NTNU – Trondheim
Norwegian University of
Science and Technology

Determination of Beta-factors for Safety Instrumented Systems

Wenjing Sun

Reliability, Availability, Maintainability and Safety (RAMS)
Submission date: June 2013
Supervisor: Marvin Rausand, IPK

Norwegian University of Science and Technology
Department of Production and Quality Engineering

RAMS
Reliability, Availability,
Maintainability, and Safety

Determination of Beta-factor for Safety Instrumented Systems

Wenjing Sun

June 2013

MASTER THESIS

Department of Production and Quality Engineering
Norwegian University of Science and Technology

Main supervisor: Marvin Rausand
Co-supervisor: Yiliu Liu

NTNU

Faculty of Engineering Science and Technology
Department of Production and Quality Engineering

Date
2013-01-14

Our reference
MR/KEDA

MASTER THESIS
2013
for
stud. techn. Wenjing Sun

DETERMINATION OF BETA-FACTORS FOR SAFETY-INSTRUMENTED SYSTEMS

(Fastsetting av beta-faktorer for instrumenterte sikkerhetssystemer)

Safety-instrumented systems (SISs) are used in many industries to prevent hazardous events and/or to mitigate their consequences. Reliability requirements to SISs are based on international standards, such as IEC 61508 and IEC 62061 (for machinery systems). The system integrator has to verify that the supplied SIS meets the given requirements. The requirements are partly qualitative and partly quantitative. The focus of this master thesis is on the effects of common-cause failures (CCFs) for the reliability of a SIS.

IEC61508 recommends the beta-factor model for for analysis of CCFs and suggests a procedure for how to determine an application-specific beta-factor. This procedure is based on a set of questions and a scoring system of the answers to these questions. A slightly different approach to determine the beta-factor is suggested in IEC62061 for high-demand systems. Another approach is suggested by the British nuclear industry and is called the unified partial method (UPM).

The methods in IEC61508 and IEC62061 are suggested without a specific justification and many risk analysts are therefore sceptical to the results obtained by these methods. The criticism has mainly been concentrated on whether the questions are appropriate and complete, and also the scoring procedure.

The overall objective of this master thesis is to evaluate the available approaches for determination of the beta-factor with respect to rationale, adequacy, and uncertainty.

As part of this master thesis the candidate shall:

1. Provide a definition of a CCF in a SIS (low-demand and high-demand), give a brief description of the beta-factor model for CCF-analysis, and list the pros and cons of the beta-

factor model.

2. Carry out a literature survey related to determination of an application-specific beta-factor. The survey shall as a minimum include the procedures in IEC61508, IEC62061, and the UPM method.
3. Make a critical evaluation of each of the 37 questions in IEC 61508, part 6, related to effect on the occurrence of CCFs, and discuss whether any of the questions should be skipped, merged, or reformulated. The candidate should also discuss the need for additional questions, e.g., related to human and organizational aspects.
4. Discuss the procedure used in IEC 61508, part 6, to calculate the beta-factor based on the answers to the 37 questions. If adequate, the candidate may suggest an improved approach.
5. Make a detailed comparison of the approaches in IEC61508 and IEC62061. Will they give similar results both for low-demand and high-demand systems?
6. Make an evaluation of the UPM method and compare this approach with the IEC approaches.
7. Identify and discuss challenges related to the determination of application-specific beta-factors, for which further research is needed.

Following agreement with the supervisors, the various points may be given different weights.

Within three weeks after the date of the task handout, a pre-study report shall be prepared. The report shall cover the following:

- An analysis of the work task's content with specific emphasis of the areas where new knowledge has to be gained.
- A description of the work packages that shall be performed. This description shall lead to a clear definition of the scope and extent of the total task to be performed.
- A time schedule for the project. The plan shall comprise a Gantt diagram with specification of the individual work packages, their scheduled start and end dates and a specification of project milestones.

The pre-study report is a part of the total task reporting. It shall be included in the final report. Progress reports made during the project period shall also be included in the final report.

The report should be edited as a research report with a summary, table of contents, conclusion, list of reference, list of literature etc. The text should be clear and concise, and include the necessary references to figures, tables, and diagrams. It is also important that exact references are given to any external source used in the text.

Equipment and software developed during the project is a part of the fulfilment of the task. Unless outside parties have exclusive property rights or the equipment is physically non-moveable, it should be handed in along with the final report. Suitable documentation for the correct use of such material is also required as part of the final report.

The student must cover travel expenses, telecommunication, and copying unless otherwise agreed.

If the candidate encounters unforeseen difficulties in the work, and if these difficulties warrant a reformation of the task, these problems should immediately be addressed to the Department.

The assignment text shall be enclosed and be placed immediately after the title page.

Deadline: June 10th 2013.

Two bound copies of the final report and one electronic (pdf-format) version are required.

Responsible Supervisor at NTNU: Marvin Rausand
Phone: 73 59 25 42
E-mail: marvin.rausand@ntnu.no

Co-supervisor: Yiliu Liu
Phone: 73 59 20 38 / 47 44 17 75
E-mail: yiliu.liu@ntnu.no

**DEPARTMENT OF PRODUCTION
AND QUALITY ENGINEERING**

Per Schjølberg

Per Schjølberg
Associate Professor/Head of Department

Marvin Rausand
Responsible Supervisor

Preface

This Master thesis is written in the international program of Reliability, Availability, Maintainability, and Safety (RAMS) at Norwegian University of Science and Technology (NTNU) during the spring semester of 2013. The topic of the thesis is *Determination of Beta-factor for Safety Instrumented Systems.* The responsible supervisor of the subject have been Marvin Rausand and Yiliu Liu.

Safety instrumented systems are very important for process industries to effectively prevent hazardous events from developing into accidents. In safety instrumented systems, there are still many kinds of failures that could could result in accidents. Common cause failures play a big part of contributing to many major accidents, which could lead to a serious consequence. For example, the offshore drilling rig accident occurred in 1982 which result in the entire 84 man crew on the rig die. Although common cause failures are mentioned in OREDA (2002) related to fire and gas detectors, there is no guidance on how to collect the data of common cause failures. For now, it is impossible to avoid common cause failures. The only thing we can do is to reduce common cause failures as many as possible.

The whole master thesis is divided into three parts. The first part is a brief introduction of safety instrumented systems. The second part is an introduction of common cause failures. The last part contains an introduction, an analysis and a comparison of three methods used to determine β-factor for SIS: IEC 61508 checklist, IEC 62061 checklist and unified partial method.

Trondheim, June 2013

Wenjing Sun

Signature

Acknowledgment

I would like to thank my supervisor Professor Rausand, from the Department of Production and Quality Engineering at NTNU, for giving me very useful advice of selecting the topic of the master thesis. Because I wrote about *SIL in Operation* for my project thesis last semester, I was unsure whether it is a good idea to continue this topic for my master thesis. After the discussion, Professor Rausand analyzed my situation and gave me a good idea about how to decide the topic. Finally, I decided to write about one of the common cause failure factors which is β-factor, which is also related to the project written in the last semester. Also, Professor Rausand provided me with some very useful materials about my master thesis. Besides, I am grateful for Professor Rausand's precious time to help me with all the problems that I encouraged during the process of writing my master thesis.

I also would like to thank my co-supervisor Yiliu Liu from the Department of Production and Quality Engineering at NTNU, for his helpful supports, invaluable advices and quick feedback on my work. Whenever I meet tough questions, he always helps me and keeps my spirits up.

Overall, I strongly believe the quality of the thesis has improved significantly with all their helps.

W.S.

Summary

Safety instrumented systems are vital safety barriers to reduce the probability of the hazardous events and mitigate the consequences. Safety instrumented systems have been widely used in many kinds of industries. Redundancy is often introduced in safety instrumented systems for higher reliability. Although redundancy has many benefits, the negative effects cannot be ignored. Redundancy induces common cause failures to safety instrumented systems. The common cause failures are a big threat to the reliability of systems, which contributes to many major accidents. Therefore, it is very important to take common cause failures into consideration in risk and reliability assessment for the whole life cycle, especially in the design phase.

There are two common cause failure modeling methods: explicit modeling and implicit modeling. The Beta-factor model belongs to implicit modeling and it is the simplest and widely used model. Many common cause failure models have been developed based on the beta-factor model. Three methods for the determination of beta-factor demonstrated in this master thesis: two IEC checklists (IEC 61508-6 and IEC 62061) and unified partial method (UPM). The procedures for beta-factor determination of these three methods are presented, the critical evaluation is performed for the IEC 61508-6 checklist, discussions on the effectiveness of questions are conducted, and a recommended question list of IEC 61508 is provided. Next, a detailed comparison between two checklists (IEC 61508-6 and IEC 62061) is carried out. As well the comparison between the checklist methods and the unified partial method is also demonstrated. Finally, some suggestions for the further work are provided at the end of this master thesis.

Contents

1 Safety Instrumented Systems

1.1 Introduction of Safety Instrumented Systems

Nowadays, in order to guarantee safety, safety instrumented systems (SISs) are increasingly used as safety barriers in all kinds of industries. A SIS is used to perform one or more safety instrumented functions (SIF) to prevent hazardous events or mitigate their consequences. According to IEC 61511 (2003), a SIS is a safety system that includes at least one electrical, electronic, or programmable electronic component. A SIS is a computer-based system which is generally composed by three parts: input elements, logic solvers, and final elements. Input elements could be sensors or pressure transmitters. Logic solvers could be programmable logic controllers (PLC). And final elements also can be called actuating items, for example could be shutdown valves. When the pressure of the system surpass the defined pressure, the signal will sent to the logic solver, and then the logic solver transmits the signal to the valves. The valves will be closed to protect the system from hazards. A simple SIS is shown in Figure 1.

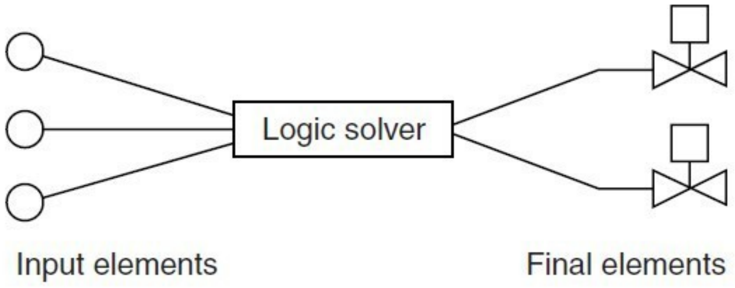


Figure 1: Main parts of a safety instrumented system (Rausand and Høyland, 2004)

1.2 Reliability Assessment of Safety Instrumented Systems

To ensure the reliability of SIS, it is very important for reliability engineers to identify whether the status of all the elements are functioning or not functioning in a functional block. However, all potential failures in SIS should be identified first.

1.2.1 Failures of SIS

For now, there is no way to identify all the potential failures because of the fact that there are too many types of failure modes. Therefore, we can classify failures based on different causes.

There are various ways to classify failures. Generally, failures can be classified based on the causes of failure and the effects of failure (Lundteigen, 2006). Rausand (2010) divides failures into two categories based on the failure effects:

- Dangerous failure

  > failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:
  >
  > a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or
  >
  > b) decreases the probability that the safety function operates correctly when required

- Safe failure

  > failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:
  >
  > a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or

b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state

In short, dangerous failures will cause damages or hazards in a system. In contrast, safe failures are failures that will not cause any damages or will not make the system fail.

Since the safe failures do not lead to major disabling of the system's functioning ability as required, sometimes only dangerous failures are taken into consideration. Dangerous failures can be further divided into:

- Dangerous detected (DD) failure

DD failures are the failures that will be detected immediately after it occurs.

- Dangerous undetected (DU) failure

DU failures are hidden failures that are only revealed by diagnostic test.

Safe failure can be comprised by

- Safe detected (SD)

SD failures are detected by automatic self-testing.

- Safe undetected (SU)

SU failures cannot be detected by automatic regular self-testing.

The classification of failure modes is shown in Figure 2.

