PDS

SINTEF

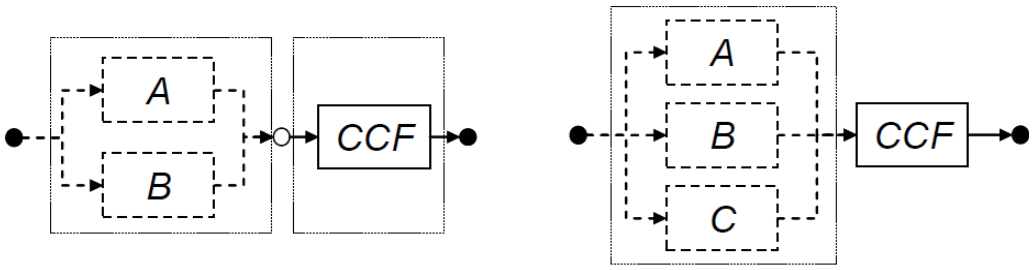
SINTEF A26922 - Unrestricted

Report

Common Cause Failures in Safety Instrumented Systems

Beta-factors and equipment specific checklists based on operational experience

Authors
Stein Hauge
Åsa Snilstveit Hoem
Per Hokstad
Solfrid Håbrekke
Mary Ann Lundteigen



SINTEF Technology and Society
Safety Research
2015-05-20

SINTEF

SINTEF Teknologi og samfunn
SINTEF Technology and Society

Address:
Postboks 4760 Sluppen
NO-7465 Trondheim
NORWAY

Telephone:+47 73593000
Telefax:+47 73592896

ts@sintef.no
www.sintef.no
Enterprise /VAT No:
NO 948 007 029 MVA

KEYWORDS:
Safety Instrumented Systems
Common Cause Failures
New beta-factors
Equipment specific checklists

Report

Common Cause Failures in Safety Instrumented Systems

Beta-factors and equipment specific checklists based on operational experience

VERSION
Final

DATE
2015-05-20

AUTHORS
Stein Hauge
Åsa Snilstveit Hoem
Per Hokstad
Solfrid Håbrekke
Mary Ann Lundteigen

CLIENT(S)
Multi-client

CLIENT'S REF.
Håkon S. Mathisen

PROJECT NO.
102001186

NUMBER OF PAGES/APPENDICES:
72 incl. 1 Appendix

ABSTRACT
This report summarizes the results of a field study of common cause failures (CCFs) in relation to safety instrumented systems (SIS) in the oil and gas industry. Some 12.000 notifications have been reviewed by the project team, involving six different installations. Main deliverables from the study are: 1) Generic beta-factor values for main component groups of safety instrumented systems, and 2) CCF checklists for assessing possible CCF causes, and defences. The checklists may be used to determine installation specific values of beta-factors for SIS. The aim has been to improve the petroleum industry's ability to predict and quantify the occurrence of CCFs. The report has been prepared as part of an ongoing research project financed by the Research Council of Norway and the PDS forum members.

PREPARED BY
Stein Hauge, Åsa Snilstveit Hoem, Per Hokstad, Solfrid Håbrekke, Mary Ann Lundteigen

SIGNATURE
Stein Hauge

CHECKED BY
Lars Bodsberg

SIGNATURE
Lars Bodsberg

APPROVED BY
Stian Antonsen, Research director

SIGNATURE

REPORT NO.	ISBN	CLASSIFICATION	CLASSIFICATION THIS PAGE
SINTEF A26922	978-82-14-05953-3	Unrestricted	Unrestricted

SINTEF

Document history

VERSION	DATE	VERSION DESCRIPTION
Draft version 0.1	2014-10-21	DRAFT report distributed to PDS members for comments
Final version 1.0	2015-05-20	Final

Preface

This report is a deliverable from the research project "Tools and guidelines for integrated barrier management and reduction of major accident risk in the petroleum industry" (2012-2015). The project has been funded by the PETROMAKS2 programme for petroleum research at the Research Council of Norway and industry participants of PDS forum. The work has mainly been carried out by SINTEF and may therefore not express the views of all the PDS participants.

PDS forum is a co-operation between oil companies, engineering companies, drilling contractors, consultants, vendors and researchers, with a special interest in safety instrumented systems in the petroleum industry. The main objective is to maintain a professional meeting place for:

- Exchange of experience and ideas related to design and operation of safety instrumented systems (SIS)
- Exchange of information on new field developments and SIS application areas
- Developing guidelines for the use of new standards on safety and control systems
- Developing methods and tools for calculating the reliability of SIS
- Exchange and use of reliability field data

Participants PDS forum

Oil companies / Operators:

A/S Norske Shell
BP Norge AS
ConocoPhillips Norge
Det norske oljeselskap ASA
Eni Norge AS
GDF SUEZ E&P
Odfjell Drilling & Technology
Lundin Norway AS
Statoil ASA
Talisman Energy Norge
Teekay Petrojarl ASA
Total E&P Norge AS

Governmental bodies (observers):

The Norwegian Maritime Directorate
The Petroleum Safety Authority Norway

Control and Safety System Vendors:

ABB AS
FMC Kongsberg Subsea AS
Honeywell AS
Kongsberg Maritime AS
Origo Solutions AS
Siemens AS
Simtronics ASA

Consultants / Engineering companies:

Aker Engineering & Technology AS
Aker Subsea AS
DNV GL Norge AS
Fabricom AS
Lilleaker Consulting AS
Lloyd's Register Consulting
Safetec Nordic AS

http://www.sintef.no/PDS

SINTEF

Table of contents

Executive summary

This report summarizes the results of a field study of common cause failures (CCFs) in relation to safety instrumented systems (SIS) in the oil and gas industry. Similar initiatives have previously been taken in other industry sectors, like the nuclear industry, but very limited field data on CCFs has been collected so far in the oil and gas industry.

CCFs include events that result in multiple component failures, affecting one or more SIS within a limited time interval. The following definition of CCF has been used during operational reviews: *Components/items within the same component group that fail due to the same root cause within a specified time.*

The purpose of this study has been to provide more insight into why and how often CCFs occur. Improved knowledge of CCF is important for operating companies as well as system designers and integrators in order to comply with the high reliability requirements of SIS in the oil and gas industry and the requirement for "sufficient independence" as stated by the Norwegian Petroleum Safety Authority.

Some 12.000 notifications have been reviewed by the project team, involving six different installations. Based on failure description and discussion with operational personnel, each failure has been grouped into independent and dependent failures to establish the fraction of all component failures that are common cause failures.

An important basis for the study has been the beta-factor model. This is a widely used reliability model for CCF introducing the Greek letter β as a model parameter. In this model the failure rate of a component (λ) is split into an independent part (1-β)λ and a dependent part (βλ) due to a common cause. The beta-factor (β) is defined as *the fraction of the component failures that result in a common cause failure*.

Main deliverables from the study are:

- Generic beta-factor values for main equipment groups of SIS
- CCF checklists for assessing possible CCF causes, and defences. The checklists may be used to determine installation specific values of beta-factors for SIS.

Generic Beta-factor values

The number of CCF events and new suggested generic beta-factor values are summarised below for main equipment groups of SIS. "Total population" is the number of component tags across all six installations, N_{DU} is the total number of dangerous failures not detected automatically, but typically revealed during functional testing or upon an actual demand (DU failure) and $N_{DU,CCF}$ is the total number of DU failures affected by a CCF event.

The recorded CCF events vary significantly between the installations. On some installations no CCF events have been observed for certain component groups, whereas on other installations an excessive fraction of CCFs has been observed.

Findings from the study suggest that the fraction of CCFs experienced during operation is higher than what is typically assumed in reliability calculations. This is an important result, as it indicates that previous reliability predictions of redundant SIS may be too optimistic, and that the independence between components may be lower than what has traditionally been assumed. The results should therefore encourage the petroleum industry to put more effort into analysing and avoiding CCFs, in design as well as during operation. Performing regular operational reviews (ref. Section 4.1) with a particular focus on systematic failures and CCFs may be a practical way of following up such failures during operation.

Equipment group	Total population	N_{DU}	$N_{DU,CCF}$	New suggested β	β from PDS 2013 data handbook (for comparison)
ESD/PSD valves (incl. riser ESD valves)	1120	279	68	**12 %**	5 %
Blowdown valves	228	73	17	**12 %**	5 %
Fire dampers	458	44	23	**20 %**	5 %
PSVs	2356	148	32	**11 %**	5 %
Gas detectors (point and line)	2239	74	20	**15 %**	7 %
Fire detectors (flame, smoke and heat)	5921	65	19	**15 %**	7 %
Process transmitters (level, pressure, temperature and flow)	1746	112	32	**15 %**	6 %

Checklists for assessing possible CCF causes, defences and installation specific beta-factors
CCF checklists are presented (in Appendix A) based on three CCF categories recorded during the operational reviews and a literature review. The following CCF categories (example sub-categories in parentheses) have been used: 1) *Design properties (*Component specification and manufacturing, material selection, etc.), 2) *Environmental control-external/internal (*climate and temperatures, corrosion and erosion, etc.), 3) *Operation, maintenance and modifications (*procedures and routines, personnel competency and training, etc.)

The main purposes of the CCF checklists are to:

- Classify and elucidate underlying factors that contribute to CCF
- Support decisions regarding possible defences or measures to reduce CCF, considering both root causes and coupling factors.
- Provide a method for adjusting generic beta-factor values to incorporate installation specific conditions for different types of SIS

For each equipment group, the user may assess the relevance of listed CCF causes and efficiency of the listed defences. A detailed weighting procedure and multiplicity factors are provided for determining the installation specific beta-factors.

