systems (e.g. loss of hydraulic, pneumatic, electric power).
  - Abnormal working environmental conditions (e.g. operating conditions exceeding the design ones).
  - Aggression from environment (e.g. excessive heat, corrosive atmosphere, lightning) impacting items located in the same area.
  - Item inadequacy (e.g. off specifications due to poor manufacturing).
  - Human interactions (e.g. items maintained by the same maintenance team).
This classification is useful to identify the origin of the dependencies and then of the common cause failures.

5.1.3.2 Logic Versus Dynamic and Lineage Dependencies

A second classification can be to split the dependencies between:

- **Logic dependencies**: they belong to the Boolean framework and can be described by conditional probabilities as this has been done in 5.1.1. The impacted items immediately fail.

- **Dynamic dependencies**: the effect of the underlying common cause is softer. It does not immediately trigger the failures of the impacted items but increases their probabilities of occurrence (e.g. the failure of the air conditioning increases the failure rate of electronic devices which, in turn, decreases the time to failure of the system). Dynamic dependencies can be intrinsic (e.g. functional dependency, soft cascade failure) or extrinsic (e.g. abnormal environment). When the effects begin to be perceptible in a short interval of time, they can be assimilated to “true” CCFs. Due to the non-immediate effect, this type of dependency is sometimes named semi-catastrophic.

- **“Lineage”** dependencies: they are linked to common causes impacting in the same way the probabilistic parameters of all the related components (e.g. when they are got from a bad batch or a good batch of components).

This classification is useful with regards to the available probabilistic models allowing to take them into consideration: the logic dependencies can be handled by Boolean family models (e.g. reliability block diagrams, fault trees, see Part 3 of the book), the dynamic dependencies by dynamic models (e.g. Markovian or Petri net approaches, see Part 4 of the book) and the lineage dependencies by using the uncertainty propagation techniques (see e.g. Chaps. 25, 32, 26 or 38).

It has to be noted that the item failures coming from a CCF are expected to occur within a limited time interval (see 5.1.1 and 5.1.2). Therefore, the qualification of CCFs strongly depends of what is meant by “limited time interval”. This is in particular the case for dynamic and lineage dependencies. For example, if an external event multiplies by 100 the item failure rates, it is likely to appear as a common cause of failure but, if it multiplies the item failure rates only by 2, it is likely to remain unnoticed. In fact, there is a continuum between failures occurring at the same time and failures occurring over a time interval and the qualification of “true” CCF may be a bit subjective.

---

1This term is used in this book to qualify non-tangible dependencies impacting items of the same origin, design, manufacturing, provider. That is to say items sharing the same pedigree (same lineage) and consequently of the same quality (good, medium or bad).
5.1.3.3 **Tangible Versus Non-tangible Dependencies**

A third classification can be to split the dependencies between:

- **Tangible or explicit dependencies**: they are the result of causes which can be clearly identified by performing in-depth system analyses (e.g. loss of power supply, pipe plugging, fire, flooding, etc.).
- **Non-tangible or non-explicit dependencies**: they are the result of causes difficult to apprehend due to the absence of field feedback or ignorance of the phenomena (epistemic problems).

This classification is useful with regards to the choice of the techniques used to take dependencies into account in the probabilistic modelling and calculations:

- The *tangible* common cause failures are easy to identify and should be identified, analysed and processed as any other event in the safety and dependability models developed in this book.
- The *non-tangible* common cause failures are difficult to identify or to qualify and generally constitute the residual failures whose causes cannot be explicitly modelled. However, they cannot be ignored without risking over-optimistic evaluations. Then broad approaches have been developed (e.g. beta-factor model, shock model) aiming to raise safeguards preventing to underestimate their impact.

5.1.3.4 **Human and Software Related Dependencies**

This chapter could not be complete without talking about the human factor which is often considered as the main source of common cause failures. The human interactions with the systems can be roughly classified as:

- Errors in the design, construction and installations: they generally belong to the *non-tangible* dependencies mentioned above.
- Errors in operation: they generally belong to *tangible* dependencies (e.g. shutting off a manual valve on the tapping of a sensor) and, as such, can be identified and quantified on their own.

Nowadays, the components and systems become more and more *smart*. That means that more and more software is introduced and software errors now tend to supersede the human factor as source of common cause failures.