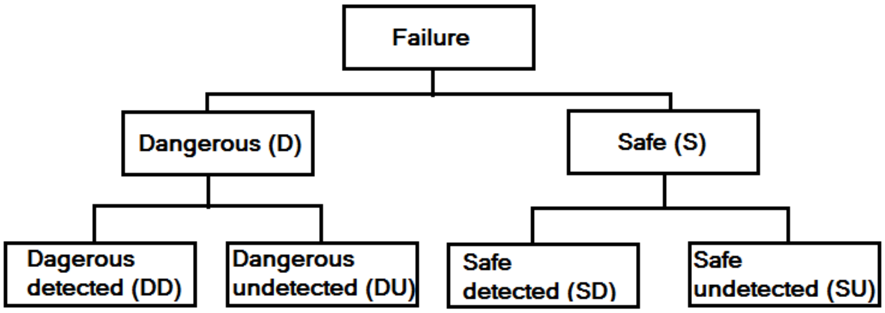


Figure 2: failure classification based on the causes of failures (Rausand, and Høyland, 2004)

IEC 61508 (2010) classified failures into random hardware failure and systematic failure based on the causes of failure. Random hardware failure can also be called physical failure. While systematic failure is nonphysical failure. The failure classification proposed by IEC 61508 is illustrated in Figure 3.

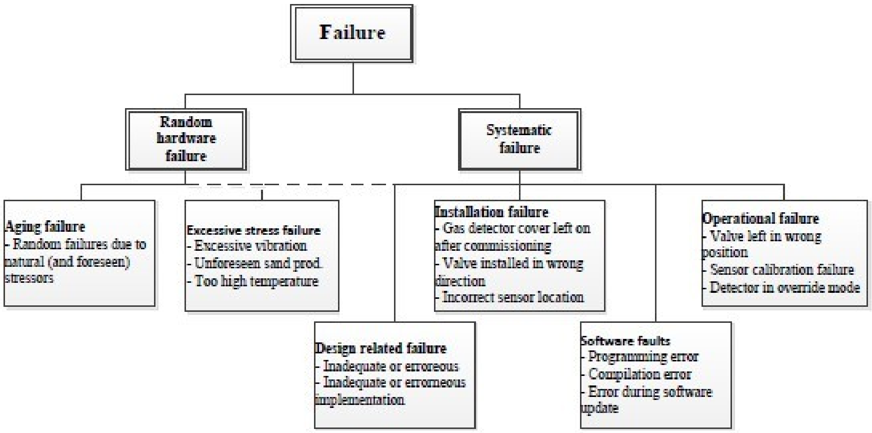

Failure
Random hardware failure
Systematic failure
Aging failure
- Random failures due to natural (and foreseen) stressors
Excessive stress failure
- Excessive vibration
- Unforeseen sand prod.
- Too high temperature
Installation failure
- Gas detector cover left on after commissioning
- Valve installed in wrong direction
- Incorrect sensor location
Operational failure
- Valve left in wrong position
- Sensor calibration failure
- Detector in override mode
Design related failure
- Inadequate or erroreous
- Inadequate or erromeous implementation
Software faults
- Programming error
- Compilation error
- Error during software update

Figure 3: Possible failure classification by cause of failure (IEC 61508, 2010)

Random hardware failure:

> A failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware. (IEC 61508, 2010)

Random hardware failure can further be divided into aging failure and stress failure. Aging failures are failures occurring because of design scope. Stress failures are failures that occur due to excessive stress on the item, which may be caused by human error when operating. (Rausand, 2004.)

Systematic failure:

> A failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors. (IEC 61508, 2010)

The overall failure classification scheme is illustrated in Figure 4 based on the bow-tie structure.

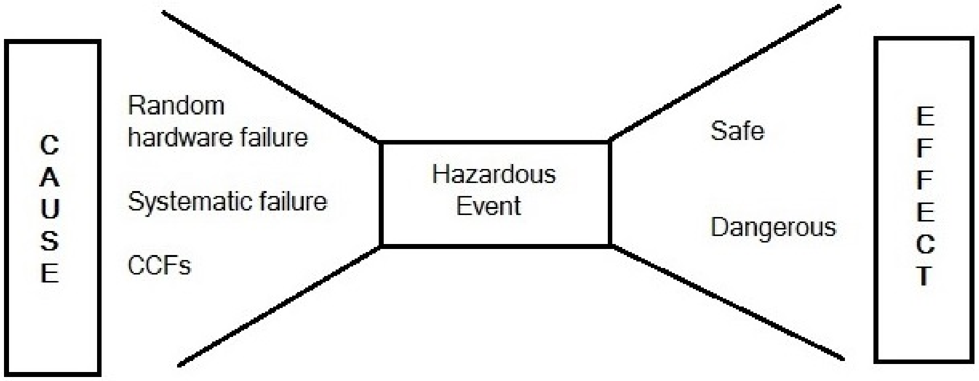


Figure 4: failure classification scheme (adopted from Lundteigen, 2006)

The PDS method (Hauge, 2010) also uses the same classification with IEC 61508, but the excessive stress failure is included in systematic failure instead of random hardware failure. The detailed failure classification illustrated in PDS method is shown in Figure 5.

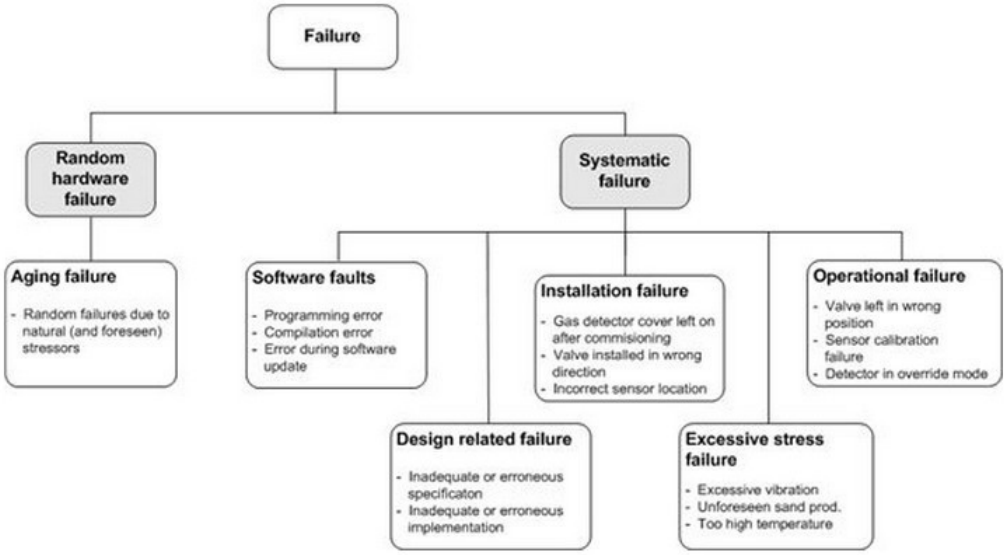

Failure
Random hardware failure
Systematic failure
Aging failure
- Random failures due to natural (and foreseen) stressors
Software faults
- Programming error
- Compilation error
- Error during software update
Installation failure
- Gas detector cover left on after commisioning
- Valve installed in wrong direction
- Incorrect sensor location
Operational failure
- Valve left in wrong position
- Sensor calibration failure
- Detector in override mode
Design related failure
- Inadequate or erroneous specificaton
- Inadequate or erroneous implementation
Excessive stress failure
- Excessive vibration
- Unforeseen sand prod.
- Too high temperature

Figure 5: Failure classification used in PDS method. (Hauge et al., 2010)

Through the classification of failures, it is easy to understand the failures and assess the reliability of SIS.

1.2.2 Reliability Assessment Methods

Low demand systems are very different from the high demand systems, not only the frequency of the failure on demand, but also the methods used to analyze the reliability of systems. The following methods are used to analyze the reliability of SIS:

- Markov methods
- Fault Tree Analysis (FTA)
- Reliability Block Diagrams (RBD)
- Risk graph
- Layer of protection analysis (LOPA)

Markov method can be a qualitative or a quantitative method. It is suitable for small but complex systems with dynamic properties. After understanding the system, transaction diagram can be built; therefore, it helps to understand how the system operates. The limitation of this method is that it only applies on small systems. Besides, the failure rate is required to be constant.

A fault tree is a top-down logic diagram which is formed by OR gates and AND gates to display the relationship between events in a system. The basic events are the events located at the lowest level. Normally, the basic events are component failures, human errors or environment conditions. Fault tree analysis can be qualitative or quantitative, and sometimes it could be qualitative and quantitative. In contrast to Markov analysis, fault tree analysis is not suitable for analyzing dynamic systems. However, it has been widely used in many application areas. Besides, it is suitable to analyze large and complex systems.

A fault tree can always be converted to reliability block diagram. Also, reliability block diagrams can always be converted to fault trees. According to Rausand (2011), a reliability diagram shows the logical connections of functioning items that are needed to fulfill a specified system function. In a block diagram, if a function could go though from the start to the end, then we say that the item is functioning.

Risk graph and LOPA are qualitative methods. Fault tree analysis and reliability block diagrams are usually used for low-demand systems, while Markov method is suitable for high-demand systems.

1.2.3 Reliability Assessment Measures

To assess the reliability of SISs, the concept of safety integrity level (SIL) is introduced.

Based on the Business Dictionary , the definition of the reliability is

> the ability of an apparatus, machine, or system to consistently perform its intended or required function or mission, on demand and without degradation or failure.

Safety integrity is the probability that the safety related systems perform the required safety function in a defined period of time under all kinds of conditions. The reliability of SIS is measured by SIL. The definition of SIL from IEC 61508 (2010) is

> Discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest.

SIL is a measure of the reliability of SIS, which is divided into four classes according to the probability of failure on demand (PFD). PFD is the average proportion of time the item is not performing its intended functioning, which is used in low demand operation mode. SIL is showed by probability of failure per hour (PFH) when it used in high demand mode or continuous mode.

When the safety related system operates in a low demand mode, SIL classification is shown in Table 1, while SIL classification is shown in Table 2 when the safety related system is in high demand mode and continuous mode.

Table 1: SIL classification on low demand mode (IEC 61508, 2010)

Safety Integrity level (SIL)	**Average probability of a dangerous failure on demand of the safety function ($\mathbf{PFD}_{avg}$)**
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Table 2: SIL classification on high demand mode (IEC 61508, 2010)

Safety Integrity level (SIL)	**Average probability of a dangerous failure of the safety function** $\left[h^{-1}\right]$ **(PFH)**
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

PFD PFD is normally calculated to measure the quality of SIF. Both standard IEC 61508 and IEC 61511 use SIL as a measure to assess the reliability of SIS. SIL is obtained and classified by the value of PFD, which has been introduced. When PFD is used for low-demand systems, it can be obtained from the following equation:

$$PFD = 1 - \frac{1}{\tau}\int_0^\tau R(t)\,dt$$

Normally the failure which is considered for PFD calculation is DU failure. For a single component, the survivor function is

$$R(t) = e^{-\lambda_{DU}\mathrm{t}}$$

Therefore,

$$PFD = 1 - \frac{1}{\tau}\int_0^\tau R(t)\,dt$$

$$= 1 - \frac{1}{\tau}\int_0^\tau e^{-\lambda_{DU}t}\,dt$$

$$PFD = 1 - \frac{1}{\lambda_{DU}\tau}\left(1 - e^{-\lambda_{DU}\tau}\right)$$

we can replace $e^{-\lambda_{DU}\tau}$ by its Maclaurins series, and get

$$PFD = 1 - \frac{1}{\lambda_{DU}\tau}(\lambda_{DU}\tau - \frac{(\lambda_{DU}\tau)^2}{2!} + \frac{(\lambda_{DU}\tau)^3}{3!} - \frac{(\lambda_{DU}\tau)^4}{4!} + ...)$$

$$= 1 - (1 - \frac{(\lambda_{DU}\tau)}{2} + \frac{(\lambda_{DU}\tau)^2}{3!} - \frac{(\lambda_{DU}\tau)^3}{4!} + ...)$$

when $\lambda_{DU}\tau$ is small enough and can be ignored, then

$$PFD = \frac{\lambda_{DU}\tau}{2}$$

The above PFD equation is for a single component. Normally, PFD is calculated using the approximate equation for KooN architecture. Using the same principle for parallel components, we can get the approximate equations. The equations are listed on the following table.