Typical applications of the CCF checklists will be:

- During early design to determine plant specific beta-factor for early SIL calculations

- During detail design phase to revise plant specific beta-factor based on additional knowledge about factors and conditions. The updated beta-factors will typically be applied for SIL calculations and possibly for input to quantitative risk analysis.
- During operational phase to justify that the assumptions for the plant-specific beta-factor are still valid.
- During all phases to assess the likelihood of CCFs for a particular design and a foreseen operational regime. A checklist may also be used more qualitatively to identify vulnerabilities to common cause failures and to point at possible defences that, if implemented, will result in a reduction of the beta-factor.

In reliability assessments it is important to adjust the generic beta-factor in light of installation specific issues and considerations. By using the proposed CCF checklists, the confidence in using beta-factor values in reliability assessment may increase, and at the same time it may encourage the implementation of specific measures to reduce the occurrence of CCFs.

1 Introduction

1.1 Background

The Management Regulation §5 is one of the key requirements that frames the design and operation of safety barriers in the Norwegian petroleum industry. It outlines the principle of having multiple, and sufficiently independent barriers to control risk and the need to prevent multiple barrier failure or degradation from single events or conditions. According to the Management Regulations §5: *"Where more than one barrier is necessary, there shall be sufficient independence between barriers"*. "Sufficient independence" means that design and/or operational measures shall be in place to avoid simultaneous failure of several barrier elements. Avoiding such failures therefore becomes an important part of barrier management and accident prevention.

Many of the safety barriers are implemented by safety instrumented systems (SISs), such as emergency shutdown (ESD) system, process shutdown (PSD) systems, and fire and gas (F&G) detection system. In addition, it is an increasing trend to introduce special-purpose SISs to compensate for the lack of inherently safe design. One example is instrumented overpressure protection systems, installed to stop pressure build-up beyond the design specification of pipelines or vessels.

The use of SISs has many advantages, in particular when it comes to flexibility and ability to provide information about the state of the system elements. At the same time, there are challenges: Using instrumented technology in more than one safety barrier introduces some dependencies, including common design principles and technology, same environment and same operation and maintenance procedures and practises. Redundancy is often introduced to make the systems more reliable; but the mentioned dependencies may reduce the intended reliability effects.

Dependencies are included in reliability assessments by modelling the effects of multiple failures with shared causes. Such CCFs are sometimes the main contributor to the total safety for systems with redundant elements or barriers. This has been illustrated in the below figure.

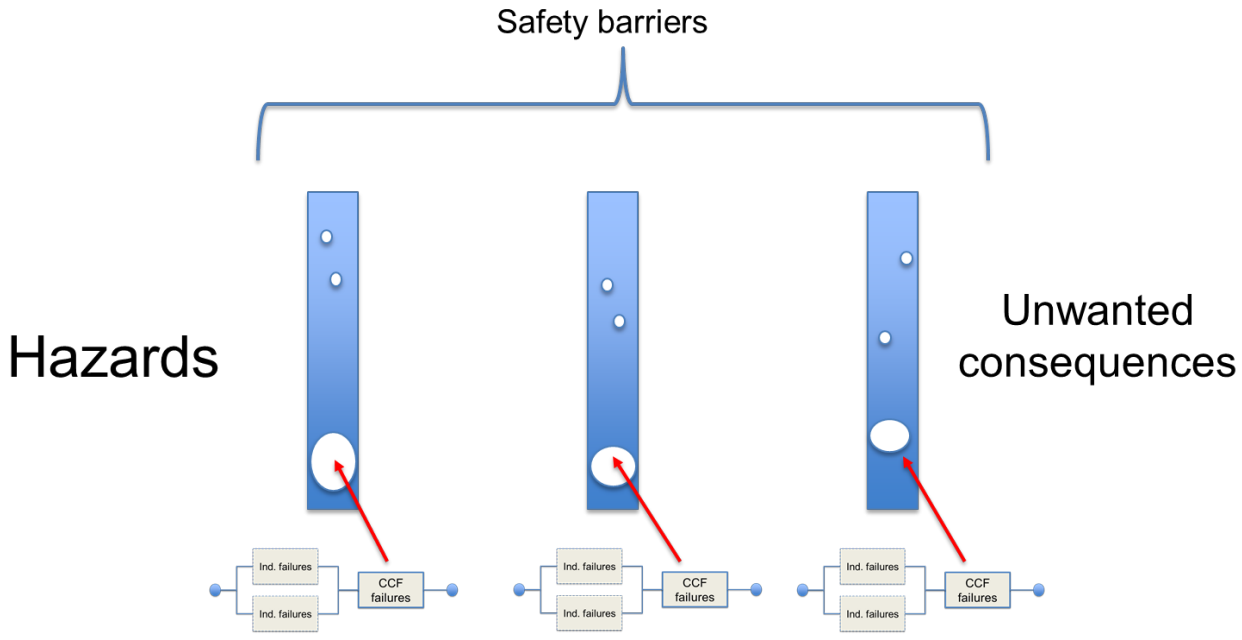


Figure 1: Possible effect on safety barriers from common cause failures.

Although CCFs are an important contributor towards the safety unavailability, very few data sources are available on such failures for assessing the associated reliability model parameters. Some data for the fraction of CCFs (such as the β in the beta-factor model) have been suggested, but these are generally based on expert judgements and figures from the nuclear industry, rather than actual operational data from the petroleum industry. It is therefore important to obtain more realistic data for CCFs relevant also for the petroleum industry.

1.2 Scope and objective

Reliability calculations basically involve two main activities:

1. Establish the mathematical/statistical model of the given system including CCF analyses, by use of e.g. analytical formulas, reliability block diagrams, fault trees, Markov models or simulation techniques.
2. Establish the value of variables and parameters to be used as input to the reliability model, typically from OREDA [2009], the PDS data handbook [2013], other data handbooks, company specific databases or vendor certificates.

Significant research efforts have traditionally been put into activity 1, both in academia, through textbooks, standards and guidelines, e.g. exemplified through the newly released ISO/TR 12489 [2013] which gives a thorough description of different reliability modelling and calculation methods.

Major initiatives are also on-going for data collection in the petroleum industry, in particular through the OREDA project and the RNNP project; "Trends in risk level in the petroleum activity" [PSAN, 2014]. Neither of these initiatives are however specific with respect to data on CCFs.

To respond to the lack of data SINTEF has, as part of the PDS research project, carried out operational failure reviews with a particular focus on identification of possible CCFs. Based on a review of some 12 000 maintenance notifications, typical CCF causes have been identified and discussed. The extent of the CCFs included in the study comprises failures introduced during design as well as failures introduced during the operational phase. Based on the registered fraction of such failures, new generic (or average) β-factors have been suggested for selected equipment groups.

Although CCF-checklists already exist in e.g. IEC 61508 and IEC 62061, the new knowledge has also been used as basis for developing *equipment specific checklists*, targeted to address the most important causes of CCFs for each equipment type.

These new data and checklists should hopefully be used for improving the quality of CCF calculations as well as performing more qualitative analyses to identify and mitigate the extent of CCFs.

1.3 Research approach and structure of report

The main approach in this research activity has been as follows:

Step 1: Carry out a literature review and a workshop on the treatment of CCFs in PDS forum. The results were used as input to steps 2–4.
Step 2: Review of reported failures (maintenance notifications). The operational reviews were facilitated by SINTEF, but involved key discipline personnel (automation, mechanical, process) from the specific

facility and company in question. Each notification was reviewed with the purpose of classifying failures according to IEC 61508 [2010].
Step 3: Analysis of results. The results from all six facilities were reviewed, and the failures associated with the same type of components with shared causes were – given a set of associated criteria - classified as CCFs or failures that could have caused a CCF.
Step 4: Suggestions for new generic β-values and development of equipment specific CCF checklists based on the results in Step 3.

The results have been structured as follows:

- Findings from the literature review and the PDS workshop is given in Chapter 2 and Chapter 3. Chapter 2 focuses on definitions and concepts related to CCFs whereas Chapter 3 discusses methods for the determination of the β-factor
- In Chapter 4 the main results from the operational reviews including analysis/discussion of the result are given. This also includes the new estimated β-values
- Chapter 5 includes an example of an equipment specific checklist. Chapter 6 provides some conclusions followed by References.
- Appendix A contains the checklists for adjusting the fraction of CCFs (β) for specific component and operating conditions.

1.4 Assumptions and limitations

Many of the assumptions and limitations when determining the fraction of CCFs are related to failure classification:

- Both dangerous undetected (DU) and dangerous detected (DD) failures may be subject to common causes. In this report we focus on CCFs related to DU failures, since DU-failures are typically the main contributor to the safety unavailability of SIS. However, it should be noted that also DD failures can give significant contributions to the unavailability if not corrected within reasonable time. The DD failures identified in the operational reviews normally seemed to be corrected within a few days. However, there were also several examples from the operational reviews where DD failures were not corrected until several weeks after the failure was detected, implying that the assumption of a negligible contribution from DD failures may not be valid.

- During the operational reviews a number of failures were classified as Safe (S) and degraded. Also such failures may be due to common causes. However, in this study it was decided to focus on failures with a main contribution to the safety unavailability of SIS.

- Failure causes introduced both in design, as well as during operational phases are included. A partition between "design", "environmental control" and "operation, maintenance & modifications" has therefore been made in the report. This may enable some users, e.g. manufacturers, to modify the generic βs if it can be argued that some failure causes are not relevant.