Unfortunately, no really effective approaches have been developed yet to properly model the interactions between hardware, human factor and software. Then, the software “reliability” is generally evaluated separately by implementing specific techniques (see IEC 62628 (2012)) and often in a purely qualitative way (see IEC 61508 (2010)). This is why, within the reliability model of a system, the software is generally considered as a single isolated item constituting an *extrinsic* dependency. Without further analyses, it can even be considered as a *non-tangible* common cause of failure in many cases. Therefore, the software should be, at least, considered
through the broad models (e.g. beta-factor model, shock model) by adjusting the parameters (e.g. by engineering judgment) of these models.

### 5.2 Examples of CCFs Observed in Real Life

The impact of CCFs is not a purely theoretical view and they are involved in many situations which frequently occur. The last in date when writing this book is the emergence of the COVID-19 which in few days has locked almost all the activities of the countries over the planet and has killed several hundreds of thousands of people. This pandemic is the last case of calamity which all over the centuries, unfortunately, periodically impact a part of the planet: plague, leprosy, Ebola, influenza (Spanish, Asian, avian), HIV, SARS, etc. or starvation due to bad climatic conditions.

Hereafter are briefly described some typical accidents where CCFs are involved and some CCFs detected from reliability data collection.

#### 5.2.1 Examples of Typical Accidents Due to CCFs

Opening newspapers is all you have to do to hear about the CCFs: they frequently inform about incidents/accidents where CCFs are involved. Hereafter are described some illustrative examples.

**Example 5.1**

Apollo 13 lunar module was provided with 2 oxygen tanks (Jones 2016). On April 13th 1970, one oxygen tank exploded and the explosion destroyed the second oxygen tank, causing the failure of the mission. The 3-man crew managed to return safely to the Earth.

The failure of the second tank is a cascade failure.

**Example 5.2**

On March 3rd 1974, a McDonnell Douglas DC-10 airplane crashed into the Ermenonville forest outside Paris (France) (JO 1976). The cargo doors of the airplane were designed to open outwards under pressure but a specific latching system was provided to lock shut each of the cargo doors under pressure. After take-off, one of the latching systems failed and the rear left cargo door opened. A section of the cabin floor was ejected. However, even with such damages, the pilots could keep the airplane under control. Unfortunately, all the redundant control cables ran beneath the damaged floor and the pilots were then unable to maintain the airplane in the air. 346 people were killed.

A proper zone analysis would have identified that the redundant control cables are located in the same area, thus a design change would have prevented the loss of control of the airplane.
Example 5.3

On March 28th 1979, an accident has occurred in unit 2 of the Three Mile Island nuclear power plant and the core partially melted down (Rogovin and Frampton 1979). This was the result of a combination of equipment malfunctions, design-related problems and human errors. Among the causes, several pressuriser valves had been mispositioned after a periodic proof test and this constitutes a typical example of common cause failure due to human error. Although no injury had been reported, this accident is often mentioned as a textbook case of common cause failures due to human factor.

A better training of the operators may decrease the probability of such an event.

Example 5.4

The Viking Sky is a cruise ship launched in 2016 (Wikipedia Viking Sky 2019). Despite the storm warnings which had been issued, she was sailing from Tromsø to Stavanger (Norway) on March 23th 2019 with 1,373 people on board when she suffered from the failure of her four engines. A loss of lubrication oil pressure has been the common cause for the shutdown of the four engines. Due to rough conditions, the rescue was difficult (another common cause!). 470 passengers have been evacuated by helicopter before that three engines have been restarted in the night of March 24th and that the Viking Sky has been able to sail again. Sixteen people have been injured, three of them seriously.

Avoiding common utilities (here the lubrication system) is a good way to prevent such common cause of failures.