Table 3: PFD of Some koon Systems of Identical and Independent Components with Failure Rate λ and Test Interval τ. (Rausand and Høyland, 2004)

k\n	**1**	**2**	**3**	**4**
1	$\frac{\lambda_{DU}\tau}{2}$	$\frac{(\lambda_{DU}\tau)^2}{3}$	$\frac{(\lambda_{DU}\tau)^3}{4}$	$\frac{(\lambda_{DU}\tau)^4}{5}$
2	–	$\lambda_{DU}\tau$	$(\lambda_{DU}\tau)^2$	$(\lambda_{DU}\tau)^3$
3	–	–	$\frac{3\lambda_{DU}\tau}{2}$	$2(\lambda_{DU}\tau)^2$
4	–	–	–	$2\lambda_{DU}\tau$

PFH The definition of PFH in IEC 61508 (2010) is

> Average frequency of a dangerous failure of an E/E/PE safety related system to perform the specified safety function over a given period of time.

PFH is used to classify SIL for continuous or high-demand mode of operation. If the E/E/PE safety related system is the last safety layer, the PFH should be calculated by

$$F(T) = 1 - R(t)$$

which is the unreliability of the system. And if the E/E/PE safety related system is not the ultimate safety layer, then the PFH should be calculated by

$$PFH = \frac{1}{MTBF}$$

which is the unavailability of the system. MTBF is the abbreviation of mean time between failure.

To calculate PFH for a safety-instrumented system, use the following formula in IEC 61508

$$PFH_{SYS} = PFH_S + PFH_{LS} + PFH_{FE}$$

S, LS, and FE represent the three parts of a safety instrumented system.

S means sensors in a safety-instrumented system;

LS means logic solvers in a safety-instrumented system;

FE means final elements in a safety-instrumented system, like valves.

1.2.4 Reliability for Redundancy Architecture

To improve the reliability of SIS, redundant components are introduced to make sure the system works if single components fail.

> Redundancy: The provision of one or more additional measures, usually identical, to provide fault tolerance. (IEC 61508, 2010)

There are two kinds of redundancy in SIS. Redundant components could be used in parallel with the single components and then share the load, which is called *active redundancy*. Also, the redundant components can be in standby position, which can be active only if the single components fail. This kind of redundancy called *passive redundancy*.

Although redundancy prevents independent failures and improves the reliability of SIS, it may lead to CCFs because coupling factors will link more than two separate channels in a multiple channel. CCFs are failures that more than two components fail and share the same cause. CCF is a kind of dependent failures. The definition of dependent failures is shown in Table 4.

Table 4: Definition of dependent failure (Rausand and Høyland, 2004)

Dependent Failure			The probability of a group of events which probabilities cannot be expressed as a simple product of unconditional probability of failure of single components.
	Common Cause Failure		This is a kind of dependent failure which occurs in redundant components in which a single common cause - simultaneously or near simultaneously leads to failures in different channels.
		Common Model Failure	This definition applies to failures of common causes in which multiple elements fail similarly in the same mode.
	Cascade Failure		These are all dependent failures that do not share a common cause, meaning they do not affect redundant components.
Additionally: The definition of dependent failures“ includes all definitions of failures that are not independent. This definition of dependent failures clearly implies that an independent failure in a group of events can be expressed as a simple product of conditional probabilities of failures of a single event.			

CCF is a part of dependent failure, while common model failure (CMF) is a part of CCFs. In this master thesis, we only focus on CCFs.

CCF is a serious threat to SIS reliability (Edwards and Waston, 1979). CCFs contribute to many major accidents, which has major negative impacts. For example, offshore drilling rig accident occurred in 1982. The entire 84 man crew on the rig was lost. The CCF is a total loss of ballast control and of stability (Rausand, 2011). Although CCFs are mentioned in OREDA (2002) related to fire and gas detectors, there is no guidance on how to collect CCFs data. For now, it is impossible to avoid CCFs. Hence, what we can do is to reduce common cause as many as possible. In the next chapter, we will present the detailed definitions of CCFs and the assessment methods.

2 Common Cause Failures

2.1 Definitions

IEC 61508 is widely used in Oil & Gas companies, which is the basic standard for industries to develop their own standards. The standards developed based on IEC 61508 are shown in the Figure 6.

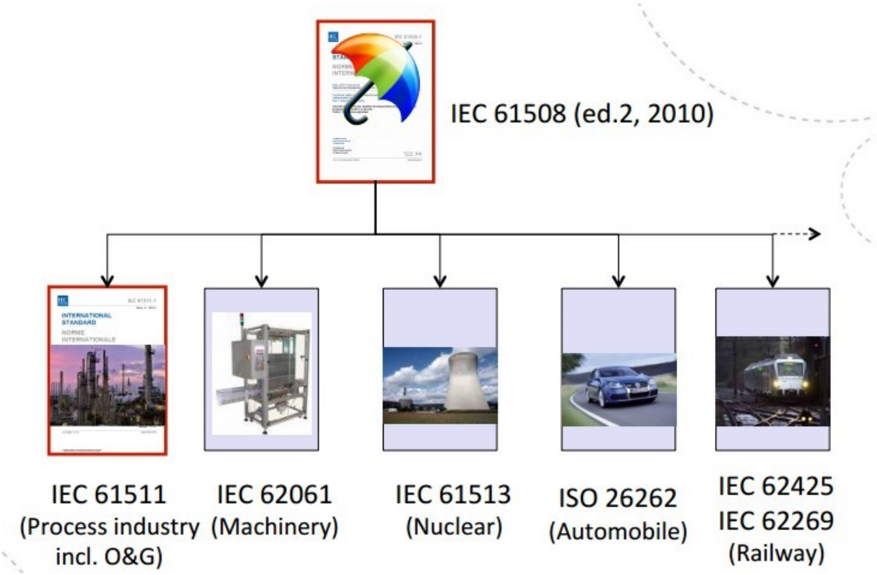


Figure 6: Standards for safety instrumented systems (Jin, 2012)

Although CCFs are taken into consideration during risk and reliability assessment for many years, there is no unified definition for industries, since different authors and engineers in different areas hold different ideas.

Wetherholt (2011) demonstrates a simple definition of a common cause failure:

> A failure of two or more components, system, or structures due to a single specific event or cause.

A more complex definition is

> An event or cause which bypasses or invalidates redundancy or independence, i.e., an event which causes the simultaneous loss of redundant or independent items which may or may not include inadvertent operation, or an unintended cascading effect from other operations or failure within the system.

In next section, definitions of CCF in different industries will be reviewed.

2.1.1 Oil and Gas Industry

Based on the standard IEC 61508, CCF is defined as

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

In this definition, the description of “concurrent failures of two separate channels in a multiple channel system” and “leading to system failure”cannot be used together in some conditions. For example, in 2oo3 or 2oo4 configuration, two separate channels failing at the same time are not belong to CCFs because the system is still functioning. Redundancy is widely used in safety instrumented systems to improve the reliability of the system. Meanwhile, redundant components exposes the system into CCFs. Therefore, the description of CCF in IEC 61508 cannot be used for KooN structure.

The standard is mainly used for Oil & Gas industry and process industry; therefore, this definition is the same with the one used in the standard IEC 61511 which is used for process industry.

2.1.2 Machinery Industry

According to the standard BS EN ISO 12100:2010, CCFs in the machinery industry is defined as

> Failures of different items, resulting from a single event, where these failures are not consequences of each other.

BS EN ISO 12100:2010 is *Safety of machinery — General principles for design — Risk assessment and risk reduction* (ISO 12100:2010). It is different from the standard BS EN 62061:2005. BS EN 62061:2005 is *Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems*. The definition of CCF in standard BS EN 62061:2005 is defined as

> Which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel (redundant architecture) subsystem, leading to failure of a SRCF. (IEC 61508-4, 3.6.10 modified)

In standard ISO 12100, "failures are not consequence of each other" are independent failures, which means that one component's failure will not affect other components' functions. The definition of CCF in ISO 62061 is modified based on IEC 61508-4. As described above, the definition is not suitable for the redundant architecture. However, standard IEC 62061 modifies this inaccurate statement, and presents that it is suitable for redundant architecture subsystem. It means that two or more than two channels failure will also cause the subsystem failures.

2.1.3 Nuclear Power Industry

Based on NEA (2004b), CCF is defined as

> 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.

In this definition, dependent failure means

> Failure whose probability cannot be expressed as the simple product of the unconditional probabilities of the individual events that caused it. (IEC 61508, 2010)

It is about two or more components fault states that exist simultaneously due to a shared cause, which do not include cascading failures. Cascading failures are component failures caused by another failure, and it is not the direct result of a shared cause. All hidden failures can be revealed during functional test; therefore, short time interval means at least from one component failed to next functional test.

2.1.4 Space Industry

According to Stamatelatos (2002a), CCF is defined as:

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

In this definition, *the system mission* means CCFs occurred during the period of a system carrying out a task, not a specific time period or time interval. For aviation industry, system mission is the time period that a plane is in the air for a flight.

2.1.5 Proposed Definition of CCFs

Based on the different definitions of CCFs, Smith and Watson (1980) reviewed nine definitions and suggest that the following six attributes have to be included in the definition of CCFs

1. The components 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 interval (e.g., the time a plane is in the air during a flight).

5. The failures are due to a single underlying defect or a physical phenomenon (the common cause of failures).

6. The effect of failures must lead to some major disabling of the system's ability to perform as required.

The first attribute presents that CCF has lead to the components failure and is unable to perform the required function. The second attribute presents that multiple failures can exist within a KooN architecture, which modified the unclear statement in standard IEC 61508. For the third attribute, "*first in line*" means the failure is caused by the root cause like human error, environment, not affected by the other component's failure. In other words, first in line failures means independent failures, and cascading failures are not included in this definition. The fourth attribute shows the time interval for the occurring of CCFs, which is a defined critical time interval. Critical time interval is different in different systems. For SIS, time interval means the time period between two functional tests for a same system. However, for aviation industry, the critical time interval is the plane in the air for one mission.

According to these six attributes, the definition of CCF is given by Smith and Watson (1980):

> Inability of multiple, first-in-line items to perform as required in a defined critical time period due to a single underlying defect or physical phenomena such that the end effect is judged to be a loss of one or more systems.

2.2 Causes of CCFs

Based on Rausand (2011), Causes of CCFs are classified into two categories:

- Root cause

The most basic reason for a component failure, which, if corrected, could prevent recurrence of this and similar failures.

- Coupling factor

  A property that makes multiple components susceptible to failure from a single shared cause.

Root causes are about why the components failed which related to the components. The coupling factors are about why more than one component are affected, which is about the relation between the affected components. Root causes are normally identified by root cause analysis (RCA), supported by checklists of generic root causes (US DOE, 1992). Both root causes and coupling factors could lead to CCFs, which is illustrated in Figure 7.

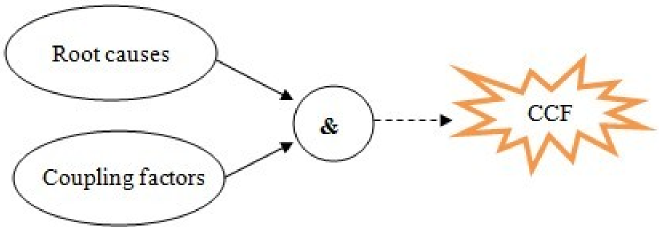


Figure 7: Causes of common cause failures (Lundteigen, 2007)

Examples of coupling factors are same designs, same procedures or same maintenance or operation staff. The majority of coupling factors contributing to CCFs are related to operational aspects (Miller, 2000). However, to save money and ease operation and maintenance, the procedures of industries have become more and more standardized. Therefore, more coupling factors arise.