Other assumptions and prerequisites of the study include:

- The equipment for which malfunction notifications have been collected and reviewed includes safety critical equipment that is mostly SIL classified (excluding PSVs).

- The report includes some of the most common equipment groups of safety instrumented systems related to sensor elements and final element. Logic units have not been included even if some failures related to the logic have been identified during the reviews. In particular, several failures on digital output (DO) and analogue input (AI) cards and failures related to loop monitoring have been revealed. These failures are, however, often registered as e.g. transmitter or valve failure. A separate review of the logic failures has however not been performed since none of the facilities have any dedicated tagging system for the relevant logic components. Therefore, due to inadequate tagging of logics components and also due to the fact that the number of DU failures and thus CCF events are limited, no CCF considerations have been made for such equipment.

- The equipment for which CCF data has been collected is subject to proof testing at regular intervals (typically annually). Hence, the underlying assumption that the fraction of CCFs (β) can be assumed independent of the length of the test intervals is considered valid.

- The data in this report is based on operational reviews performed in the Norwegian offshore industry and considers facilities for the Norwegian Continental Shelf only. Data from both offshore and onshore facilities have been collected, but the amount of CCF events is too limited to differentiate between fractions of CCFs for offshore versus onshore equipment.

- CCF data has been collected for entire populations of similar equipment, e.g. for all ESD valves on the six installations. For many equipment types like blowdown valves and ESD valves, the valves will normally be located in single (1oo1) configurations. Simultaneous failures of such components (e.g. failure of two single blowdown valves located on two adjacent process segments) have been treated as a CCF. This is further discussed in Chapter 3, where estimation of the fraction of CCFs is treated.

1.5 Abbreviations

Abbreviations used in the report are given below:

AI	-	Analogue Input
BWR	-	Boiling Water Reactor
CCF	-	Common Cause Failure
CMF	-	Common Mode Failure
DD	-	Dangerous Detected
DO	-	Digital Output
DU	-	Dangerous Undetected
ESD	-	Emergency Shutdown
HMI	-	Human Machine Interface
HPU	-	Hydraulic Pressure Unit
ICDE	-	International Common Cause Data Exchange
PDS	-	(Norwegian abbreviation for) Reliability of safety instrumented systems
PFD	-	Probability of Failure on Demand
PSAN	-	Petroleum Safety Authority Norway
PSD	-	Process Shutdown
PSV	-	Pressure Safety Valve
RNNP	-	Trends in risk level in the petroleum activity.
S	-	Safe
SAP	-	Systeme, Anwendungen und Produkte in der Datenverarbeitung

SIF	-	Safety Instrumented Function
SIL	-	Safety Integrity Level
SIS	-	Safety Instrumented System
SKI	-	Swedish Nuclear Power Inspectorate
UPM	-	Unified Partial Method

2 Definitions and concepts

In this chapter selected definitions and concepts related to CCFs are discussed. When relevant, these concepts and definitions have been related to the approach taken in the operational reviews and the results presented in this report.

2.1 Definitions

2.1.1 CCF definitions

CCF definitions have been proposed and refined over several decades. There are several CCF definitions available and inconsistencies can be found between these definitions.

IEC 61508 [2010] defines a CCF as *a failure, that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to system failure*. A channel is defined as an element or group of elements that independently implement a safety function (or part of a safety function).

NUREG [1988] defines CCFs as *a subset of dependent failures in which two or more component fault states exist at the same time, or with a short interval, because of a shared cause.*

ISO/TR 12489 [2013] defines CCFs as *failures of different items, resulting from a single event, where these failures are not consequences of each other*. It is also noted that it is generally accepted that the failures occur simultaneously or within a short time of each other.

In PDS [Hauge et.al. 2013] the fraction of CCFs (β) is defined as: *The fraction of failures of a single component that causes both components of a redundant pair to fail "simultaneously"*. In configurations with more than two redundant components, modification factors (i.e. C_{MooN} factors) are then applied together with the β value to estimate the likelihood of more than two components failing simultaneously.

Smith and Watson [1980] review nine different definitions of CCF and suggest the attributes that a definition of CCF must encompass:

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 failure.
4. The failures occur within a defined critical time period (e.g. the time a plane is in the air during a flight).
5. The failures are due to a single underlying defect or 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 (complete CCF).

In this report, the term *CCF* (or CCF event) is used to denote multiple events that fulfil criteria 1.-5., but not necessarily criterion 6. E.g. in a 2oo4 configuration, two components may fail due to a common cause, but the system will still function. Hence, this is a CCF but will not disable the system's ability to function (criterion 6).

Note that failure of two or more components due to a common cause is considered a CCF although the components are not part of the same SIF (ref. criterion 2.). For example blowdown and ESD valves are often

configured as 1oo1 in a typical SIF. However, if two such blowdown valves (or two ESD valves) fail simultaneously, this has been registered as a CCF. This information is e.g. important when assessing the combined probability of failure of several blowdown valves (or ESD valves) at different locations on a plant in case of a process leak or a fire/explosion. This is further discussed in Chapter 4.

The term *complete CCF* is a set of failures that fulfil all the six criteria and thus result in a system failure (or a failure of the SIF) when occurring. Thus a complete CCF can be considered a subset of CCFs. In this report and for practical purposes, the term complete CCF has not been applied and we rather use the term *CCF event*, which complies with criteria 1. – 5. above.

2.1.2 Practical CCF definitions and challenges when determining CCFs

The following definition of CCF has been used during the operational reviews:

> *Components/items within the same equipment group that fail due to the same root cause within a specified time.*

The identification of CCFs among reported failures would overlook many possible causes of CCFs if focusing only on the CCF events. Systematic failures, i.e., failures that are due to errors made in specification, design, installation, or operation and maintenance, and which are not due to natural degradation of the component state, may be replicated for several components. When a systematic failure is found, it is important to also ask if other components may have been affected. Therefore, in the failure reviews, it has, for each systematic failure, been questioned whether the failure could have resulted in multiple failures within a relatively short time window. If yes, the failure has been considered as a *potential CCF*.

The term *potential* CCFs is thus used to capture a broader category of CCFs, and includes all foreseeable causes that may result in a CCF based on a review of recorded failures and failure causes. This term is also mentioned in the ICDE guideline [NEA, 1012], but not formally defined. In practice we see that a potential CCF very much resembles a systematic failure. The two are however not identical; A failure may be systematic without necessarily having the potential to create a CCF (under given conditions and configurations). On the other hand, a potential CCF (as interpreted in this report) will always have the properties of a systematic failure.

CCF events and potential CCFs have been introduced to serve two different purposes. CCF events may, when counted up, be used to estimate how often CCFs have occurred, i.e. for finding the beta-factor. The main problem is that a facility specific CCF failure rate (and even aggregated CCF failure rates over several facilities) will have a high level of uncertainty, due to limited data sample. Potential CCFs cannot be included, at least not with the same weight as CCF events, in the estimation of beta. However, potential CCFs are important, since they include additional information about potential failure causes and thus can be used for identifying vulnerabilities in design or its operating environment that, if prevented or modified, could reduce the future occurrence of CCFs and systematic failures.

Even with the fairly pragmatic CCF definitions discussed above, it may be challenging to decide whether a failure is a CCF or not when performing failure data classification. Consider an example from a facility where several ESD valves require hydraulic power to close. Upon a shutdown it was observed that some of the ESD valves did not close according to the required closure time. At first glance this appears to be a typical CCF event, however since the shutdown occurred during a fire event, further investigation was initiated. It was then revealed that the ESD valves were powered from the same HPU which had recently been completely overhauled and flushed. After this overhaul there had probably been some remaining air in the hydraulic lines, which caused the ESD valves to close too slowly. Consequently, the HPU was a common

component that shall ideally be modelled as a separate failure sources in the reliability calculations. The issue of common components versus common cause is further discussed and exemplified in Chapter 4 (results from the operational reviews).

It will also sometimes be difficult to distinguish between failures that have occurred suddenly (due to a kind of shock; e.g. cold temperatures, extreme snowfall, electrical failure, maintenance errors, etc.) and failures that have developed gradually over time (e.g. due to stress beyond design specifications, such as excessive vibration). Despite the difficulty of distinguishing these types of failures (e.g. due to lack of detailed information in the maintenance notifications), they have generally been considered as CCFs in the failure classification, given that the failures are detected close in time (typically during the same preventive test).

It should be noted that multiple failures with CCF characteristics may occur over a time period longer than a test interval. This is mainly because the (common) root cause of the failure is not detected nor repaired after the first failure, and a similar failure therefore may still occur on another component during the next test interval. When going through operational failure data we have included only CCFs that have been detected during the same PM/test or have been revealed at the "same" time during operation.

2.1.3 Some additional definitions

Below, some additional terms used in this report are further explained.

Dangerous failure; A failure which has the potential to put the component in a hazardous or fail-to-function state (IEC 61508-4 relates a dangerous failure to system failure, but the common interpretation is to relate the failure classification to the component level).

Dangerous detected (DD) failure; Dangerous failure detected by self-test or online comparison of instruments. For example this can be a dirty detector lens which is automatically alarmed in CCR.

Dangerous undetected (DU) failure; Dangerous failure not detected automatically, but typically revealed during functional testing or upon an actual demand. For example this can be a valve which does not close during a functional test.

Degraded failure; A failure that is not critical, but may gradually develop into a critical failure [NEA 2012].

Safe failure; A failure which does not have the potential to put the component in a hazardous or fail-to-function state. Such failures may result in a transition to a safe state of the component, which again may lead to a production shutdown.

Redundancy; The existence of more than one means for performing a required function or for representing information [IEC 61508 2010].