Example 5.5

The electric blackouts are a typical common cause of loss of electrical power supply for many people at the same time and at the level of towns, regions or even whole countries. The blackout is often itself the result of cascading failures from a single cause (e.g. high-voltage line break, electrical power plant shutdown, over consumption leading to protective circuit breaker opening). This arises rather often and see, for example, Wikipedia Blackouts (2020) or Wikipedia Outages (2020):

- United States: 1965 (230 kV line failure, Northeast), 1977 (storm, New York city), 2003 (electric power station failure, Northeast, 55 millions consumers impacted), 2008 (storm, California), 2008 (electric station failure, Florida), 2019 (Manhattan).
- France: 1978 (grid collapse), 1987 (winter cold), 1999 (storm).
- Japan: 1987 (winter cold), 2011 (seism magnitude 9).
- Canada: 1989 (solar wind), 1998 (freezing rain).
- Europe: 2006 (grid collapse, 15 million consumers impacted).
- Argentine, Paraguay, Uruguay: 2019 (grid collapse, 48 million consumers impacted).
- India: 2012 (grid collapse, 670 million consumers impacted).
Beyond the technical failures, the above list highlights the impact of meteorological or environmental (e.g. seism or solar winds) conditions as a source of common cause failures.

### 5.2.2 Examples of Typical CCFs Detected from Field Feedback

The reliability data collection is also an opportunity to identify common cause failures as this is highlighted with the two examples presented hereafter.

**Example 5.6**

A data collection and analysis of CCF data was performed in 2014-2015 on offshore platforms in the North Sea on several safety items (Hauge et al. 2015). Some of the CCF events recorded for Pressure Safety Valves (PSV) involved:

- Pilot exhaust lines plugged.
- Rust within the valves.

That means that, when analysing the collected data related to similar items having failed within a short interval of time, it has been discovered that these failures were due to a true CCF rather than to independent failures.

**Example 5.7**

The Organisation for Economic Co-Operation and Development (OECD) Nuclear Energy Agency (NEA) has set up the International Common Cause Data Exchange (ICDE) Project to collect and analyse CCF events on nuclear power plants.

The main causes of CCF for batteries are (NEA/CSNI/R (2003)19 2003):

- Battery design or manufacture inadequacy.
- Maintenance-induced failures.
- Internal malfunction.

Once more, that means that when analysing the collected data related to similar items having failed within a short interval of time, it has been discovered that these failures were due to a true CCF rather than to independent failures.

### 5.3 Dependent Failures Identification

When analysing a system, it is important to identify the potential CCFs as soon as possible to prevent them as far as possible. This is mainly important with regards to redundancy which is likely to be seriously impeded when CCFs are present. Then
a basic principle in dependent failure identification is to consider that dependent failures can occur as soon as items are on redundancy.

Any of the analysis techniques described in this book offers, to some extent, opportunities to identify common cause failure candidates provided that they are oriented toward this purpose. Specific approaches have also been designed for CCF identification. Hereafter are described three simple approaches which can be used for this purpose:

**Identification during preliminary analyses**

All the inductive approaches described in Chaps. 7–12 can be used. For example, hazard identification methods such as checklists (Chap. 11), Preliminary Hazard Analysis (Chap. 8) or even FMEA (Chap. 10) prove to be effective for identifying potential common cause failures (e.g. external events or possible cascade failures).

**Minimal cut sets analysis**

Reliability block diagram (Chap. 15) or fault tree (Chap. 16) approaches can also be used through the thorough analysis of each minimal cut set (see Chap. 16) with an order equal to or greater than two. This provides an effective technique to help to identify which causes are good candidates to produce CCF (see Chap. 17).

**Zone analysis**

The zone analysis (Desroches et al. 2015) is a specific technique focused on the identification of failure modes and scenarios of accidents by considering the geographical arrangement of the system all over its mission. It is the unique method for determining what could happen on redundant items located close to each other, for example, in the same room or the same cabinet (e.g. fire, flooding, overheating, corrosion).

### 5.4 CCF Data Collection

As for any other probabilistic calculations, no relevant result involving common cause failures could be obtained without sound estimations of the related probabilistic parameters. Like other probabilistic parameters, it is expected to obtain them from statistical analysis of field feedback collected through reliability data collection systems (see Chap. 38).

However, CCF events are typical rare events (far scarcer than events involved for ordinary reliability data collection). Then it is beyond the capability of a single operator to collect CCF data alone: it is therefore essential to collect and combine the CCF field feedback from many operators from different countries to perform meaningful estimations. This implies to implement rigorous data collection frameworks to gather, exchange and combine CCF data. As presented hereafter, this is done, for example, in nuclear industry and oil and gas industry.
Experience on CCF is scarce and most of it is coming from the nuclear industry:

- The US Nuclear Regulatory Commission issues many documents:
  - explaining how to code, collect and elaborate CCF data (NUREG/CR 4780 1988; NUREG/CR-5485 1998; NUREG/CR 6268 Rev. 1 2007);
  - providing CCF parameters about valves, pumps, heat exchangers, etc. (NUREG/CR-5497 2016).