The nuclear power industry has proposed a classification for CCFs causes, which is shown in Table 5 NEA (2004):

Table 5: ICDE classification of common causes (NEA, 2004)

Classification of root causes	**Classification of coupling factor**
• State of other components • Design, manufacture or construction inadequacy • Human actions • Maintenance • Internal to component • Procedure inadequacy • Abnormal environmental stress • other	• Same/similar hardware: - Hardware design - System design - Hardware quality deficiency • Same/similar operational conditions: - Maintenance/test schedule - Maintenance/test procedure - Maintenance/test staff - Operation procedure - Operation staff • Same/similar environmental exposure: - Internal - External • other

Many authors and studies have done investigation of root causes of CCF events. Based on Common Cause Failure Modeling: Status and Trends (2008), the following Tables 6, Table 7 and Table 8 are the proposed classification schemes of these events.

Table 6: Root causes of CCF events (design, manufacturing, construction, installation and commissioning)

Cause type	**Examples of specific cause**
Design requirements and specifications inadequacy	Designer failure to predict an accident Designer failure to recognize what protective action is needed
Design error or inadequacy in design realization	Inadequate facilities for operation, maintenance, testing or calibration Inadequate components Inadequate quality assurance
Design limitations	Financial Spatial
Manufacturing error or inadequacy	Failure to follow instructions Inadequate manufacturing control Inadequate inspection Inadequate testing
Construction/installation / commissioning	Failure to follow instructions Inadequate construction control Inadequate inspection Inadequate testing

Table 7: Root causes of CCF events (operation)

Cause type	**Examples of specific cause**
Lack of procedures	Lack of repair procedures Lack of test or calibration procedures
Defective procedures	Defective repair procedures Defective test or calibration procedures
Failure to follow procedures	Failure to follow repair procedures Failure to follow test or calibration procedures
Supervision inadequacy	Inadequate supervisory procedures Inadequate action or supervisory communication
Communication problems	Communication among maintenance staff
Training inadequacy	Operator training in handling emergency situations

Table 8: Root causes of CCF events (environmental)

Cause type	Examples of specific cause
Stress	Chemical reactions (corrosion)
	Electrical failure
	Electromagnetic interference
	Materials interaction (erosion)
	Moisture
	Pressure
	Radiation
	Temperature
	Vibration
Energetic	Earthquake
	Fire
	Flood
	Impact loads

2.3 Common Cause Failure Modeling

There are two kinds of modeling for CCFs

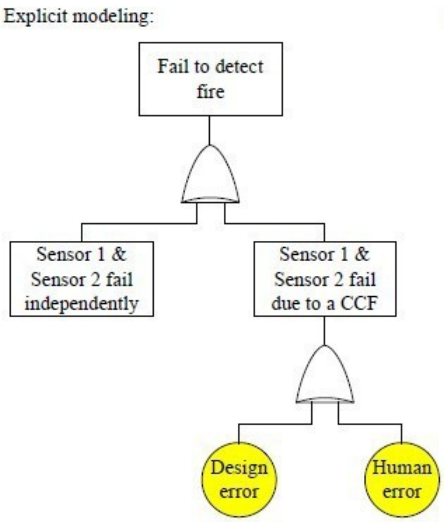
- Explicit Modeling
- Implicit Modeling

2.3.1 Explicit Modeling

When the specific causes of CCFs can be identified and the causes are dependent failures, it is better to model CCFs explicitly. The basic events in a fault tree model are considered as specific causes. Therefore, it is modeled explicitly. Examples of explicit causes are human error, utility failures or environmental events. One of the advantages of explicit modeling is that all the root causes of CCFs can be identified.

2.3.2 Implicit Modeling

When the causes of CCFs are difficult to be identified or cannot be identified, then the CCFs will be modeled implicitly. The limitation of the implicit modeling is that the causes of the failures cannot be identified clearly. The difference of explicit modeling and implicit modeling are shown in figure 8.


Explicit modeling:
Fail to detect fire
Sensor 1 & Sensor 2 fail independently
Sensor 1 & Sensor 2 fail due to a CCF
Design error
Human error

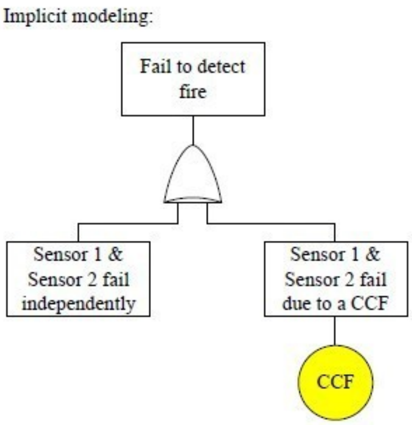

Implicit modeling:
Fail to detect fire
Sensor 1 & Sensor 2 fail independently
Sensor 1 & Sensor 2 fail due to a CCF
CCF

Figure 8: The difference between explicit modeling and implicit modeling (Wang, 2011)

All the following models belong to implicit models:

- The basic parameter (BP)model
- C-factor model
- The Multiple Greek Letter (MGL) Model
- The Multiple Beta-factor (MBF) Model
- The Binomial Failure Rate (BFR) Model
- The Alpha Factor (AF) model

For the above models, the CCFs can be modeled implicitly or explicitly, depending on whether the explicit causes can be identified or not. The above models are based on the β-factor model which is the most commonly used one because of its simplicity. Only one parameter is taken into consideration in β-factor model. Beta-factor is the most basic factor for CCFs. In the next section, β-factor model will be reviewed, and its advantages and disadvantages will be presented.

2.4 Beta-Factor Model

The β-factor model was proposed by Fleming in 1975. Nowadays, it is still a widely used CCF model because of the simplicity. It can be explained by a simple example.

If a system includes n identical components, and all the components have a constant failure rate λ, two kinds of failure rates are introduced :

λ_i is the independent failure rate, which will not cause other component's failure.

λc is the common cause failure rate, which denotes all the component's failure caused by a shared cause.

Therefore, the total failure rate for component is

$$\lambda = \lambda_i + \lambda c$$

For two components, the relationship of CCFs and independent failures is shown in Fig9.

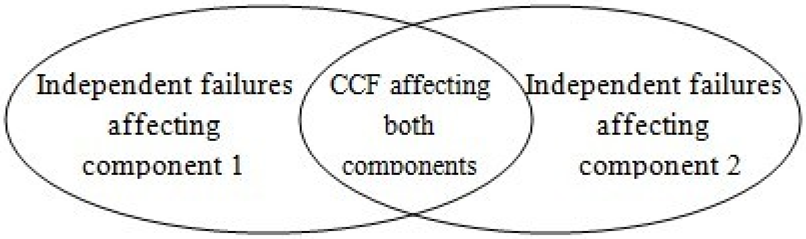

Independent failures affecting component 1
CCF affecting both components
Independent failures affecting component 2

Figure 9: Relationship between independent failure and CCF (Rausand and Høyland, 2004)

Beta-factor denotes the fraction of common cause failure among all failures of a component.

Beta-factor can be expressed by failure rate, then

$$\beta = \frac{\lambda_c}{\lambda}$$

$$\lambda_c = \beta\lambda$$

therefore,

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

If a component fails, β is the probability of CCF, and then the probability of independent failure is (1-β). The relationship between CCF and independent failure is expressed by β. The relationship for two components and three components is shown in Figure 10

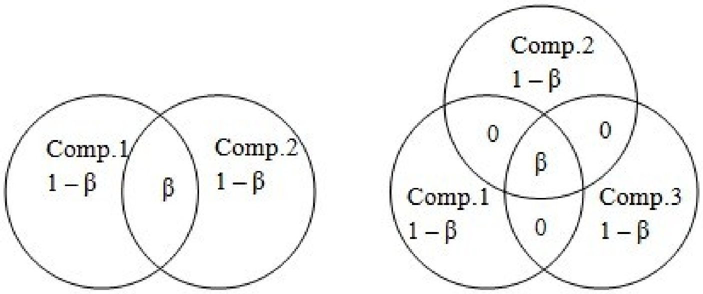


Figure 10: β-factor relationship between components

Beta-factor model can be considered as a shock model where shocks occur randomly according to a homogeneous Poisson process with rate λ_c. (Rausand, 2011) Every time the shock occurs, all the channels of the system fail regardless of the status of the channel.

Advantages of beta-factor model:

- It is simple.
- Only one parameter β need to be estimated when the data are available.
- It is easy and widely used. Some standards recommend this β-factor model to assess the reliability of SIS.
- Many models are developed based on β-factor model, such as C-factor model, multiple Beta-Factor model, Multiple Greek Letter model and so on.
- Many checklist methods are proposed to determine plant specific β-factor, such as IEC 61508-6 checklist and IEC 62061checklist.

Disadvantages of beta-factor model:

- It is simple for simple parallel systems, but it is not used for high redundancy systems.

- $\lambda_i = (1-\beta)\lambda$ and some database record historical total failure rate λ which are constant like OREDA; therefore, λ_i will be different when the plant specific β factor changes. Therefore, this equation: $\lambda_i = (1-\beta)\lambda$ is not right.

- It is not reward for different levels of redundancy.

- The traditional probability of the possible multiplicities of failure rates are (Rausand, 2011):

$$f_{1,n} = 1-\beta$$

$$f_{k,n} = 0$$

$$f_{n,n} = \beta$$

Therefore, for β-factor model, intermediate values of the multiplicity of the failure event are not possible when a failure occurs. It is either 1 or n.

- The β-factor is used for identical components with the same constant failure rate λ. It is difficult for nonidentical components to estimate β-factor. Sometimes, the following approach could be used to define β-factor by geometric average of the failure rate, but it is not commonly used.

$$\lambda_c = \beta * \left(\prod_{i=1}^{n} \right)^{1/n}$$

For now, it is impossible to avoid β-factor; therefore, determining and reducing β-factor is the priority to reduce CCFs. IEC 61508 is the basic standard for many kinds of industries, and it proposes a quantitative method which is a checklist to determine β-factor. Besides, systems can operate in two demand modes which are low-demand and high-demand mode. Therefore, in section 4, checklists used for low-demand and high-demand mode systems will be presented separately, and a comparison is made. Some industries require very high reliability for SIS, such as nuclear power industry. Hence, a method (UPM) which is used for high reliability system will be presented.

3 Determination of Beta-Factors for SIS

There are many models existing for modeling CCFs. The most simple model is β-factor model, because only one parameter is estimated. The β-factor maybe estimated by the use of the following methods(Lundteigen, 2010):

- Expert judgments
- Checklists
- Estimation models
- Using historical data

In this part, two IEC checklists and a estimation model will be introduced. The two checklists are IEC 61508-6 checklist and IEC 62061 checklist. The estimation model is unified partial model.

3.1 IEC 61508 Checklist

3.1.1 Introduction

For SISs, three parts are included: the sensors, the logic subsystem and the final elements. The β-factor for these three parts are different; therefore, β-factor should be calculated or estimated separately.

In this checklist, the following eight defenses are used. Furthermore, and 37 measures are developed for these eight defenses. For the complete checklist, see the standard IEC 61508-6 (2010), table D1.

- Separation/segregation
- Diversity/redundancy
- Complexity/design/application/maturity/experience
- Assessment/analysis and feedback of data

- Procedures/human interface
- Competence/training/safety culture
- Environmental control
- Environmental testing

This is a comprehensive checklist, 37 questions need to be answered based on the engineering judgment. The questions will be evaluated in the next section.

In the checklist method, the influence of extensive diagnostic tests is taken into consideration for β-factor estimation. The overall CCF rate is divided into dangerous detected (DD) failure rate and dangerous undetected (DU) failure rate. DU failures cannot not be influenced by diagnostic tests. Therefore, the overall β is equal to β_{DU}. Non-simultaneous CCFs may be detected by diagnostic test, so CCF rate can be reduced. Then, the overall β can be reduced. The overall failure rate is given by

$$\lambda_D\beta = \lambda_{DU}\beta + \lambda_{DD}\beta_D$$

where

- λ_D is the dangerous failure rate of a single unit.
- β is the overall common cause failure factor which is also undetected failure factor, without take diagnostic test into consideration.
- λ_{DU} is the dangerous undetected failure rate of a single unit.
- λ_{DD} is the dangerous detected failure rate of a single unit.
- β_D is the CCF factor for dangerous detected failures which is taken diagnostic test into consideration.