2.2 CCF concepts

2.2.1 Dependent failures and independency

Dependent failures are traditionally split into three categories [Amendola 1989]:

- ***CCF (common cause failure)*** *causing multiple failures from a single shared cause. The multiple failures may occur simultaneous or over a period of time.*

- ***CMF (common mode failure)*** *which is a subgroup of CCF where multiple component items fail in the same way / same failure mode*
- ***Cascading failures*** *which are propagating/escalating failures*, i.e. failure mode of one or more components giving other operational conditions, environment, etc. such that other components fail.

Dependency is a general term that includes more failures than CCF. Examples of dependencies may be properties related to design, such as common technology or common utility systems, it may be related to a common external environment or it may be commonalities related to personnel that operate and maintain the systems. Hence, dependencies can be seen as factors or conditions that enable CCFs as well as cascading failures.

In this report and in the operational reviews we have focused on CCFs (and CMFs). When classifying failures we often experience that the failure cause is not described in detail or not described at all. However, from the maintenance notifications it can be observed that a number of similar components have failed in the same way (or mode) and can therefore be classified as CCFs.

Cascading failures are traditionally not included in common cause failure calculations as they affect different types of components and origin from a failure in another component. For the same reason they do not easily fit into the models that are available for CCF. Additionally, they will be very difficult to identify from review of maintenance notifications. Cascading failures have therefore, although important, not (intentionally) been included in this study. It may however, happen, that such failures are included unintentionally due to the way in which CCF data have been collected and the fact that the failure cause will sometimes not be described in detail. It should however be noted that in cases of inadequate failure cause description in the maintenance notification, operational personnel have been consulted for more detailed information.

2.2.2 Root causes and coupling factors

Root causes and coupling factors are two key attributes for understanding how and why CCFs occur. The two attributes were first introduced in the Nuclear industry, see e.g., Parry [1991] and Paula et al. [1991].

A **root cause** is the most basic reason or reasons for the component failure, which if corrected, would prevent recurrence [NUREG 1998]. Examples of root causes are high or low temperature, excessive sand production, large vibrations, earthquake, fire, sudden changes in loads, high or low pressures, moisture or high humidity, heat radiation, electrical failure, lack of procedures, failure to follow repair or test procedure, systematic calibration failures, design failure, inadequate testing/inspection/follow-up etc.

All too often, the description of a failure is limited to the most obvious (or direct) cause or a simple statement that "the component has failed". Without a proper identification of the root cause, it is difficult to select the most efficient defence measure. For example, in the review of reported failures, we see that failed detectors are often just replaced by a similar type without further analysis. We also see that valves being stuck during a functional test may be cleaned and lubricated and then operated successfully. Lubrication has a short term effect on the valve performance, and the actual root cause is seldom revealed. Such short term strategies are therefore often insufficient for the purpose of selecting the most effective defence measures.

A **coupling factor** is a characteristic of a group of components or parts that identifies them as susceptible or vulnerable to the same causal mechanisms of failure [NUREG 1998]. Such characteristics may be related to the use of common procedures, common design principles, the same environmental exposure and/or operating environment, and the same personnel involved in design, installation, operation, or maintenance. Some examples of coupling factors may be that the same operator calibrates all level transmitters mounted on the same vessel. Another example is that a whole set of flame detectors are located in an area exposed to

sea water spraying. A coupling does not trigger any failure by itself, but its presence may replicate or allow the replication of the same failure onto several components.

In Figure 2 we have tried to illustrate the relationship between a root cause, a coupling factor and the further development into a CCF. A root cause, such as increased sand production in a pipe, combined with a coupling factor such as two similar valves in the same pipe segment, may result in degradation of the valves and eventually a simultaneous failure of both valves.

Similarly a root cause such as a systematic calibration error can in combination with a coupling factor such as similar transmitters on the same vessel, result in a simultaneous failure of all transmitters on the vessel.

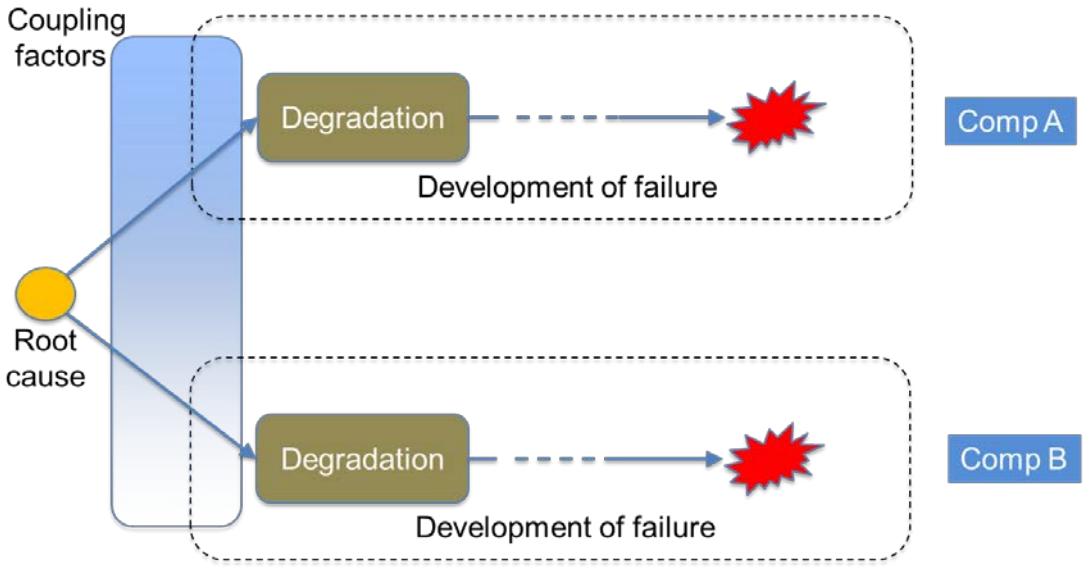


Figure 2: Illustration of root cause and coupling factor leading to CCF of two components.

Root causes and coupling factors are not always easily distinguishable in practice, e.g. due to lack of detailed descriptions in the maintenance notification. For the purpose of this study they have therefore been combined into **CCF categories**. Jointly they represent *enabling conditions that need to be present in order to experience a CCF*. In practice CCF categories therefore represent a combination of the root causes and the coupling factors that must be present to enable a CCF to occur. This is further discussed in Chapter 5.

2.2.3 Defences against CCFs

Protection against CCFs aims to eliminate or reduce the root causes of equipment failure and/or to eliminate/reduce the coupling mechanisms between components. Examples of measures to remove root causes can be the installation of sand filters to prevent erosion, training of operators to avoid miscalibration of transmitters or redesign of junction boxes to avoid water intrusion. Examples of measures to reduce coupling can be the installation of weather protection to prevent common exposure to seawater spraying, relocation of pressure transmitters from the same pipe segment (physical separation), or the application of diverse redundancy.

According to IEC 61508 [2010] **diversity** is defined as *different means of performing a required function.* Diversity may be achieved by different physical methods or different design approaches, e.g. by applying

two different types of measurement principles for level control. In theory, diversity is considered a positive feature with respect to reducing the occurrence of CCFs. In practice there may however also be some potential challenges of introducing diversity. A negative effect of diversity is that the more devices present at a facility, the more chance there is that a technician will not work on a device for a period of time and therefore become less familiar. Thus, diversity may introduce human errors. On the other hand, for example; high quality measurement of level is hard to achieve with the same measurement principle under changing densities and compositions, and in such cases it may be important to rely on diverse, rather than identical measurement principles. For other equipment, such as valves and pressure transmitters, the effects of diversity are more limited as the functional capability of the equipment is more “stable” in the different modes of operation.

In practice, there may be operational constraints that limit the choice of available defence measures. For example, root causes that are external, such as snow, sea spray, low/high ambient temperatures, or process parameters such as acidity and sand content in fluid, cannot always be modified, and their effects must be catered for during design and by selecting defence measures that reduce the coupling factors.

3 Methods and data for determination of beta-factor

"Essentially, all models are wrong, but some are useful" (George E.P. Box)

IEC 61508, and related standards like IEC 61511, require that the contribution from CCFs shall be included in the quantification of reliability. A number of different reliability models for CCFs are available [Hokstad and Rausand, 2008]. Among the most popular models is the beta-factor model using the parameter β to represent the fraction of all item failures that are CCFs. The PDS CCF model is an extension of the beta-factor model.

In this chapter we will:

- Give a short review of selected methods for determining plant-specific beta-factor values
- Briefly discuss the general shortage of relevant CCF data
- Present some selected estimators for the β factor when field data is available

First some methods for determining the beta-factor are discussed.

3.1 Methods for determining plant-specific beta-factor values in reliability analysis

3.1.1 Humphreys' method

Generic beta-factor values will be indicative but does not necessarily represent our best knowledge for a particular facility which has implemented several measures against CCF. What is sometimes referred to as the Humpreys' method [Humpreys, 1987] is one of the first attempts to determine an application specific beta-factor. In this method eight factors influencing the beta-factor value are identified (grouped in *design*, *operation* and *environment*). The factors are weighted based on expert judgment to determine a beta-factor between 0.01% and 30%.

3.1.2 IEC 61508 and IEC 62061

IEC 61508 [2010], Part 6, annex D presents a checklist of about 40 questions that can be used to determine a plant-specific value of the beta-factor for safety instrumented systems. The IEC 62061 [2005] standard includes a similar checklist (but simplified compared to IEC 61508).