- The Nuclear Energy Agency (BEA) from OECD manages an international joint project focused on CCF data exchange and also issues documents like NEA/CSNI/R(2003)19 (2003) about batteries, NEA/CSNI/R(2011)12 (2012) about CCF data exchange or NEA/CSNI/R(2019)4 (2019) about nuclear power plant modifications.

In the oil and gas industry, works are also achieved to collect and elaborate CCF data. For example, Hauge et al. (2013) provides CCF data elaborated mainly from the OREDA database (OREDA 2020). This database shared between several operators implements the ISO 14224 (2016) standard which provides some guidance about CCF data and has been developed to collect and exchange reliability data in the oil and gas industry.

The latest CCF data collection exercises related to safety instrumented systems (SINTEF A26922 2015) show that:

- The limited time interval to consider in the definition of CCF is of 1 year (the most common interval between proof tests, see Chap. 36).
- Due to the limited information on CCF frequency, only approaches with a low number of parameters are reasonably usable: the higher the number of parameters of the method, the higher the number of assumptions needed to implement the method.
- There are few CCF events on the items belonging to the same system so the past data collection exercises have been extended to identical items belonging to different systems. As a consequence, additional assumptions have been introduced for calculating the parameters of the various methods.

It has to be noted that, when dealing with safety systems, the unavailability is caused by dangerous failures and mainly by the dangerous undetected failures. Then, a proper identification and quantification of CCF is crucial for dangerous undetected failures. This is why the data collection exercises mentioned in reference SINTEF A26922 (2015) and NEA/CSNI/R(2003)19 (2003) are focused on such failures.

This leads to modelling methods related to dangerous undetected failures. However, they are often considered to be also applicable to dangerous detected failures or spurious failures but this is questionable.
5.5 CCF Modelling

5.5.1 Introduction

Let us consider a component $I_1$ belonging to a set of two similar components $\{I_1, I_2\}$. Its failures can be split into independent failures $\bar{I}_{1}^{Ind}$ and failures due to logic (see 5.1.3) common causes $\bar{I}_{1}^{2}$ between $\bar{I}_1$ and $\bar{I}_2$. This leads to:

$$\bar{I}_1 = \bar{I}_{1}^{Ind} \cup \bar{I}_1^2$$  \hspace{1cm} (5.5)

If the same component belongs to a set of three similar components $\{I_1, I_2, I_3\}$, its failures can be split in addition into the common causes $\bar{I}_{1}^{3}$ between $\bar{I}_1$ and $\bar{I}_3$ and also into the common causes $\bar{I}_{1}^{2,3}$ between $\bar{I}_1$, $\bar{I}_2$ and $\bar{I}_3$. This leads to:

$$\bar{I}_1 = \bar{I}_{1}^{Ind} \cup \bar{I}_1^2 \cup \bar{I}_1^3 \cup \bar{I}_{1}^{2,3}$$  \hspace{1cm} (5.6)

It has to be noted that in the above formulae $\bar{I}_{1}^{2} \equiv \bar{I}_2^1$, $\bar{I}_{1}^{3} \equiv \bar{I}_3^1$ and $\bar{I}_{1}^{2,3} \equiv \bar{I}_{1}^{1,3} = \bar{I}_3^{1,2}$

For a set of four components, this leads to:

$$\bar{I}_1 = \bar{I}_{1}^{Ind} \cup \bar{I}_1^2 \cup \bar{I}_1^3 \cup \bar{I}_1^4 \cup \bar{I}_{1}^{2,3} \cup \bar{I}_{1}^{2,4} \cup \bar{I}_{1}^{3,4} \cup \bar{I}_{1}^{2,3,4}$$  \hspace{1cm} (5.7)

And so on: even if some terms do not exist, their number increases very quickly when the size of the set of components increases and, except when tangible common causes are clearly identified, it is generally not really possible to take into account all the events involved in the above formulae. This is why simplified broad parametric models involving a limited number of terms have been developed to model the impacts of logic CCFs on system failures.