Two sets of values X and Y are used to estimate β-factor. X means that the diagnostic test improves the effectiveness of the items. While Y means that there is no influence from diagnostic test. For each question or measure in the table, if the answer is a yes, then the corresponding scores of the X and Y are obtained. And the ratio of X and Y represents the extent to which the measure's contribution against CCFs can be improved by diagnostic test (IEC 61508, 2010).

In the table,

- X_{LS} means the improved question value by diagnostic test for logic solver.
- Y_{LS} means the value that is not influence by diagnostic test for logic solver.
- X_{SF} means the improved defense value by diagnostic test for sensors or final elements.
- Y_{SF} means the value that is not influence by diagnostic test for sensors or final elements.

All the measures or the questions should be estimated and then the value for the elements can be found. After that, sums the columns X_{LS}, Y_{LS}, X_{SF}, Y_{SF} are calculated respectively. The value Z can be yield using the Table 9 for logic subsystem and Table 10 for sensors and final elements. Factor Z stands for diagnostic test which is determined by the factor diagnostic coverage and diagnostic test interval.

Then, S can be calculated by using the following equations:

$$S = \sum X_i + \sum Y_i$$

which is to obtain the β_{int} value for undetected failures, and

$$S_D = \sum X_i(Z+1) + \sum Y_i$$

which is used to get the value of β_{Dint} for detected failures.

Table 9: Value of Z for programmable electronics (IEC 61508, 2010)

Diagnostic coverage	**Diagnostic test interval**		
	< 1 min	Between 1 min and 5 min	> 5 min
$\geq$ 99%	2.0	1.0	0
$\geq$ 90%	1.5	0.5	0
$\geq$ 60%	1.0	0	0

Table 10: Value of Z for sensors and final elements (IEC 61508, 2010)

Diagnostic coverage	**Diagnostic test interval**			
	< 2 h	Between 2 h and two days	Between two days and one week	> one week
$\geq$ 99%	2.0	1.5	1.0	0
$\geq$ 90%	1.5	1.0	0.5	0
$\geq$ 60%	1.0	0.5	0	0

Based on the values of S_D and S, β_{int} or β_{Dint} for 1oo2 system can be obtained using Table 11.

In this method, the range of β-factor value is from 0.5% to 5% for logic solvers; and from 1% to 10% for final elements or sensors.

Table 11: Calculation of β_{int} or β_{Dint}(IEC 61508, 2010)

Score (S or S_D)	**Corresponding value of β_{int} or β_{Dint} for the:**	
	Logic Subsystem	**Sensor or final elements**
120 or above	0.5%	1%
70 to 120	1%	2%
45 to 70	2%	5%
Less than 45	5%	10%
NOTE 1 The maximum levels of β_{Dint} shown in this table are lower than would normally be used, reflecting the use of the techniques specified elsewhere in this standard for the reduction in the probability of systematic failures as a whole, and of common cause failures as a result of this. NOTE 2 Values of β_{Dint} int lower than 0,5 % for the logic subsystem and 1 % for the sensors would be difficult to justify.		

The β-factor obtained from the above table is for 1oo2 system. The β-factor is different for the different level of redundancy, which can obtained from the Table 12 for some other redundant systems.

Table 12: Calculation of β for systems with levels of redundancy greater than 1oo2 (IEC 61508, 2010)

MooN		N			
		2	3	4	5
M	1	β_{int}	*0.5* β_{int}	*0.3* β_{int}	0.2 β_{int}
	2	–	1.5 β_{int}	0.6 β_{int}	0.4 β_{int}
	3	–	–	1.75 β_{int}	0.8 β_{int}
	4	–	–	–	2 β_{int}

3.1.2 Questions Evaluation

IEC 61508 checklist is used for determining β-factor to estimate the influence of CCFs for SIS. Thirty seven measures are included for minimizing the probability of occurrence of CCFs. Because it is performed by design engineers in the design phase; and it includes some questions about the maintenance and operation procedure, assumptions about the maintenance activities or operation procedures are made to estimate β-factor. Most of the questions are easy to read from the design drawing. However, although the design drawing is very detailed, some questions are still difficult to tell from the design drawing.

Before installation of SIS, the fifth phase of the safety lifecycle is overall safety requirements allocation (safety function (SIL) allocation). In this phase, the purpose of reliability calculation is to get SIL of SIS. Before performing calculation of PFD, IEC 61508 checklist should be performed to determine β-factor to take CCFs into consideration. Also, in this phase, the compliance report should be prepared.

IEC 61508 checklist includes thirty-seven questions in eight groups, the questions will be evaluated one by one in the following.

Separation/segregation For separation/segregation, this is about the design of the system. If the engineers understand the design very well, there will be easy to evaluate and get the correct scores.

- Q1: Are all signal cables for the channels routed separately at all positions?

It may take sometime for engineers to check the architecture of signal cables. This is a good question for determining β-factor because if all signal cables do not routed separately, then CCFs will be caused by a shock or an accident easily. It is safer to locate signal cables separately to reduce the probability of CCFs.

- Q2: Are the logic subsystem channels on separate printed-circuit boards?

If the logic subsystem channels are on separate printed-circuit boards, the probability of occurring CCFs will be reduced when there is a physical damage on one printed-circuit board, such as humidity, pressure, shock and so on. Although it is not the same thing with Q1, it is not necessary to list Q1, Q2 separately.

- Q3: Are the logic subsystems physically separated in an effective manner? For example, in separate cabinets.

For this question, the engineers need to get familiar with the design principle and the function of the design. Effective manner means logic subsystems physically separated and they are independent with each other. If the logic subsystems are physically separated in an effective manner, the cascading failure do not exist. Therefore, there is no CCFs caused by cascading failure. The overall probability of CCFs will be reduced.

- Q4: If the sensors/final elements have dedicated control electronics, is the electronics for each channel on separate printed-circuit boards?

When the electronics for each channel on separate printed-circuit boards, the probability of the failures caused by a common reason is very low unless it is design or technical defect.

- Q5: If the sensors/final elements have dedicated control electronics, is the electronics for each channel indoors and in separate cabinets?

This question is familiar with the above question. If the electronics for each channel indoors, the probability of CCFs caused by whether such as raining or lightening is very low. And if the electronics located in separate cabinets, some kinds of CCFs could be avoided or the probability will be very low, like physical damage and human errors. This question cannot be answered based on the design drawing. Also, since the system has not been installed, whether the electronics for each channel indoors or not cannot be told from the design drawing. To answer this question, some assumptions should be made.

In "separation/segregation" part, it is mainly about physical separation of the cables or elements. The location of the elements is very important, because locating in different places reduce the probability of CCFs efficiently due to accidents, damages or human errors.

Diversity/redundancy

- Q6: Do the channels employ different electrical technologies; for example, one electronic or programmable electronic and the other relay?

If the answer of this question is a "yes", then the probability of CCFs caused by technology defects or design error will be reduced. It is not difficult to read it from the design drawing.

- Q7: Do the channels employ different electronic technologies; for example, one electronic, the other programmable electronic?

This question is similar with the above question. If the channels employ different electronic technologies, the probability of CCFs, due to technology defects, will be much lower than using the same technology. It can be merged with Q6. The question should be "Do the channels employ different technologies?" As long as the technologies are different, the CCFs caused by technology defect can be avoid.

- Q8: Do the devices employ different physical principles for the sensing elements; for example, pressure and temperature, vane anemometer and Doppler transducer, etc?

This question can be answered by reviewing the design drawing if it is in detail. If physical principles are different, then the probability of CCFs caused by a shared cause like pressure or temperature can be reduced.

- Q9: Do the devices employ different electrical principles/designs for example, digital and analogue, different manufacturer (not re-badged) or different technology?

When the devices employ different electrical principles or designs, the system will not fail because of the manufacturer's error or technical/design deficiency. Therefore, different electrical principles reduce the probability of CCFs which caused by technology or design defect.

- Q10: Is low diversity used, for example hardware diagnostic tests using the same technology?

Diversity means different means of performing a required function. (IEC 61508, 2010)

If the system use the low diversity, the probability of CCFs will be higher than high diversity due to technical defects.

- Q11: Is medium diversity used, for example hardware diagnostic tests using different technology?

About the medium diversity, using different technology will not easily cause CCFs due to a specific technology's fault. In my opinion, this question could be merged with Q10 because it is about the level of diversity. The best way to mention diversity is that *what is the level of diversity used?*. Then based on the expert judgment to get the score from 0-10. For example, after the analysis of the system, the expert assesses the level of the diversity. The higher the diversity, the higher the score can be obtained.

- Q12: Were the channels designed by different designers with no communication between them during the design activities?

For this question, regarding to CCFs, when the channels designed by different designers with no communication, then the probability of the CCFs caused by the same design defects is extremely low or there is no CCFs. Besides, the anti-pressure or humidity of the channels will also be different, which reduces the probability of CCFs caused by environment factor or external pressure efficiently.

- Q13: Are separate test methods and people used for each channel during commissioning?

To answer this question, it is based on the assumptions made in design phase because the system has not installed. Also, relevant documents should be reviewed, which is another time-consuming work. To consider CCFs, if the same test methods and people are used, and the method is not perfect for that channel or the people have the same habits, CCFs are easily introduced.

- Q14: Is maintenance on each channel carried out by different people at different times?

This is also based on the assumptions in design phase. This question is about human factor. The purpose of this question is that different people and different time perform maintenance to make sure CCFs are not caused by human mistake or same technology error.

Complexity/design/application/maturity/experience

- Q15: Does cross-connection between channels preclude the exchange of any information other than that used for diagnostic testing or voting purposes?

This question should be answered by on the real scenario.

- Q16: Is the design based on techniques used in equipment that has been used successfully in the field for > 5 years?

If the design based on techniques used in equipment successfully more than 5 years, the record of safety is good. Hence the probability of CCFs will be very low.

- Q17: Is there more than 5 years experience with the same hardware used in similar environments?

This is a similar question with the above one. If the same hardware is used for more than 5 years in similar environments, the technology is mature and the probability of CCFs caused by technology defects will be extremely low.

- Q18: Is the system simple, for example no more than 10 inputs or outputs per channel?

There is no definite relation between the simplicity of the system and CCFs, but compared with the different technologies being used, the probability of CCFs caused by the complexity of the system is much lower.

- Q19: Are inputs and outputs protected from potential levels of over-voltage and over-current?

For this question, it is just necessary to check the design map. If inputs and outputs protection exist, the probability of occurrence of CCFs caused by over-voltage or over-current is very low.

- Q20: Are all devices/components conservatively rated (for example, by a factor of 2 or more)?

This is a ambiguous question for engineers to answer, which is even more difficult for design engineers. If the answer is a “yes”, it means all devices/components rated in a safer way. The score will be get. The overall score will be higher, and hence the value of β-factor will be lower.

Assessment/analysis and feedback of data

- Q21: Have the results of the failure modes and effects analysis or fault-tree analysis been examined to establish sources of common cause failure and have predetermined sources of common cause failure been eliminated by design?

About this question, the engineers should review all the failure records and check if the sources of CCFs have been eliminated after performing failure modes and effects analysis or fault-tree analysis. If sources of CCFs have been eliminated, the probability of CCFs will be reduced sharply.

- Q22: Were common cause failures considered in design reviews with the results fed back into the design? (Documentary evidence of the design review activity is required.)

For this question, it is necessary to review the records of the design document to check if the CCFs are considered. If CCFs are considered, the probability of CCF being analyzed from risk analysis will be much lower. However, this question could be merged into Q21, because it is all about common cause failures considered in design phase, which fed back into design.

- Q23: Are all field failures fully analyzed with feedback into the design? (Documentary evidence of the procedure is required.)

To answer this question, engineers need to review all the failure documents to check whether the results of failure analysis are used for design. However, one problem is that the failures are classified when performing risk analysis. If some failures are not classified, it will be difficult to answer the above question.

To get the answer of this part, it takes engineers a lot of time to review the documents and records. Moreover, the engineers should be familiar with the system.