In IEC 61508, each question is answered by “yes” or “no”. X and Y scores are given for each question and, for all questions with answer “yes”, the corresponding X values and Y values are summed up. A table is used to determine the beta-factor based on a total score for X and Y summed up for all questions:

$$Score = \sum (X + Y)$$

This method provides a beta-factor between 0.5 % and 5 % (for logic solvers) and between 1 % and 10 % for sensors and final elements. The original Humphreys' method gave a maximum of 30%, and it may be questioned if this is too high in light of more recent technology. At the same time, failure reviews indicate that 10% may be a too low value for some facilities and several component types.

The 40 checklist questions in IEC 61508-6 are categorized into eight groups:

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

One problem with the IEC 61508 checklist is its relatively low sensitivity to changes in score of each checklist question. The scores of several questions must usually be improved in order to move from one beta-factor value to the next. For example, introducing a measure that will improve separation of redundant components will not make any change in beta-factor value. Also, some of the checklist questions in IEC 61508 are quite general by nature, and difficult to answer during a design phase. The checklist in IEC 62061 appears to have some of the same challenges.

3.1.3 Unified Partial Method

The unified partial method (UPM) was proposed by Brand [1996] and further developed by Zitrou and Bedford [2003]. It assumes that the beta-factor is influenced by the following eight underlying factors:

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

The factors are not independent of each other. Each underlying factor is associated with a weight and a score. A mathematical relationship is established between these factors (i.e., their weights and scores) and the beta-factor. It is therefore a strong similarity between the UPM method and the IEC 61508/62061 checklist and Humphreys method. UPM has been adapted as the standard approach in the UK nuclear industry, but does not seem to be well known in other sectors.

3.2 CCF data

Very few data sources for CCF data are available, at least in the petroleum industry. The nuclear industry has given CCFs more attention and carried out several CCF data collection projects to build generic reliability data bases on CCFs. Similar initiatives have been limited in the petroleum industry.

3.2.1 ICDE data base

The nuclear industry has been a pioneer in the study of CCFs (NUREG/CR-5485 [1998], NUREG/CR-6268 [2007], NEA [2004], NEA [2014]). Several guidelines have been developed for qualitative and quantitative analysis of CCFs. Many analyses of CCF data that give insight into causes of CCFs have also been published.

In a recent report the International Common Cause Data Exchange (ICDE) project has been described [NEA 2014]. The ICDE project was initiated in 1994 and collects and analyses CCF event data from the nuclear

industry in nine countries. Since April 1998, the project has been operated by the Nuclear Energy Agency (NEA). The objectives of the ICDE project are to:

1. Collect and analyse CCF events on a long term basis so as to better understand such events, their causes, and their prevention.
2. Generate qualitative insights into the root causes of CCF events which can then be used to derive approaches or mechanisms for their prevention or for mitigating their consequences.
3. Establish a mechanism for the efficient feedback of experience gained in connection with CCF phenomena, including the development of defences against their occurrence, such as indicators for risk based inspections.
4. Generate quantitative insights and record event attributes to facilitate quantification of CCF frequencies in member countries.
5. Use the ICDE data to estimate CCF parameters.

Various summary reports are available on collection and analysis of CCF of e.g., safety and relief valves, check valves and level measurements, and these may be accessed via the ICDE webpage http://www.oecd-nea.org/jointproj/icde.html . ICDE also gives general recommendations regarding classification of CCF data, for example regarding coupling factors, root causes and detection methods.

3.2.2 SKI reports

SKI (Swedish Nuclear Power Inspectorate) has published several reports investigating CCFs in boiling water reactors (BWR). In particular, SKI [1992] gives field data on safety/relief valves from different BWR generators located in Sweden. The database contains about 200 events, and failures are classified according to severity, failure mode, detection method, and which part of the component that failed. Failure cause is given, and the multiple events are classified as “complete CCFs”, “potential CCFs” or “recurring faults”.

3.3 Beta-factor estimators

Estimation of the β in the beta-factor model could be challenging. In principle we should first define the "CCF groups", specifying that a "true" CCF event has occurred only if two or more components within such a group fail "simultaneously". Usually we let the CCF groups consist of identical components within the same system (or safety function). However, it might be a problem that the failure data are not sufficiently detailed in order to decide with certainty whether the components failing in an event due to a common cause, actually belong to the same system.

Further, another problem is that – according to the beta- factor model – *all* components of such a CCF group will fail when a CCF occurs. That is, either there is a single (independent) failure, or we have a CCF event where *all* components of CCF group fail. So, if for instance, the CCF group has n=4 components, then, according to the beta-factor model, a CCF event with either two or three components failing *cannot* occur. However, in practice we get observations where these events actually do occur, and we have to do some compromising, actually leading to "illogical" estimates.

Below we first present the NUREG estimators for the β of DU failures, and next a β estimator based on the PDS method is discussed.

3.3.1 NUREG estimators

Let N_{DU} be the total number of DU failures experienced for a certain population. Further, let $N_{DU,CCF}$ be the total number of DU failures included in all CCF events having occurred. A recognized estimator, NUREG/CR-4780 [1988], now equals:

$$\hat{\beta}_1 = \frac{N_{DU,CCF}}{N_{DU}} \quad (1)$$

As discussed in Section 3.1, in the failure reviews simultaneous failures of two (or more) components have been classified as CCF events, although the components do not necessarily belong to the same safety function. Therefore, the above estimator will be rather conservative when estimating beta-factors in general.

A more appropriate estimate for the beta-factor value may be [NUREG/CR|-4780 1988]:

$$\hat{\beta}_2 = \frac{2 \cdot N_{CCF}}{N_{DU,I} + 2 \cdot N_{CCF}} \quad (2)$$

Here, N_{CCF} is the number of observed CCF events (regardless of number of DU failures in each CCF event), and $N_{DU,I}$ are the independent DU-failures, and thus $N_{DU} = N_{DU,I} + N_{DU,CCF}$. This estimate *assumes* that each CCF event results in failures of two components; i.e. $N_{DU,CCF}$ in eq. (1) is replaced by $2N_{CCF}$, which is usually smaller than $N_{DU,CCF}$. This approach may be considered non-conservative since all CCF events that include more than two failures are only counted as double failures.

Note that neither of the two NUREG estimators specifically requires that a CCF event shall affect components of the same safety function or system. When components fail due to the same cause, this will be considered to be a CCF event, also when the components belong to different systems or functions.

Numerical example – NUREG estimators

Based on the review of level transmitters, (a total population of 346 transmitters), 54 components had a DU failure. 13 of these failures occurred in CCF events, implying that the number of independent DU failures was 41. So $N_{DU} = 54$, with no. of single failures, $N_{DU,I} = 41$, and $N_{DU,CCF} = 13$ components fail due to CCF. Further, the number of CCF events equals $N_{CCF} = 3$. In these three events, respectively, 9, 2 and 2 components failed, (giving the total of 13 failed components). The data do not specify which loops are affected by the CCF events, but this information is however not required in the NUREG estimator. The estimates become:

$$\hat{\beta}_1 = \frac{13}{54} \approx 0.24$$

$$\hat{\beta}_2 = \frac{2 \cdot 3}{41 + 2 \cdot 3} \approx 0.13$$

3.3.2 PDS related estimators

As discussed earlier in the report, the β-factor can for a duplex system be interpreted as the fraction of failures of a single component that causes both components of the redundant pair to fail due to a CCF. However, in the PDS model the β-factor can be given a similar interpretation in any system: Given that one specific of the redundant components has failed, β is the probability that another specific component fails "at the same time" (*i.e.* due to a CCF). This coincides with the standard β-factor definition for a system with two components, but not otherwise. In the standard β-factor model a CCF is assumed to affect *all* the redundant components. In the PDS model, modification factors (C_{MooN}-factors) are introduced to allow any number of components to fail in a CCF of any voting configuration, see e.g. [Hauge et.al. 2013]. As a result of this alternative definition of β, a somewhat different estimation procedure may be considered for the β.

The estimation of β was considered in Hokstad [2004], and an estimate was provided for the case of systems with the same number of components. Now let:

n = Number of redundant components in system/group - usually not equal to the entire population N

K = Number of failure events, i.e. the number of discrete events including one or more failures

Y_j = Number of failed components (failure multiplicity) of failure event j, (j= 1, 2, ..., K),

then the MLE (maximum likelihood estimate) was found equal to[1]

$$\hat{\beta}_{MLE,K} = \frac{\sum_{j=1}^{K} Y_j(Y_j-1)}{(n-1)\sum_{j=1}^{K} Y_j} \quad (3a)$$

Note that if there is just one observation (with n components, where Y_1 of these have failed) the estimator becomes:

$$\hat{\beta}_{MLE,1} = \frac{Y_1-1}{n-1} \quad (3b)$$

which is the rather intuitive estimate based on one observation; (given that one specific of the n components have failed, the given observation will provide the estimate (Y_1-1)/(n-1) for the probability that an arbitrary of the other n-1 components also fails). The expression (3a) can be seen as a weighting of the individual estimates, using weights:

$c_j = Y_j / \Sigma_i Y_i, j = 1, 2, \ldots K.$

When we have observations with different n's, the situation is more complex, but was treated in Hokstad et al [2006], giving an expression, which in our current notation can be written:

$$\hat{\beta}_3 = \frac{\sum_{j=1}^{K} Y_j(Y_j-1)/\,[n_j(n_j-1)]}{\sum_{j=1}^{K} Y_j\,/\,n_j} \quad (4a)$$

Note that we can write this as

$$\hat{\beta}_3 = \sum_{j=1}^{K} c_j \frac{Y_j-1}{n_j-1} \quad (4b)$$

That is $\hat{\beta}_3$ represents a weighting of the above "intuitive" estimates (Y_j -1)/(n_j-1), cf. eq. (3b), using weights

$$c_j = \frac{Y_j/n_j}{\sum_{i=1}^{K} Y_i/n_i} \quad j = 1, 2, \ldots, K$$

We note that $\hat{\beta}_3$ reduces to $\hat{\beta}_{MLE,K}$ when all n_j are equal to *n*.