They are the main models used for CCF analyses and they aim to:

• provide a realistic prediction (i.e. conservative but not too much) of the probability of failure of systems comprising redundant components or, more generally, involving minimal cut sets of an order greater than one;
• prevent to perform unrealistic non-conservative predictions in case of non-tangible CCF;
• aid to determine the weak points involving CCFs and identify which defences against them are the most efficient.

The broad CCF modelling methods can be classified according to the number of required parameters (single or multiple) and according to the impact on item failures (i.e. if they occur with a probability equal to one or not).

The main broad models described hereafter comprise the beta-factor model (single parameter model) and the shock model (three parameters). Both models are devoted to logic CCFs and are recommended by IEC 61508-6 (2010).
5.5.2 The Beta-Factor Model

This is the simplest parametric model. It is described in IEC 61508-6 (2010), ISO/TR 12489 (2013), Humphreys and Proc (1987) and SINTEF A26922 (2015). This approach considers that the failure rate $\lambda$ of an item is the sum of an independent failure rate $\lambda_{Ind}$ and of a CCF failure rate $\lambda_{ccf}$:

$$\lambda = \lambda_{Ind} + \lambda_{ccf} \quad (5.8)$$

Then the beta factor, $\beta$, is defined as the ratio of the CCF failure rate to the (total) failure rate (i.e. the failure rate generally found in the reliability data handbooks OREDA (2015)):

$$\beta = \frac{\lambda_{ccf}}{\lambda} = \frac{\lambda_{ccf}}{\lambda_{Ind} + \lambda_{ccf}} \quad (5.9)$$

With: $1 > \beta > 0$

Then, from this definition:

$$\lambda_{ccf} = \beta \cdot \lambda \quad \text{and} \quad \lambda_{Ind} = (1 - \beta) \cdot \lambda \quad (5.10)$$

Values up to 10\% can be considered for the beta factor (IEC 61508-6 2010, Table D1).

This model is interesting because it can be easily modelled by Markov graphs (Chap. 31), Petri nets (Chap. 33) and Boolean models (Chap. 23).

It has to be noted that the same definition is also used to split the probability to fail due to a demand $\gamma$ such as:

$$\gamma = \gamma_{Ind} + \gamma_{ccf} \quad (5.11)$$

With:

$$\gamma_{ccf} = \beta \cdot \gamma \quad \text{and} \quad \gamma_{Ind} = (1 - \beta) \cdot \gamma \quad (5.12)$$

This method being very straightforward is well known and widely used. It can be easily implemented in the various models (reliability block diagrams, fault trees, Markovian approach or Petri nets) described in the other parts of this book.

Its main drawbacks are:

- without further additional assumptions, it can be used only with items exhibiting the same failure rate;
- it only models the failure of all the impacted items.

Compared to the formula established in 5.3.1, this approach consists in keeping only the last terms:
• $\bar{I}_1 = \bar{I}_{1 \text{Ind}} \cup \bar{I}_1^2$ for two components;
• $\bar{I}_1 = \bar{I}_{1 \text{Ind}} \cup \bar{I}_1^{2,3}$ for three components;
• $\bar{I}_1 = \bar{I}_{1 \text{Ind}} \cup \bar{I}_1^{2,3,4}$ for four components;
• etc.

Of course, the beta-factor model can be extended to more than one parameter in order to take other terms into account as this is done in various ways by the other modelling methods mentioned in 5.5.4.

### 5.5.3 The Shock Model

The shock model, also named the binomial failure rate (BFR) model (Atwood 1986), is a three parameter parametric CCF model.

- $\omega$: occurrence rate for lethal shocks.
- $\rho$: occurrence rate for non-lethal shocks.
- $\gamma$: conditional probability of failure of each item, given a non-lethal shock.

According to the definition of the above parameters, the common cause failure rate, $\lambda_{ccf}$, of a given item impacted by a shock (lethal or non-lethal) is given by:

$$\lambda_{ccf} = \omega + \gamma \cdot \rho \quad (5.13)$$

And the total failure rate of this item can be written as:

$$\lambda = \lambda_{\text{Ind}} + \omega + \gamma \cdot \rho \quad (5.14)$$

Like for the beta-factor model, $\lambda_{ccf}$ and $\lambda_{\text{Ind}}$ can be expressed as percentages of the item failure rate, $\lambda$:

- $\lambda_{\text{Ind}} = (1 - \beta) \cdot \lambda$.
- $\lambda_{ccf} = \beta \cdot \lambda$.