Procedures/human interface

- Q24: Is there a written system of work to ensure that all component failures (or degradations) are detected, the root causes established and other similar items inspected for similar potential causes of failure?

This is also a complicated work to do. Many kinds of documents need to be reviewed. However, if the written system of the work exists, measures will be developed to reduce the probability of CCFs and other kinds of failures.

- Q25: Are procedures in place to ensure that: maintenance (including adjustment or calibration) of any part of the independent channels is staggered, and, in addition to the manual checks carried out following maintenance, the diagnostic tests are allowed to run satisfactorily between the completion of maintenance on one channel and the start of maintenance on another?

Because the question is answered in design phase, the procedures for maintenance activities cannot be read from the design drawing. It is also based on the assumptions made in design phase.

- Q26: Do the documented maintenance procedures specify that all parts of redundant systems (for example, cables, etc.) intended to be independent of each other, are not to be relocated?

If all parts of redundant systems are independent to each other, there is no cascading failures. Therefore, the probability of CCFs caused by other component failure is low. Under this condition, the probability of occurring CCFs is much lower than the condition of dependent components.

- Q27: Is all maintenance of printed-circuit boards, etc. carried out off-site at a qualified repair center and have all the repaired items gone through a full pre-installation testing?

If all repaired items gone through a full pre-installation testing, not functioning spare parts can be avoided. Therefore, the probability of CCFs caused by the new items can be reduced.

- Q28: Does the system have low diagnostic coverage (60 % to 90 %) and report failures to the level of a field-replaceable module?
- Q29: Does the system have medium diagnostics coverage (90 % to 99 %) and report failures to the level of a field-replaceable module?
- Q30: Does the system have high diagnostics coverage (>99 %) and report failures to the level of a field-replaceable module?

Question 28 to 30 are about the diagnostic coverage. The higher the diagnostics coverage is, the more the failures are detected and avoided. Therefore, the less CCFs arise. These three questions are not necessary to be listed one by one, and can be merged into one question and three levels of score.

- Q31: Do the system diagnostic tests report failures to the level of a field-replaceable module?

For low-demand systems, this is a very important aspect to check. The system is doing diagnostic test all the time. If the failure of a component is revealed when the function of this component is not on demand, and the failure is reported to the level of a field-replaceable module, the component could be replaced, and CCFs caused by this component is avoided. However, the CCFs, under this condition, cannot be avoided because the failure occurs when the function of the component is on demand. Also, if the system diagnostic tests report failures to the level of a field-replaceable module, the probability of occurring CCFs will be low. If the system diagnositc tests do not report failures, the probability of CCFs will increase.

Competence/training/safety culture

- Q32: Have designers been trained (with training documentation) to understand the causes and consequences of common cause failures?

It is a company's culture. If the designers have been trained, they will understand the causes of CCFs, so pay attention to it and avoid it. Then, the probability of occurring CCFs could be reduced.

- Q33: Have maintainers been trained (with training documentation) to understand the causes and consequences of common cause failures?

This is a similar question with Q32. If maintainers have been trained, causes will be easily found out, maintained and checked, so the probability of CCFs will be very low.

Environmental control

- Q34: Is personnel access limited (for example locked cabinets, inaccessible position)?

It is in the design phase to perform this checklist, the system has not installed, so there is no way to check it. To answer this question, it has to be based on the assumptions made in design phase. If the access is not limited, then non-professional staff or irrelevant staff may enter into this area and lead to CCFs.

- Q35: Is the system likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc., over which it has been tested, without the use of external environmental control?

If the system is likely to operate within the range of temperature, humidity, corrosion, dust, vibration, etc., over which it has been tested, then the probability of CCFs caused by temperature, humidity, corrosion, dust, vibration, etc will be reduced.

- Q36: Are all signal and power cables separate at all positions?

This is a time consuming question. Engineers should take much time to check and find out the result. However, if all signal and power cables separate at all positions, CCFs caused by a shock or external stress will not happen.

Environmental testing

- Q37: Has the system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognized standards?

To answer this question, what the engineers need to do is to review the documents to check if the system has been tested under all relevant environmental condition. To check the environmental control questions, environmental testing should be done first.

3.1.3 Discussions

After the evaluation of this checklist, I think the measures related to human error/factor are not enough. More questions about human factor should be developed and should be a big part of this checklist because human factor influences the CCFs significantly. For example, over-time working distract engineers, thus leading to shutdown of the system. Also, different people may treat problems differently. Besides, questions included in one factor are similar. It makes the questions repetitive. Therefore, I think this checklist is not perfect, and I will propose a question list in subsection 4.1.5.

3.1.4 Advantages and Disadvantages

The checklist is performed by a group of integrity engineers who cooperate with the other engineers in a company. It is mainly used in process industry. It is used to determine plant specific β-factor of CCFs. It is widely used for low-demand system.

The advantages of the IEC 61508-6 checklist are listed below:

- The specific β-factor value can be obtained.

- Many kinds of factors are considered.

- The influence of diagnostic test is considered.

- 37 measures are proposed to reduce the probability of common cause failure.

Although the advantages of IEC 61508-6 checklist, some disadvantages of this checklist cannot be ignored.

The disadvantages of IEC 61508-6 checklist are

- Some questions are difficult to answer because they are based on practice.

- It takes much time to review all the relevant documents.

- Human factors questions are not considered enough.

- It requires design engineers or specific engineers to perform this checklist.

3.1.5 Proposed Checklist

I think some of the questions are not necessary because some of them are similar and can be merged. Also, in my opinion, the scoring system of this checklist is not perfect because there is no definite answer for some questions. The answer “yes” or “no” cannot describe the condition of the system. In addition, because there is no available database to support this checklist and the procedure of calculation, I propose that the score of each value should have a range from one to ten. For example, if the system uses very high diversity, the score could be nine or ten. If the system uses low diversity, the score could be 2 or 3 based on the expert judgment. In my proposed checklist, the same eight factors are taken into account.

Separation/segregation

What degree of the overall physical separation of the systems (including signal cables, main elements of the system) are used?

Diversity/redundancy

What degree the diversity the systems are used?

What degree the test methods (different test methods are used for each channel) are used?

What degree the technologies the system are used?

Complexity/design/application/maturity/experience

What degree the maturity of the design technology is?

Is the design has been used in a similar environment for more than 5 years successfully (experience)?

What degree of the inputs and the outputs are protected (like over-voltage, over-current protection)?

Assessment/analysis and feedback of data

What degree of the failures data (obtained from risk analysis in design phase like FMECA) feed back into design and be used to eliminate the sources of CCFs?

Procedure/human interface

What the degree of the training to understand CCFs (only trained before work once, or regular training every week, or a written procedure that tell staff how to treat and recognize CCFs) is?

What degree the failures revealed by the diagnostic coverage being reported to the level of a field-replaceable module?

How people trained about how to deal with different failures?

Environmental control

What extent the access limited is? (only relevant engineer, or all staff, or inaccessible?)

Environmental control

Is the system has been tested in all relevant environmental condition (like temperature, humidity, vibration, shock, corrosion, dust etc.) and meet the standard requirement?

The reason why above questions are listed is that these questions cover all eight factors. The checklist I propose is much simpler than the one from IEC 61508, but it covers most aspects of the eight factors. Take the separation factor as an example, it is about physical separation, so one question about the degree of the separation of the system is enough. Based on the expert judgment of the system, the corresponding score is obtained. If the elements or cables separate very well, the score is 10. If there is almost no separation of the cables or elements, then the score could be 0. This checklist should be performed by the professional engineers with experience.

3.2 IEC 62061 Checklist

3.2.1 Introduction

Standard IEC 62061 is *Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems.* Be similar to IEC 61508-6 checklist, IEC 62061also determines β-factor by expert judgment, answering a list of questions. Besides, this is a qualitative based method. The difference from IEC 61508 is that IEC 62061 checklist is used for machinery field which is for high demand operation mode.

IEC 62061 checklist is less complicate than IEC 61508-6 checklist. Only 14 items are included in this checklist. The measures are shown in Table 13:

Table 13: IEC 62061 checklist of determine CCF (IEC 62061, 2005)

Item	**Reference**	**Score**
Separation/segregation		
Are SRECS signal cables for the individual channels routed separately from other channels at all positions or sufficiently shielded?	1a	5
Where information encoding/decoding is used, is it sufficient for the detection of signal transmission errors?	1b	10
Are SRECS signal and electrical energy power cables separate at all positions or sufficiently shielded?	2	5
If subsystem elements can contribute to a CCF, are they provided as physically separate devices in their local enclosures?	3	5
Diversity/redundancy		
Does the subsystem employ different electrical technologies, for example, one electronic or programmable electronic and the other an electromechanical relay?	4	8
Does the subsystem employ elements that use different physical principles(e.g. sensing elements at a guard door that use mechanical and magnetic sensing techniques)?	5	10
Does the subsystem employ elements with temporal differences in functional operation and/or failure modes?	6	10
Do the subsystem elements have a diagnostic test interval of $\leq$1 min?	7	10
Complexity/design/application		
Is cross-connection between channels of the subsystem prevented with the exception of that used for diagnostic testing purposes?	8	2

Item	**Reference**	**Score**
Assessment/analysis		
Have the results of the failure modes and effects analysis been examined to establish sources of common cause failure and have predetermined sources of common cause failure been eliminated by design?	9	9
Are field failures analyzed with feedback into the design?	10	9
Competence/training		
Do subsystem designers understand the causes and consequences of common cause failures?	11	4
Environmental control		
Are the subsystem elements likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc. over which it has been tested, without the use of external environmental control?	12	9
Is the subsystem immune to adverse influences from electromagnetic interference up to and including the limits specified in Annex E?	13	9
NOTE: An alternative item (e.g. references 1a and 1b) is given in Table F.1		
where it is intended that a claim can be made for a contribution towards		
avoidance of CCF from only the most relevant item.		

Compared with IEC 61508-6 checklist, IEC 62061 evaluates six defenses instead of eight which are:

- Separation/segregation
- Diversity/redundancy
- Complexity/design/application
- Assessment/analysis
- Competence/training
- Environmental control

Also, the scoring system is used. If the answer of the question is a “Yes”, the corresponding score can get. After answering all the questions in figure, it is easy to sum up the scores. Finally, use the overall score to find the corresponding β-factor value by table 14.

Table 14: Estimation of CCF (β-factor) (IEC 62061, 2005)

Overall score	**Common cause failure factor (β)**
< 35	10% (0.1)
35-66	5% (0.05)
65-85	2% (0.02)
85-100	1% (0.01)

If the total score is 70 based on the checklist, then the β-factor is 2% based on the above table.

Compared with IEC 61508-6 checklist, this one is much easier and simpler.

3.2.2 Discussions

This checklist method is a very simple qualitative based approach to estimate CCF (β-factor). It used for machinery industry which is a high-demand operation system. Compared with the IEC 61508-6 checklist, one of the advantages of this is that it is much simpler and only 14 questions to check. However, to perform this checklist, the engineers should be professional design engineers. Besides, a lot of documents need to be reviewed, which takes much time.

3.3 Comparison of IEC 61508 and IEC 62061 Checklists

3.3.1 Similarity of Two Checklists

Both checklists are used to determine plant specific β-factor of common cause failures for SIS. These two IEC checklists provide series of measures to defense against CCFs, which is evaluated by expert estimation. Both checklist methods use scoring system and are used for design phase.

3.3.2 Main Differences Between Two Checklists

IEC 61508-6 is a method for quantifying the effect of CCFs, while IEC 62061 is a qualitative based approach to estimate common cause failures. Generally, IEC 61508 checklist method is used for low-demand operation system, and IEC 62061 checklist is used for high-demand operation system. IEC 61508 includes eight defenses with 37 measures, while IEC 62061 contain six defenses with 14 measures. Two conditions are included in IEC 61508 method: one is take diagnostic test into consideration, and the other one is diagnostic test is not taken into account, while IEC 62061 checklist only considers the condition that includes diagnostic test. The basic differences between IEC 61508 and IEC 62061 checklist is shown in Table 15.