Numerical example – PDS estimators

Below we will use the same example as above with level transmitters, where we had 54 DU failures of which 13 were part of a CCF event and 41 of the failures were single (independent) events.

[1] In Hokstad [2004] the observations were expressed by other random variables, so the estimator there *appears* different from this formula, if the reader visits the article.

For estimating $\hat{\beta}_3$ we now need to define the parameters n_j, K and Y_j.

We will start with K: When originally classifying the failures, there were three CCF events with 9, 2 and 2 DU failures respectively. In addition we had the single failure events (41). Thus, K=44.

Defining n_j is somewhat more challenging due to how the data has been registered and collected. The CCF data has been collected from six installation with level transmitter populations from some 30 -140 components. For a given installation many of the transmitters will be single, other transmitters will be redundant (1oo2) and some transmitters may even be triplicated (2oo3). This information, i.e. how the components are "looped" together, is however not explicitly known. We therefore have to make some assumptions about the size of each component "group" within which the CCF events have been observed. Based on the observed CCF events, we see that these events have typically occurred for components that are physically located "close" to each other. We will therefore assume that the CCF event with most failures (for level transmitters this equals 9) is dimensioning, in the sense that all component groups for which a single or a multiple failure has occurred is assumed to include 9 components (a similar assumption has been made for all different equipment types).

Summarising, we assume that 41 single DU failures have occurred and three CCFs with 9, 2 and 2 failures each. The number of *failure events K* then becomes 41+3 = 44, with $n_1 = n_2 = \ldots\ldots = n_{44} = 9$ and: $Y_1 = Y_2 = \ldots = Y_{41} = 1$, $Y_{42} = 9$ and $Y_{43} = Y_{44} = 2$. Applying formula (3a) (or alternatively (4a)), this gives:

$$\hat{\beta}_3 = \frac{41 \cdot 1 \cdot 0 + 9 \cdot 8 + 2 \cdot 2 \cdot 1}{8 \cdot (41 \cdot 1 + 9 + 2 \cdot 2)} = 0.1759 = 18\,\%$$

It should be noted that the $\hat{\beta}_3$ estimator is rather sensitive to the assumptions made concerning group size (i.e. the n_j) and the number of failures in each component group (i.e. the Y_j).

4 Results from the operational reviews

Operational reviews of failures (maintenance notifications) reported during the last 3–4 years have been performed for six facilities. The operational reviews were facilitated by SINTEF and have involved personnel from key disciplines such as automation, safety, mechanical and process from the specific facility and company in question. Each notification was reviewed with the purpose of classifying failures according to IEC 61508 and considering CCFs in particular. The reviews have considered the following equipment groups:

Transmitters	**Detectors**	**Final elements**
Level transmitters	Point gas detectors	ESD and PSD valves
Pressure transmitters	Line gas detectors	ESD riser valves
Temperature transmitters	Flame detectors	Blowdown valves
Flow transmitters	Smoke detectors	Pressure Safety Valves
	Heat detectors	Fire dampers
		Deluge valves

Data on other components such as various emergency preparedness equipment, safety logic, watertight doors and fire doors have also been collected, but results for these equipment groups are not included in the present report, mainly due to insufficient amount of data and number of CCF events.

4.1 Operational reviews – why and how

Operational reviews – why?
The purpose of the operational reviews is to verify the performance of SIL rated equipment and to give recommendations related to future operation and data collection. All safety instrumented functions on a facility should be followed up. However, since a facility often comprises several hundred different loops or safety functions, it is assumed that follow-up of equipment groups is satisfactorily. If the failure rate for each equipment group is within the assumed failure rate from design, then all the safety loops are also assumed to fulfil their SIL requirements. Thus, each equipment group must be reviewed with respect to number of dangerous undetected (DU) failures over a specific period of time.

Since the CCF contribution often is dominating in PFD calculations for redundant systems, there should also be focus on identification of CCF during data collections. Some failures are "obvious" CCFs, while other failures may be more difficult to identify, e.g. due to time lags between occurrence and also between registration in the maintenance system.

Operational reviews – how?
The failure reviews have been carried out as 3–5 day meetings with representatives from the operators and SINTEF. As input to the meeting, a comprehensive Excel report has been prepared in advance, summarising all notifications registered in the maintenance system (e.g. SAP) for SIL rated equipment for the period under consideration. This Excel report is then applied as a basis for further failure classification during the meetings. Also, during the meetings there is always a maintenance system expert attending, so that it is possible to access the maintenance system and extract additional details if required (and if available).

The operational reviews have been facilitated by SINTEF and have involved key discipline personnel (automation, safety, mechanical, process, maintenance, etc.) from the specific facility and company in

question. Also, subject matter experts from the company have frequently been called upon during the meetings to solve ad hoc questions regarding the notifications and the equipment under consideration. A multidisciplinary group is important both with respect to quality assurance of the classifications and to achieve a collective understanding of status and challenges for the operator and personnel involved.

The work during and after the failure reviews has typically included:

- A thorough review of each notification within an equipment group, in particular with respect to detection method, failure mode, criticality of failure and failure cause.
- Depending on the failure mode and the detection method in particular, each failure has been classified according to IEC 61508 and IEC 61511; i.e., is the failure Safe (S), Dangerous Detected (DD) or Dangerous Undetected (DU)? Or is the registered notification considered not applicable (NA), i.e. a notification written against the tag but not affecting the main function of the component (e.g. removal of fire insulation on an ESD valve)
- A discussion of the identified failures, in particular those classified as DU and those that are potential CCFs;
- Preparing a summary report from the review that includes:
    - An estimate of updated failure rates based on the operational experience and the registered failures;
    - A description of experienced CCF events;
    - A consideration of whether these updated failure rates and experienced CCF events may justify or require certain measures such as less or more frequent functional testing, a more detailed root cause analysis, etc.;
    - Additional recommendations concerning future operation and maintenance, including measures related to improving the quality of failure reporting, improved testing procedures, improved operational procedures, and measures to reduce repeating failures and reduce the frequency of safety critical failures in general.

Ideally, an operational review should be performed once a year. Then the notifications are more recent and fresh in mind and thus easier to classify. Also, when performing the reviews annually the number of notifications to go through is more manageable - typically 300-600 during one year of operation on an average facility.

Operational reviews – some benefits

Operational reviews can be considered an integral part of the required barrier management in the operational phase. The overall aim of such reviews is to verify performance requirement from design and if necessary put measures in place to maintain the reliability of the component and thereby the safety on the facility.

During an operational review, a large amount of maintenance notifications are manually gone through by an expert team. As a result, the operator gets a very good overview of their safety critical equipment with respect to amount of failures, typical problem areas, possible improvement areas, etc.

The vendors are interested in operational feedback on the equipment they deliver, but often express frustration about lack of information from the operators. Thus, operational reviews can be seen as a good opportunity to systematically collect information on a component level which can be shared with the equipment manufacturer/vendor.

Finally, by collecting all these data, databases and handbooks such as OREDA and PDS will gradually improve and hopefully approach some typical values experienced by the industry. However, it should be

noted that the failure rates for most equipment groups varies significantly between facilities. Thus, facility specific factors should, whenever possible, be taken into account when considering future reliability performance and rate of CCFs.

Operational reviews – focus on CCF

The impression from the operational reviews is that limited attention is given to CCFs during daily plant operation and in particular during failure registration and follow-up. Many multiple failures revealed in these reviews were not identified or registered as CCFs, even if the same type of failure had been notified by several alarms or observed in many subsequent tests. This can be explained by inadequate investigation of the failure cause in the first place, inadequate overview of the failure history and maybe most importantly; a limited focus on CCFs in general.

4.2 Input data and estimated beta-factor values

In this section new beta-factor (β) values have been calculated based on the estimators discussed in section 3.3 and the data from the operational reviews. The background (or input) data from the operational reviews are summarised below.

Table 1 Input data from operational reviews for each equipment group

Equipment group	# Tags	Total operational time (hours)	N_{DU}	$N_{DU,I}$	N_{CCF}	$N_{DU,CCF}$
ESD/PSD valves (incl. riser ESD valves)	1120	2,52E+07	279	211	12	68
Blowdown valves	228	7,00E+06	73	56	4	17
Fire dampers	458	1,59E+07	44	21	6	23
Deluge valves	177	1,56E+06	5	3	1	2
PSVs	2356	7,45E+07	148	116	11	32
Gas detectors (point and line)	2239	6,51E+07	74	54	5	20
Flame detectors	1779	5,71E+07	23	15	3	8
Smoke detectors	3945	1,31E+08	41	30	5	11
Heat detectors	197	6,16E+06	1	1	0	0
Level transmitters	346	1,24E+07	54	41	3	13
Pressure transmitters	917	3,23E+07	44	31	4	13
Temperature transmitters	369	1,33E+07	3	3	0	0
Flow transmitters	114	3,89E+06	11	5	2	6

Here "Total operational time" is the aggregated operational hours for the entire population (across the six facilities), NDU is the total number of DU failures experienced for the population and NDU,I are 'independent' (single) DU-failures. NCCF is the number of registered CCF events (regardless of number of DU failures in each CCF event) and NDU,CCF is the total number of DU failures affected by a CCF event. E.g. for ESD/PSD valves, 12 CCF events were experienced involving a total of 68 valves.