For the shock model, $\lambda_{ccf}$ can be split in turn with regards to the lethal and non-lethal shocks:

- Lethal failure rate: $\omega = \beta_{LC} \cdot \lambda$.
- Non-lethal failure rate: $\lambda_{nLC} = \gamma \cdot \rho = \beta_{nLC} \cdot \lambda$.

This implies:

- $\beta_{nLC} = \gamma \cdot \rho / \lambda$.
5.5 CCF Modelling

- $\beta_{LC} = \omega/\lambda$

- $\beta = \beta_{LC} + \beta_{nLC}$

And finally:

$$\lambda_{ccf} = \beta \cdot \lambda = (\beta_{LC} + \beta_{nLC}) \cdot \lambda$$ \hspace{1cm} (5.15)

$$\lambda_{Ind} = (1 - \beta) \cdot \lambda = [1 - (\beta_{LC} + \beta_{nLC})] \cdot \lambda$$ \hspace{1cm} (5.16)

Methods for assessing the parameters of the shock model are given in IEC 61508-6 (2010) (annex D), ISO/TR 12489 (2013) and Leroy (2018).

When a collection of $N$ similar items is affected by a lethal shock, all of the $N$ items fail and this has a similar impact as in the beta-factor model described above. This is the same for the non-lethal shock and when $\gamma = 0$, $\gamma = 1$ or $\rho = 0$, this approach is equivalent to the beta-factor model which takes only lethal shocks into account. As explained above for the beta factor, this can be easily modelled by Markov graphs (Chap. 31), Petri nets (Chap. 33) or Boolean models (Chap. 23).

Concerning the non-lethal shock, the probability of failure between $t$ and $t + dt$ of one impacted item is given by $\gamma \cdot \rho \cdot e^{-\rho \cdot dt}$: if this can be easily modelled by Markov graphs (Chap. 31) or Petri nets (Chap. 33), this is not directly possible by Boolean models (Chap. 23). Fortunately, integrating this formula over an interval $[0, t]$ gives the probability of failure of an impacted item as $\gamma \cdot [1 - e^{-\rho \cdot t}]$. This formula, which combines the probability that the non-lethal shock has occurred over $[0, t]$ and the probability of failure of the impacted item, can be handled by Boolean models (see Chap. 23).

Nevertheless, this is an approximated approach which should be used only when the CCFs cannot be clearly identified or when the related reliability data are not easily available (e.g. non-tangible CCFs).

When a collection of $N$ similar items is affected by a non-lethal shock, $\rho$, the probability that $k$ among them fail is equal to $C_N^k \cdot \gamma^k (1 - \gamma)^{N-k}$ where $C_N^k$ is the number of combinations of $k$ items among $N$. This binomial formula explains the name of binomial failure rate given to the approach.

With regards to a given item this implies:

$$\lambda_{nLc} = \gamma \cdot \rho \equiv \gamma \cdot \rho \cdot \sum_{k=0}^{N-1} C_N^k \cdot \gamma^k (1 - \gamma)^{N-k}$$ \hspace{1cm} (5.17)

Where $\sum_{k=0}^{N-1} C_N^k \cdot \gamma^k (1 - \gamma)^{N-k} = 1$ because encompassing all the possible cases of failure (from 0 to $N - 1$) of the $N - 1$ remaining items. This gives:
\[
\lambda_{nLc} = \rho \cdot \sum_{k=0}^{N-1} C_N^k \cdot \gamma^{k+1} (1 - \gamma)^{N-k} = \beta_{nLC} \cdot \lambda \tag{5.18}
\]

And then:
\[
\beta_{nLC} = \frac{\rho \cdot \sum_{k=0}^{N-1} C_N^k \cdot \gamma^{k+1} (1 - \gamma)^{N-k}}{\lambda} \tag{5.19}
\]