Table 15: Differences of IEC checklists

IEC 61508-6 Checklist	**IEC 62061 Checklist**
Mainly used for process industry	For machinery industry
Performed by integrity engineers cooperate with company	Performed by design engineers
Two conditions: diagnostic test; and no diagnostic test	Only diagnostic test condition
Evaluate logic subsystem & sensor/final elements separately	All together
Design phase (assumptions in operational phase)	Design phase
Only for hardware-related CCF	Overall CCF
Consider maintenance activities	Only design activities
Procedure of calculation	Different procedure
Used for low-demand system	For high-demand system
Include 8 factors	6 factors
37 measures	14 measures

3.3.3 Comparison of Measures

Because these two checklists have similar defenses, the defenses will be discussed and compared one by one in this section.

Separation/segregation Both checklists contain the factor separation, and because IEC 61508 treats logic subsystems and sensors/final elements differently, the measures are differently listed. Therefore, the questions of two checklists developed on separation are very alike. It is about the physical separation and signal cables separation. The only difference about separation is that IEC 61508 has different items for logic subsystem and sensors/final elements.

Diversity/redundancy IEC 61508 and IEC 62061 have two similar questions. Because IEC 61508 takes diagnostic test into consideration, it includes more questions for diagnostic tests. Besides, IEC 61508 is also used for operation phase, and more questions about maintenance and procedure problems included. The IEC 62061 only have one question about diagnostic test interval, and it is *Do the subsystem elements have a diagnostic test interval of* $\leq$ *1 min?*

Complexity/design/application The title about this sub-factor is for IEC 62061. This factor for IEC 61508 is complexity/design/application/maturity/experience. IEC 61508 is used for low-demand operation system. And if the experience is not enough or the technology is immature, it may cause failures very often or influence the operation of the system; therefore, it is very important for IEC 61508 checklist. Also the frequency of low-demand is less than one time per year. The maturity of the technology maybe need more than five years for low-demand system. While for high-demand system, if the technology or the experience is used more than 1 year, then the technology is mature; therefore the maturity of technology is not so meaningful for high-demand system (IEC 62061) as long as it experiences the experiment and it has been put in use for one year. In addition, one question for IEC 61508 is that *Is the system simple, for example no more than 10 inputs or outputs per channel?*, which is not so relevant with common cause failure, so it could be ignored.

Assessment/analysis and feedback of data The title of this sub-factor is for IEC 61508, while there is no feedback of data for IEC 62061. Three questions for

IEC 61508 and two for IEC 62061. The two questions in IEC 62061 are almost the same with two of them in IEC 61508. IEC 61508 has one question more than IEC 62061 which is *Were common cause failures considered in design reviews with the results fed back into the design?* As discussed in questions evaluation, this one could be emerged to the first question of this factor.

Procedures/human interface This title is for IEC 61508, while this factor does not not exist in IEC 62061 because IEC 62061 is only used for facilitating design. Therefore, this sub-factor is not suitable for IEC 62061 checklist.

Competence/training/safety culture This title is for IEC 61508 while IEC 62061 does not include safety culture. There are two questions for this defense in IEC 61508, one is for design engineer, and one is for maintenance engineer. IEC 62061 contains only one question for design engineer which is the same question with IEC 61508. Because IEC 62061 is only for design phase, maintenance activities or training should not be included in this factor.

Environmental control Both checklists have the same factor of this. They have a same question about the subsystem likely to operate within the range of temperature, humidity, corrosion, dust, vibration, etc. Because IEC 61508 is for low-demand system, it also includes personnel access limitation. Also the question in IEC 61508 *Are all signals and power cables separate at all positions?* should be included in factor separation.

Environmental test This factor is included in IEC 61508, not included in IEC 62061.

According to the measures comparison in subsection 4.3.3 and Table 15, if IEC 61508 is used in high-demand system, the questions under the assumptions of operational phase will not be considered. Besides, only hardware-related CCF considered and it ignores other kinds of CCFs. In addition, 23 questions will be ignored in high-demand system. Hence, the value of β-factor obtained from IEC

61508 checklist cannot be the same when the checklist is used for low-demand and high-demand systems.

4 Unified Partial Method

The unified partial method (UPM) was proposed by Brand (1996) and further developed by Zitrou and Bedford in 2003 (Rausand, 2011). It is CCF quantification through improving Partial Beta Factor method (PBF) for component level analysis. And it uses cut-off method structure for system level analysis. UPM is the standard approach for UK nuclear industry determining β-factor. It is popular and widely used in high reliability industry. The reason is popular that it can be used when available data are limited.

PBF method contains 19 factors influence β-factor, while UPM method combines these 19 factors into the following eight underlying factors, which can cover the all the aspects that effect the probability of common cause failure of the system. These 19 sub-factors are belong to three areas, see Table 16.

Table 16: UPM sub-factors (Wang, L.Y., 2011)

Factor	Sub-factor
Design	Redundancy and diversity (s_1)
	Separation (s_2)
	Understanding (s_3)
	Analysis (s_4)
Operation	Operator interaction(s_5)
	Safety culture(s_6)
Environment	Environmental control (s_7)
	Environmental tests(s_8)

The above eight factors show the probability of all aspects that effect the common cause failures of the system equipment. Each factor has five attributes (A to E) and each attribute has a corresponding weight and score. Analyzing these eight factors is to combine the design of the system and the experienced data provided by UPM to make the analysis process much more practicable.

Brand (1996) provides a application guide to use unified partial method. It is shown in Figure 11

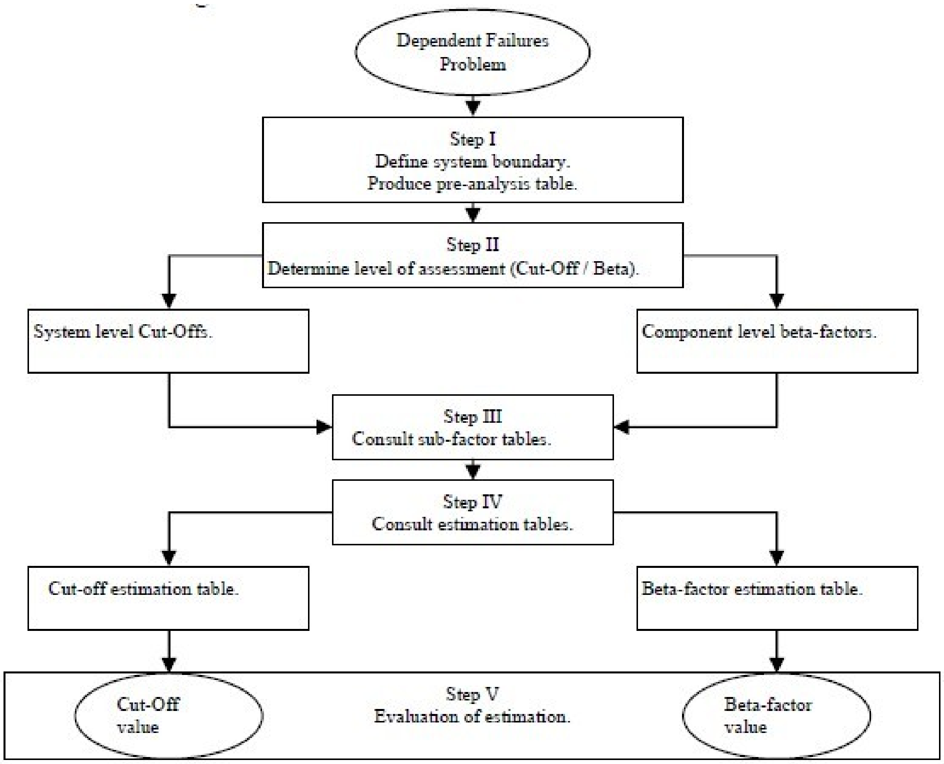

Dependent Failures Problem
Step I
Define system boundary.
Produce pre-analysis table.
Step II
Determine level of assessment (Cut-Off / Beta).
System level Cut-Offs.
Component level beta-factors.
Step III
Consult sub-factor tables.
Step IV
Consult estimation tables.
Cut-off estimation table.
Beta-factor estimation table.
Step V
Evaluation of estimation.
Cut-Off value
Beta-factor value

Figure 11: UPM application guide (Brand, 1996)

To perform UPM, the first step is to define the physical boundary of the system. And a pre-analysis table is produced for assessment. The second step is to choose which method should be used. If it is a system assessments, the Cut-off method is selected. And Partial Beta Factor method should be selected for component level assessment. The third step is to assess the sub-factors which are the defenses against failures. There are eight sub-factors and each factor have five criteria to assess the quality of the defense. About the criteria for sub-factors and how to assess it will be described in next section. Based on the expert judgment, the corresponding scores are obtained by Table 17.

Table 17: UPM determination of β-factor (Tim, 2011)

Common Cause Factors	**A**	**A+**	**B**	**B+**	**C**	**D**	**E**
Design							
Redundancy & diversity	1750	875	425	213	100	25	6
Separation	2400		580		140	35	8
Understanding	1750		425		100	25	6
Analysis	1750		425		100	25	6
Operation							
Man, Machine, Interface	3000		720		175	40	10
Safety culture	1500		360		90	20	5
Environment							
Control	1750		425		100	25	6
Tests	1200		290		70	15	4

The final step of the guide is to calculate Cut-Off factor $\hat{Q}$ or beta factor $\hat{\beta}$ based on the values obtained from the above table. To calculate $\hat{\beta}$ use the following equation:

$$\hat{\beta}=\frac{s_1(x_1)+s_2(x_2)+\ldots s_8(x_8)}{d}$$

where d is a constant number which is 50000. The ranges of the obtained estimates is $10^{-2} \leq$ Q $\leq 10^{-6}$ when the cut-off method is chose. The ranges of the estimation of β-factor is $0.302 \leq \beta \leq 0.00102$ when the partial β-factor method is required. (Athena, 1996)

4.1 Description of the Defenses

4.1.1 Environment Control

This factor is to control the people who can access the working field of common unit equipment. Attribute A is that other machines and process exist, which are irrelevant functioning. Attribute B is to separate the workshop and limit the access, and the risk of machinery damage is low. Only authorized people have access to this area, and all the activities is relevant, so the attribute is C. Attribute D is under the strict surveillance, and only trained persons can access the limited area. All the equipment and service depend on the designed control. Attribute E means much more narrow activity scope, like the cockpit of the plane or the other control room.

4.1.2 Environment Test

The environment test is about the condition of the environment test of the common equipment. Attribute A is that there is no environment test except the standard environment test provided by manufacture. The environment test is the condition that uses the sample device and requires the operation staff, which is the attribute B. Attribute C is to perform a detailed experiment on sample device to make sure the device can survive under all kinds of condition, like humidity, temperature, vibration and so on. Attribute D is to perform the experiment to use the device, operate and test in a reasonable period of time. Attribute E is to work with the existing equipment for a period of time before put it in use.

4.1.3 Analysis

This factor reflects the analyzed system. Normally, it is the feedback of whether the staff have the experience of failure analysis. It also reflects whether the design engineers have the full understanding of the common cause failure and the measurements. If there is no formal safety assessment and no design experiment of the relevant common cause failure, the attribute is A. If higher level research is performed, like FMEA, or the design engineers have the full understanding of the relevant failure problem, the attribute is considered as B. When the attribute is C, then reliability assessment and feedback should exist, and the engineers have the specific knowledge of the relevant failures. Attribute D is very similar with attribute C. At the same time, having the management supports for the feedback of the design or working evaluation. Having the reliability assessment and the management support for the feedback of the design or working evaluation. Meanwhile, the designers have the knowledge of the relevant failures.

4.1.4 Safety Culture

This factor reflects the training of the staff and the condition of the safety culture of the company. If the company performs on-the-job training, then the attribute is A. If the company provides systematic and regular training, including normal and emergency operational training, it belongs to attribute B. If the company provides the simulator training for normal operation, or dedicated staff are able to demonstrate that the safety culture is good including systematic training , the attribute is C. In addition to C, it belongs to attribute D if the company provides the simulator training for normal operation, or dedicated staff are able to demonstrate that the safety culture is good including systematic emergency operation training. When the simulator training for normal and the emergency operation are provided, and the company have the clear safety policy or culture, the attribute can be considered as E.