Based on these data and the different estimators described in section 3.3, three estimates of the β-value have been calculated for each equipment group and the results are summarised in the table below. Note that for fire detectors (flame, smoke and heat) a common β-value has been estimated. For temperature and flow transmitters a common β-value has also been estimated and for deluge valves no separate β-value has been estimated, both due to inadequate amount of data.

Table 2 β-estimates for the equipment groups

Equipment group	$\hat{\beta}_1$	$\hat{\beta}_2$	$\hat{\beta}_3$ [1)]	New suggested (generic) β	β from PDS 2013 data handbook (for comparison)
ESD/PSD valves (incl. riser ESD valves)	24 %	10 %	16 %	**12 %**	5 %
Blowdown valves	23%	13%	15 %	**12 %**	5 %
Fire dampers	52 %	36 %	37 %	**20 %**	5 %
PSVs	22 %	16 %	11 %	**11 %**	5 %
Gas detectors (point and line)	27 %	16 %	16 %	**15 %**	7 %
Fire detectors (flame, smoke and heat)	29 %	26%	15 %	**15 %**	7 %
Level transmitters	24 %	13 %	18 %	**15 %**	6 %
Pressure transmitters	30 %	21 %	19 %	**15 %**	6 %
Temperature and flow transmitters	43 %	33 %	33 %	**15 %** [2)]	6 %

Note 1): The $\hat{\beta}_3$estimator has been calculated based on the assumption that the group size for which CCF events are registered equals the size of the CCF event with most failures. This is further discussed in section 3.3

Note 2): $\hat{\beta}_3$ has, due to few registered failures, been set equal to the β for level and pressure transmitters although estimated βs may indicate a somewhat higher value.

From the table we see that the type of estimator chosen and the underlying assumptions have a major influence on the estimated β-value. Neither $\hat{\beta}_1$ nor $\hat{\beta}_2$ explicitly takes into consideration the number of failures in each CCF events nor the size of the component group for which CCFs are registered. As discussed in section 3.3.2, the $\hat{\beta}_3$estimator has been calculated based on the assumption that the size of the component group (n_j) equals the size of the CCF event with most failures. Hence, the $\hat{\beta}_3$estimator is considered somewhat more "adjusted" to the underlying data material than the $\hat{\beta}_1$ and $\hat{\beta}_2$ estimators.

Concerning the new suggested β-values, the main approach has therefore been to give most credit to the $\hat{\beta}_3$estimates, but adjusted for several considerations as discussed below:

- From Table 2 it can be observed that the estimated βs for valves are generally lower than for the other equipment groups. It therefore seems reasonable to suggest lower β-values for valves than for detectors and transmitters.
- For ESD/PSD valves and blowdown valves the β-estimators differ slightly, but due to the somewhat limited number of CCF events for blowdown valves, the suggested β-value is the same for both equipment groups.
- For fire dampers the observed βs from the operational reviews are so high that it has been suggested to apply a lower value than the relevant $\hat{\beta}_3$estimate. As further discussed in section 4.3.3, design related issues, and in particular actuator design, contribute significantly towards fire damper failures.
- For fire and gas detectors the suggested β-value has been slightly reduced compared to the estimated values, one reason being that similar βs have traditionally been applied for fire and gas detectors in PDS.
- For process transmitters (level, pressure, temperature and flow) a common β-value of 15 % has been suggested although the β-estimators vary significantly between the different transmitter types. For some transmitters (temperature and flow in particular) there are a very limited amount of CCF observations and hence it seems reasonable to suggest a common value.

One important observation from the above table is that for all equipment groups under considerations the average observed β-values based on operational experience are significantly higher than what has traditionally been assumed in design calculations. It can therefore be concluded that more effort should be put into systematically analysing and reducing the extent of CCFs. It must also be considered whether the new knowledge about the β-value should affect design calculations and follow-up in operation.

It should however also be emphasised that the observed β-values vary significantly between the installations. On some installations no CCF events have been observed for certain equipment groups, whereas on other installations a very high rate of CCF events has been observed for certain equipment. For example, for ESD/PSD valves, where the accumulated number of observed DU failures and CCFs are highest, the estimated β-values between the installations vary from 5% up to the extreme case of 40 %. Another example is fire dampers, where on one installation all registered DU failures are CCFs. It is therefore important to adjust the generic (or average) estimates of β, based on installation specific conditions. For this purpose, equipment specific CCF checklists have been developed (ref. Chapter 5).

In the following sections, more detailed results for each equipment group is given in terms of

- A short description of the equipment's functionality and safety critical failure modes
- Experiences from operational reviews with respect to complete and potential CCF events

For each equipment type, the occurrence of CCFs has been related to three CCF categories; "Design properties", "Environmental control (internal and external)" and " Operation, maintenance and modifications". These CCF categories are further described in chapter 5.

4.3 Valves

4.3.1 Shutdown valves - topside ESD and PSD incl. riser ESD valves

The shutdown valves shall close upon a demand (i.e. a signal from the ESD and/or the PSD logic). Several of them also have requirements with respect to closing time and some of them to maximum leakage rate in closed position. The table below lists the critical failure modes for the shutdown valves (topside ESD and PSD valves) and the distribution of DU-failures and CCFs between the failure modes.

Table 3 Registered failures for ESD/PSD valves (riser ESD valves not included)

Failure mode		Comment	DU-failures	CCFs
Fail to close on demand	FTC	A few of the ESD valves also have a fail-to-open function (located at a spec-break) and therefore three fail to open (FTO) failures are also included.	100	7 CCF events
Delayed operation	DOP	The ESD and/or PSD valve has closed too slow.	153	3 CCF events
Leakage in closed position	LCP	Relevant only for those valves with leakage requirements and leakage rates above the leakage criterion for the particular valve.	13	1 CCF event

266 DU failures were observed for the shutdown valves from the six operational reviews. The total underlying population included 1065 valves (note that in Table 1, riser ESD valves are also included in the total population).

The 11 CCF events involved the following failures:

- 19 DU failures (delayed operation) were due to poor design of hydraulic connections resulting in too long closing times.
- 11 other DU failures (fail to close) were due to incorrect valve type for the specific application (fail-open valves installed in fail-close application).
- Additional six DU failures (fail to close) of another type of valve were due to poor design (these were not designed for the intended use and degraded immediately). All these valves had to be replaced.
- Six DU failures (delayed operation) were due to changing hydraulic oil viscosity (caused by temperature variations).
- Four DU failures (fail to close) were due to actuator capacity. The operation of these valves is normally assisted by pipeline pressure, but when testing with no (delta) pressure over the valve they were unable to close.
- Three DU failures (fail to close) were due to damaged gaskets combined with dirt from operation.
- Three DU failures (leakage in closed position) were due to a leakage problem with a group of valves of similar type. No root cause of this problem was revealed.
- Two DU failures (fail to close) were caused by wrong mounting of solenoid valves while modifying the control of these valves.
- Two DU failures (fail to close) on similar types of valves were detected simultaneously (unknown cause).
- Two DU failures (fail to close) were caused by corrosion on the actuator stem due to wrong material selection.

- An additional (unknown) number of DU failures (delayed operation) were due to inadequate bleed-off (wrong tuning of bleed-off valve).

In addition, several systematic failures were observed with a potential of causing CCF events. Examples of such potential CCFs include:

- Three valves failed due to cold temperatures and subsequent freezing possibly resulting in failures of other valves as well.
- One valve had stuck hand wheel due to rust. This could have affected similar valves in the same area.
- One valve was not sufficiently lubricated. Could have affected other valves due to same operational procedures and maintenance personnel.
- One valve was considered as vulnerable to corrosive attack due to weather exposure. If other valves were exposed to the same conditions, this could have resulted in a CCF.
- One valve did not function due to nitrogen leakage from the accumulators. Leakage was considered as a possible problem also for other similar valves, but not explicitly identified.
- One valve had been incorrectly adjusted during previous maintenance. Could have affected other valves due to same operational procedures and maintenance personnel.
- The design of an unknown number of valves was not fit for the intended operation (the spring was too weak to operate the valves adequately).

Based on the distribution of the complete and the potential CCF events, a distribution between the three CCF categories has been made. Some CCF events have more than one single cause and may therefore be distributed among several CCF categories. A subjective weighting of the three different CCF categories has however been made, where the general rule has been that the CCF events have been given the highest weight and the potential CCFs has been applied as additional input when establishing the distribution.

Table 4 Distribution of CCF categories for ESD/PSD valves

CCF categories	Distribution
Design properties	45%
Environmental control (internal and external)	20%
Operation, maintenance and modifications	35%

This distribution is an important input to the weights given in the equipment specific checklists.

Additional ESD riser valves

In addition to the topside ESD/PSD valves a total of 55 riser ESD valves have also been included in the operational reviews. In general they have the same functionality and critical failure modes as the other topside ESD/PSD valves. Riser ESD valves will normally have requirements to keep tight in closed position within a specified acceptable max leakage rate.

In total, 13 DU failures were observed for the riser ESD valves on the offshore facilities. Ten DU failures were related to the same notification and the same CCF: All ESD riser valves on a facility did not close upon low pressure due to oxidized aluminum gasket and defect (creased) spring. It should be noted that the valves did close under normal operation (upon pressure). The consequence, however, was that the valves did not close upon low pressure as required (since the ESD valves are required to close upon a LowLow pressure situation). All valves therefore had to be overhauled.