The above formulae can be simplified because, when dealing with a collection of numerous components affected by the same non-lethal shock, the probability of e.g. four component failures is negligible: this has never been observed for non-tangible CCFs and this is generally realistic for industrial systems. A conservative approach may be to consider that the quadruple failures due to a non-lethal shock are certainly at least lower than 10 times the double failures due to the same non-lethal shock. This implies \(C_N^2 \cdot \gamma^2 (1 - \gamma)^{N-2} > 10 \cdot C_N^4 \cdot \gamma^4 (1 - \gamma)^{N-4}\) which leads to:
\[
\frac{\gamma}{1 - \gamma} < \sqrt{\frac{C_N^2}{10 \cdot C_N^4}} \tag{5.20}
\]

When \(\gamma < 0.1\) then \(\frac{\gamma}{1 - \gamma} \approx \gamma\) and choosing \(\gamma \approx \sqrt{\frac{C_N^2}{10 \cdot C_N^4}}\) is certainly a conservative assumption. This allows to “tune” the value of \(\gamma\) to make the impact of CCF vanishing when the number of impacted items, actually failing on a non-lethal shock, increases.

Finally, for a set of \(N\) similar items with the same global failure rate, \(\lambda\), and impacted by a non-lethal shock, the parameters can be estimated as follows:

- Estimation of the global beta factor: \(\beta\).
- Independent failure rate: \(\lambda_{Ind} = (1 - \beta) \cdot \lambda\).
- Estimation of the lethal part of the beta factor: \(\beta_{LC}\).
- Lethal failure rate: \(\lambda_{Lc} = \beta_{LC} \cdot \lambda\).
- Non-lethal part of the beta factor: \(\beta_{nLC} = \beta - \beta_{LC}\).
- Non-lethal shock failure rate: \(\lambda_{nLc} = \beta_{nLC} \cdot \lambda\).
- Lethal failure rate: \(\omega = \beta_{LC} \cdot \lambda\).
- Non-lethal failure rate: \(\lambda_{nLc} = \beta_{nLC} \cdot \lambda\).
- Conditional probability of failure on non-lethal shock: \(\gamma \approx \sqrt{\frac{C_N^2}{10 \cdot C_N^4}}\).
- Occurrence rate of non-lethal shock: \(\rho = \frac{\lambda_{nLc}}{\gamma}\).

The above approach is effective when a great number of items are impacted by a non-lethal shock (e.g. a water hammer in hydraulic system): it allows to introduce the repartition between lethal and non-lethal shocks in order that the beta factor be kept constant and that, beyond the double or triple failures, the contribution of unrealistic multiple failures is neglected.
Then, the shock model is closer to the physical reality than the simple beta-factor model. The price to pay is the need for three parameters, $\beta_{LC}$, $\rho$ and $\gamma$ instead of one. But this number is independent of the number of items affected in the system.

### 5.5.4 Other Modelling Methods

From the seventies until now, several methods have been developed to extend the beta-factor model as, for example:

- **Basic parameter model** (NUREG/CR-5485 1998): it involves all the conditional probabilities identified in formula 5.7. As they are normally not readily available, other models with less stringent requirements on data were developed.

- **Multiple Greek letter model** (Fleming 1989; NUREG/CR-5497 2016): it is one of the models used by the US Nuclear Regulatory Commission for the assessment of the parameters of the CCFs.

- **Alpha-factor model** (NUREG/CR-5485 1998; NUREG/CR 6268 2007; NUREG/CR-5497 2016): it is also one of the models used by the US Nuclear Regulatory Commission for the assessment of the parameters of the CCFs.

- **PDS method**: developed for safety instrumented systems within the framework of the offshore petroleum industry (STF50 A0603 2006).

The above approaches are designed to be implemented at the level of a whole group of impacted items and they model how, among $m$ impacted items, 2, 3, 4 … items fail. They are interesting, on a case-by-case basis, to model the CCFs of such groups. However, they cannot be easily implemented into systemic models (e.g. reliability block diagrams, fault trees or Petri nets) for modelling large systems involving many other items. This is why they are not described in more detail in this book.