4.1.5 Separation

To assess this factor, it should be based on the layout of the design and the working place for the common cause equipment. The unified partial method treats electric equipment and machinery equipment differently. It also can be divided into 5 categories. For electric equipment, if the common cause components locate in the same cabinet, the attribute of separation should be the first category. If the common cause components locate in the same cabinet, but they are separated by a barrier, it is the second category. When the common cause components locate in the different cabinet, the category is the third one. However, when the common cause components locate in the different cabinet, and there is distance between cabinets, it is the forth category. If the common cause components locate in the different room, it is the last category.

For machinery equipment, if the common cause components locate in the same room, it belongs to category one. When the common cause components locate in the same room, but there is a physical separation between the devices, it is the second category. If the common cause components device locate in adjoining room, it is class three. When the common cause components device not locate in the adjoining room, it is the forth category. If the common cause components device locate in the different workshop, then it is the last category for machinery equipment.

4.1.6 Redundancy and Diversity

This factor reflects the redundancy and the functioning, and it also reflects the diversity of the operation. It divided into seven attributes. Attribute A means the minimum redundancy, for example 1 out of 2, 2oo3, or 3oo4 systems. The attribute A+ means the enhanced redundancy which is the 1oo3, 2oo4 systems and so on. Attribute B is for correspond to the extreme strong redundancy, such as 1oo4, 1oo5, or 2oo5 system. Attribute B+ means the high redundancy for the same components, for example 1 out of 8 system. Attribute C means the same components have the enhanced redundancy and the diversity for functioning; C also means the same components having the extreme high redundancy and the operation diversity. Besides, the same components have high redundancy in the passive system. Attribute is D when the corresponding same components have extremely high redundancy like 1oo4 architecture, and the functioning are diversity. Attribute E corresponding two completely different and independent subsystem.

4.1.7 Understanding

The understanding reflects the technology maturity that the common cause components used. This unified partial method assesses this factor from four aspects:

- the running experience of the common cause components, if the experience is more than 10a or less than 10a.

- the novelty of the technology that the common cause components used if the running of the equipment need the support of the computer software.

- the complexity of the technology that the common cause components adopts.

- if the adopted technology of the common cause components satisfy the design requirement.

For the above four aspects, all the conditions belong to attribute A except the condition that the system have the software. The last three aspects are considered as "big" or "small". Then, it is able to evaluate the attribute of this factor. For example, when the experience is more than 10a, and two "big", one "small", the attribute is C.

4.1.8 Operator Interaction

This factor reflects the complete degree of the operating procedure, and the probability of operating and maintenance staff making mistakes.

4.2 Discussion

For now, UPM is the most popular and widely used method in the UK nuclear industry for analyzing CCFs. The method is performed step by step based on the standard guide. Compared with other models of determining β-factor, UPM has some advantages.
Advantages:

- simple model

- overall consideration of personnel experience and safety culture

- non-professional people have access to the framework

- experienced expert and non-professional staff get the same answer

- can be used for both component level system and system level system
- do not require much system-specific data
- have a standard guide, so easy to perform
- it is a decision making process

Disadvantages are also inevitable:

- In this method, the values are determined by expert judgment, if there is design and operation change, the scores have to be adjust.
- Because non-experts can perform this method, the result may not so accurate.

4.3 Comparison Between IEC Checklists and UPM

The three methods described in this master thesis are used to determine common cause failure (beta-factor). IEC 61508-6 checklist is used for low-demand systems, mainly for process industry, while UPM is used for high reliability industry, most commonly used for nuclear power industry. IEC checklist is performed only by professional engineers while UPM can be performed by both professional and non-professional engineers. Both IEC checklists and UPM use defenses to reduce the system vulnerability to CCFs. However, IEC checklists are supplemented by series of questions (measures) to get scores, while UPM uses genetic tables to look for the corresponding scores. UPM provides a systematic framework which can be used for both system level and component level assessment. IEC checklist can only used for single level assessment. All the three methods take human factor into consideration, but IEC checklists only mentioned a little. In contrast, UPM considered enough human factor.

5 Summary and Recommendations for Further Work

5.1 Summary

In this master thesis, SIS is designed to meet the requirements of IEC61508 to verify if the risk reduction targets have been achieved. In order to improve the reliability of the SIS, redundancy is often introduced. However, redundancy also increases the vulnerability of the system to CCFs. There is no unified definition of CCFs, because different authors and specialists in various fields have different opinions. Therefore, a review of the definitions of CCFs has been presented. There are two kinds of causes of CCFs. One is root causes which are the basic causes of the failures. Another one is coupling factors which are coupled with redundancy. CCFs are very important consideration in probability safety assessment (PSA), since they may lead to disaster accidents. As a result, CCFs have attracted many researchers in recent years.

The most widely used method for modeling CCFs is beta-factor model. The brief introduction has been written in the early part of this master thesis, including advantages and disadvantages. Determining β-factor is an inevitable and vital part to modeling CCFs. Therefore, the main part of this master thesis is the methods determining β-factor. Three methods are described: IEC 61508-6 checklist for low-demand system, IEC 62061 checklist for high demand system, and UPM for high reliability industry. The advantages and disadvantages of these methods have been listed. Besides, the detailed comparisons between these three methods are conducted.

From my point of view, IEC checklists do not take much human factors into consideration. Human errors or action could affect the operation and the reliability of the system significantly. Therefore, more questions about human factors should taken into account. For IEC 62061 checklist which is for high-demand operation system, human factors are especially important because wrong operation could lead to the shutdown of the whole system. Further, it may cause the production loss or more severe consequences. In short, IEC checklists should consider more about human factor (training, working hours, etc).

5.2 Challenges

There are some difficulties occurred when people use this kinds of methods. When performing the critical evaluation of the 37 questions of IEC 61508-6 checklist, it is difficult for analysts well understand how the system works and know what kinds of documents the company should have. Besides, it requires the professional engineers to assess the checklist, and they must be very familiar with the design architecture of the system. Therefore, it is also difficult to judge if the questions are challenges for engineers. The only thing in this thesis is to connect the questions to CCFs, and then find out the consequences of not including these measures. However, the expriences of engineers who evlauate the checklist have significant influence on the result, because some of the questions need operation experience to get the answer.

One challenge in the method of IEC 61508 is that it is not well approved. There is still dispute on this checklist among researchers and engineers. No enough evidence is provided that the beta-factor determined by the IEC 61508 checklist reflect the real situation. Actually there is not much history data supporting the scoring system of both IEC 61508 and IEC 62061 checklists.

Another challenge is that there is no common CCF definition for all industries. As a result, the effectiveness of some measures in checklist methods maybe not the same in different industries.

5.3 Recommendations for Further Work

For further work, a general definition of CCFs should be proposed that can be used in all industries. Nowadays, although it is well known that CCFs are very important and it is a big threat to reliability assessment, there is no engouht studies on CCFs, and CCFs are not documented carefully. In the future, it is important to develop a more specific and accurate model for modeling CCFs. Also, for further work, collecting CCFs data from different industries and creating documents for CCFs could be done. And for IEC 61508 checklist, more questions about human factors should be considered and developed.

For the future work of β-factor determination, a general and more accurate method should be developed based on these three methods for all industries. In the operational phase, more CCFs maybe involved, but they are not well considered in existing checklists. Therefore, it is necessary to identify and model CCFs of the operational phase in determining β-factor.

Nomenclature

BFR	Binomial Failure Rate
BP	Basic Parameter
CMF	Common Mode Failure
DD	Dangerous Detected
DU	Dangerous Undetected
FTA	Fault Tree Analysis
LOPA	Layer Of Protection Analysis
MBF	Multiple Beta-Factor
Model	Multiple Greek Letter
MTBF	Mean Time Between Failure
PBF	Partial Beta Factor
PFD	Probability of Failure on Demand
PFH	Probability of Failure per Hour
PLC	Programmable Logic Controllers
PSA	Probability Safety Assessment
RBD	Reliability Block Diagrams
RCA	Root Cause Analysis
SD	Safe Detected
SIF	Safety Instrumented Functions

SIL	Safety Integrity Level
SIS	Safety Instrumented Systems
SU	Safe Unetected
UPM	Unified Partial Method

References

[1] IEC 61508 (2010). Functional safety of electrical/ electronic/programmable electronic safety-related systems. Parts 1–7. International Electrotechnical Commission, Geneva.

[2] BussinessDictionary, retrived from http://www.businessdictionary.com/ definition/reliability.html.

[3] Jin, H. (2012). Reliability of safety systems: Design to operation. Department of Production and Quality Engineering, NTNU

[4] OREDA (2002). Offshore reliability data, 4th ed. Available from: Det Norske Veritas, NO 1322 Høvik, Norway.

[5] Smith, A. M. and Watson, I. A. (1980). Common cause failures – a dilemma in perspective. pp 127–142.

[6] Hauge, S., Lundteigen, M. A., Hokstad, P., and Håbrekke, S. (2010). Reliability prediction method for safety instrumented systems, PDS method handbook. Technical Report Sintef A13503, NO-7465 Trondheim, Norway.

[7] Rausand, M. and Høyland, A. (2004). System Reliability Theory: Models, Statistical Methods, and Applications. Wiley, Hoboken, NJ, 2nd edition.

[8] Lundteigen, M. A. (2006). Hardware safety integrity (HSI) in IEC 61508/ IEC 61511, Lecture slides.

[9] Wetherholt, J., (2011). Common cause failure modes. NASA Marshall Space Flight Center, Huntsville, Alabama, USA.

[10] Lundteigen, M. A. (2007). CCFs - definitions, models and defenses. Lecture slides.

[11] NEA (2004). International common-cause failure data exchange. (NEA/CSNI/R(2004)4). Neclear Energy Agency.

[12] NEA (2004b). International common-cause failure data exchange. ICDE general coding guidelines. Technical report R(2004)4, Nuclear Energy Agency, Paris.

[13] IEC 615011 (2003). IEC 61511 Standard. Functional safety - safety instrumented systems for the process industry sector.

[14] NUREG/CR-4780 (1988). Procedures for treating common-cause failures in safety and reliability studies.

[15] NASA (2002). Probabilistic risk assessment procedures guide for nasa managers and practitioners. Technical report, NASA Office of Safety andMission Assurance.,Washington DC.

[16] Rausand, M. (2011). Risk Assessment: Theory, Methods, and Applications. Wiley, Hoboken, NJ.

[17] Stamatelatos, M., Apostolakis, G., Dezfuli, H., Everline, C., Guarro, S., Moieni, P., Mosleh, A., Paulos, T., and Youngblood, R. (2002A). Probabilistic risk assessment procedures guide for NASA managers and practitioners. Technical report, U.S. National Aeronaustics and Space Administration, Washington, DC.

[18] US DOE (1992). Root cause analysis guidance document. Technical Report DOE-NE-STD-1004-92, U.S. Department of Energy, Office of Nuclear Energy, Washington, DC.

[19] Miller, A. G., Kaufer, B., and Carlson, L. (2000). Activities on component reliability under the OECD Nuclear Energy Agency. Nuclear Engineering and Design, 198:325-334.

[20] Brand, V.P., (1996). UPM 3.1: A pragmatic approach to dependent failures assessment for standard systems. AEA Technology plc (Warrington), SRDA-R13.

[21] Lundteigen, M. A. (2010). Lecture slides: Common cause failures. RAMS Group. NTNU

[22] Zitrou, A. (1996). Exploring a Bayesian Approach for Structural Modeling of Common Cause Failures. University of Strathclyde Department of Management Science

[23] Wang, L. Y. (2011). Common Cause Failure Modeling in Risk and Reliability Assessments: An Evaluation of Approaches. Project Thesis. RAMS Group. NTNU

[24] Tim, B. (2011). Common cause failure: a modeling perspective. University of Stathclyde Glasgow, Scotland.

[25] Hokstad, P., Rausand, M. (2008) Common Cause Failure Modeling: Status and Trends. Handbook of Performability Engineering 2008, pp 621-640.