### References

ATWOOD CL (1986) The binomial failure rate common cause model, technometrics vol 28(2). American Statistical Association and American Society for Quality, USA

Desroches A, Leroy A, Vallée F (2015) La gestion des risques, Principes et pratiques. Lavoisier-Hermès, Paris, France, pp 41–67

Fleming KN (1989) Parametric models for common cause failure analysis in advanced seminar on common cause failure analysis in probabilistic safety assessment, Ispra Course. Ispra, Italy, pp 159–174

Hauge et al (2013) Reliability prediction method for safety instrumented systems—PDS method handbook, 2013th edn. SINTEF, Trondheim, Norway

Hauge S et al (2015) Common cause failures in safety instrumented systems—beta-factor and equipment specific check-lists based on operational experience, SINTEF A26922. Trondheim, Norway
Humphreys R, Proc A (1987) Assigning a numerical value to the beta factor common-cause evaluation. Proceedings of the National Reliability Conference, UK, 1987

IEC 60050-192 (IEV192) (2015) International electrotechnical vocabulary—Part 192: Dependability. International Electrotechnical Commission (IEC), Geneva, Switzerland

IEC 61508-6 Ed. 2.0 (2010) Functional safety: safety of electrical/electronic/programmable/electronic safety related systems, Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3, edition 2.0. Geneva, Switzerland

IEC 62628 (2012) Guidance on software aspects of dependability. International Electrotechnical Commission. Geneva, Switzerland

ISO/TR 12489 Ed. 1.0 (2013) Petroleum, petrochemical and natural gas industries. Reliability modelling and calculation of safety systems. International organization for standardization (ISO), Geneva, Switzerland

ISO 14224 Ed. 3.0 (2016) Petroleum, petrochemical and natural gas industries. Collection and exchange of reliability and maintenance data for equipment. International organization for standardization (ISO), Geneva, Switzerland

JO (1976) Rapport final de la Commission d’Enquête sur l’accident de l’avion D.C. 10 TC-JA V des Turkish Airlines survenu à Ermenonville le 3 mars 1974. (Année 1976. N°27. 12 mai 1976) Journal Officiel de la République Française

Jones H (2016) Common cause failures and ultra reliability. https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/. NASA Technical report server. Accessed September 2020

Leroy A (2018) Production availability and reliability. Use in the oil and gas industry, 1st edn. Wiley-ISTE, London, UK

Modarres M, Kaminskiy MP, Krivtsov V (2017) Reliability engineering and risk analysis—a practical guide, 3rd edn. CRC-Press

Mosley et al. (1988) Procedure for treating common cause failures in safety and reliability studies, U.S. Nuclear Regulatory Commission, NUREG / CR-4780, vol I and II. Washington, DC, USA

NEA/CSNI/R(2003)19 (2003) ICDE Project report: collection and analysis of common—cause failures of batteries, OECD Nuclear Energy Agency, Paris, France

NEA/CSNI/R(2011)12 (2012) International common cause failure data exchange (ICDE). General coding Guidelines. Nuclear Energy Agency. Paris, France

NEA/CSNI/R(2019)4 (2019) Collection and Analysis of Common-Cause Failures due to Nuclear Power Plant Modifications. Nuclear Energy Agency. Paris, France

NUREG/CR-5485 (1998) Guidelines on modelling common-cause failures in probabilistic risk assessment, US Nuclear Regulatory Commission, Washington

NUREG/CR-5497 2015 update (2016) Common-cause failure parameters estimations, 2015 Update. US Nuclear Regulatory Commission, Washington

NUREG/CR 6268 Rev. 1 (2007) Common-cause failure database and analysis system: event data collection, classification, and coding US Nuclear Regulatory Commission, Washington

OREDA Handbook (2015) Ed. 6.0 Offshore and Onshore reliability data. Prepared by SINTEF and NTNU. Hovik, Norway

OREDA database (2020) https://www.oreda.com/database/. Accessed September 2020

Rausand M (2014) Reliability of safety-critical systems: theory and applications. Wiley. Hoboken, New Jersey, USA

Rogovin M, Frampton GF (1979) Three mile Island: a report to the commissioners and to the public vol 1 to 3. NUREG /CR-1250. USNRC. USA

Wikipedia Blackouts (2020) https://fr.wikipedia.org/wiki/Liste_de_pannes_de_courant_importantes. Accessed September 2020

Wikipedia Outages (2020) https://en.wikipedia.org/wiki/List_of_major_power_outages. Accessed September 2020

Wikipedia Viking sky (2019) https://en.wikipedia.org/wiki/MV_Viking_Sky. Accessed September 2020