Due to limited number of DU failures and only one CCF, the distribution of failure modes and CCF CCF categories are assumed to be similar for riser ESD valves as for ESD/PSD shutdown valves. A common checklist therefore applies for PSD/ESD shutdown valves and riser ESD valves (ref. Table 16 and Appendix A.1.1).

4.3.2 Blowdown valves

Blowdown valves shall open upon signal/demand within a specified permitted time. Critical failure modes for blowdown valves include Fail to Open (FTO) and Delayed operation (DOP).

Failure modes

The table below lists the failure modes for the blowdown valves and the distribution of DU-failures and CCFs between the failure modes.

Table 5 Registered failures for blowdown valves

Failure mode		Comment	DU-failures	CCFs
Fail to open on demand	FTO	Include failures where valve does not open at all or valve does not open 100%.	36	2 CCF events
Delayed operation	DOP	Considering only delayed operation with respect to opening.	37	2 CCF events

In total, 73 failures were defined as DU failures for blowdown valves from the six operational reviews. The total population of blowdown valves included 228 valves.

The four CCF events involved the following failures:

- Two valves (functioning in pair) failed to open on the same test due to strongly corroded actuators.
- Three DOP-failures (on two distinct valves) were due to N_2 leakage from the accumulators caused by a failure related to the nitrogen pressure.
- Ten FTO-failures were also caused by too low supply air pressure due to leakage from the pneumatic tubing to accumulators. In a blowdown situation there would not have been sufficient air pressure to blowdown all the inventories (sequential blowdown).
- Two DOP-failures were revealed on the same test and were due to corrosive attack on ball. Also another FTO-failure was due to the same cause.

In addition, several systematic failures were observed with a potential of causing CCF events. Examples of such potential CCFs include:

- Two FTO-failures were due to limited operational pressure during testing (ref. previous failures on ESD valves due to limited differential pressure). Similar failures were observed on different facilities and/or at different times and can therefore only be considered as a potential CCF.
- One valve failed to open, probably due to ice or hydrate in valve.
- Three FTO-failures (on two distinct valves) were due to corrosive attack. Weather protections were installed, but the failures reoccurred and the effect of the weather protection seemed to be limited.
- Two valves failed to open due to a software error.
- One valve failed to open due to wrong mounting. Could have affected similar valves due to commonalities during installation

- One valve failed to open, and a quick-relief valve had to be installed in order for the blowdown valve to open. It was not registered that this had to be done on any other valves, but could have affected several valves.

Based on the distribution of the complete and the potential CCF events, a distribution between the three CCF categories has been made. Some CCF events have more than one single cause and may therefore be distributed among several CCF categories. A subjective weighting of the three different CCF categories has however been made, where the general rule has been that the CCF events have been given the highest weight and the potential CCFs has been applied as additional input when establishing the distribution. Note that the failures caused by too low supply air pressure due to leakage from the pneumatic tubing to accumulators has been divided between "design properties" and "operation, maintenance and modifications", since it has been assumed that improved maintenance of the pneumatic utility system could have prevented some of the failures.

Table 6 Distribution of CCF categories for blowdown valves

CCF categories	Distribution
Design properties	40%
Environmental control (internal and external)	25%
Operation, maintenance and modifications	35%

The checklist for blowdown valves is comparable to the checklist for the ESD/PSD valves, however with somewhat different weights. See Appendix A.1.2.

4.3.3 Fire dampers

The fire dampers shall close upon a signal/demand within the required closing time. The critical failure modes are fail to close (FTC) and delayed operation (DOP). Note that all failures registered on fire dampers were classified as FTC.

In total, 44 failures were defined as DU failures for fire dampers from the six operational reviews. 458 fire dampers made up the aggregated population from the six facilities.

Six CCF events were registered for the fire dampers. These involved the following failures:

- Six fire dampers on the same air inlet failed to close on tests. The cause was unclear, but "slowness in shafts" and need for lubrication was noted in the notifications
- The same six dampers failed during test two years later but the cause was not further investigated.
- Nine DU-failures were due to actuator / solenoid / damper motor not fit for operation. This involved three different CCF events (on two different facilities) with 4, 3 and 2 DU failures respectively. For most of the cases the actuator was replaced with a new type. For some of the dampers, additional problems were revealed on the damper motor and/or the solenoid as well.
- Two DU-failures revealed on the same tests were due to wrong mounting of the actuator (probably mounted at the same time and by the same operators).

In addition, a number of systematic failures were observed with a potential of causing CCF events. Examples of such potential CCFs include:

- Eight DU-failures (occurring at different times and facilities) were apparently due to lack of lubrication. If regular lubrication had been performed, all these dampers would probably have functioned upon demand/test.
- Two DU-failures may have been prevented if regular maintenance had been performed. Maintenance activities had probably been insufficient due to difficult access, i.e. inadequate maintainability.
- One fire damper did not close due to dirt. Could have affected other dampers as well.
- One fire damper did not close due to a design error (no further information was available from the notification).

Based on the number and distribution of the complete and the potential CCF events, a distribution between the three CCF categories has been made. Some CCF events have more than one single cause and have therefore been divided between several categories.

From the failure history it appears that latent errors from design play a more important part for fire dampers than for the valves discussed above. Also note that the sub-category "location" which in our scheme is part of "design properties" here becomes high due to the two registered failures of all six dampers on one air inlet. Environmental influences appear to play a more limited role with respect to critical fire damper failures.

Table 7 Distribution of CCF categories for fire dampers

CCF categories	Distribution
Design properties (incl. location)	50%
Environmental control (internal and external)	15%
Operation, maintenance and modifications	35%

The checklist for fire dampers is quite similar to the one for shutdown valves (and blowdown valves). A separate checklist for fire dampers have been suggested in Appendix A.1.3.

4.3.4 Deluge valves

Deluge valves shall open and release a specified amount of water upon a signal/demand. The critical failure modes for deluge valves is fail to open (FTO) and insufficient delivery of water (IDW). The most common failure mode is FTO, but some solenoid failures (ref. below) may result in IDW.

Only five DU failures have been revealed for deluge valves (including a population of 177 valves). One of the failures has been classified as a CCF; after maintenance work in the deluge cabinet the operator had forgotten to turn on the N_2 pressure after finishing the work. N_2 pressure is necessary in order to get water through the deluge valves. It is not known how many valves this failure actually did influence.

Most of the critical failures registered for the deluge valves seem to be related to solenoid failures. Thus, many DU-failures have (correctly) been registered against the deluge solenoids. Solenoid valves have not moved sufficiently, causing the deluge valve to fail.

Based on the limited number of DU failures and CCFs for deluge valves, a subjective distribution between the three CCF categories classes has been suggested. The suggested distribution of the CCF categories is based on the assumptions that a CCF will most probably be due to operational/maintenance failures or

environmental exposure (corrosion, freezing, etc.) and less probable "design properties" since little design related errors have been observed.

Table 8 Rough distribution of CCF categories for deluge valves

CCF categories	Distribution
Design properties	25%
Environmental control (internal and external)	35%
Operation, maintenance and modifications	40%

Due to lack of data, no separate CCF checklist has been suggested for deluge valves.

4.3.5 Pressure Safety Valves (PSV)

The PSVs shall open on a predefined set point. During testing of PSVs, a failure is usually registered if the valve does not open within 120% of the set point pressure. The critical failure mode for a PSV is thus fail to open (FTO).

In total, 148 failures were defined as DU failures for the facilities where PSV valves have been reviewed (constituting a total of 2356 PSVs).

11 CCF events were registered and involved the following failures:

- Seven of the *CCF events* comprised simultaneous failure (i.e. failure on the same test/demand) of PSVs located near each other (e.g., on the same vessel) without any further information about failure cause(s). One event involved DU-failures of six PSVs, one event involved three PSVs and five events involved DU-failures of two PSVs.
- One CCF event involved failure of five PSVs. The pilot exhaust lines from these valves were plugged.
- Two CCF events both involved a failure of three PSVs located near each other due to rust.
- Two PSVs located near each other failed to open due to medium inside the valve, probably from operational conditions.

Also, a number of systematic failures were observed with a potential of causing CCF events. Examples of such potential CCFs include:

- One PSV failed due to hydrate caused by loss of heat tracing. Could have affected other PSVs
- One PSV was filled with sand.
- One PSV had loose bolts.
- For one PSV the insulation was defect.
- Three PSVs (on two different facilities) had incorrect adjustments of set point.
- At least three PSVs failed (at different times and/or facilities) due to degraded O-rings (which were replaced).

As can be seen from the above descriptions, limited information has been found in the notifications regarding the cause of failures of PSVs. So even if the number of failures (and CCFs) is rather high, the quality of the data could nevertheless have been improved.

It should also be noted that some of the failures registered may be conservatively classified as DU due to the testing practice on some of the facilities; this test is based on the operating personnel's ability to hear when the PSV valve opens. If the PSV is placed in a noisy area, it may sometimes be difficult to confirm that the PSV opens, and a failure has conservatively been assumed by the operating personnel.

Based on the number and distribution of the complete and the potential CCF events, a distribution between the three CCF categories has been made. Some CCF events have more than one single cause and have therefore been divided between several CCF categories.

From the failure history it appears that internal and external environmental influences (sand, hydrates, corrosion, contaminations, etc.) seem to be an important cause of CCF and potential CCFs. Furthermore, the sub-category "location" which in our scheme is part of "design properties" becomes high due to several CCF events for PSVs located near each other. A somewhat more limited number of failures seem to be caused by operational/maintenance errors.

Table 9 Distribution of CCF categories for PSVs

CCF categories	Distribution
Design properties (incl. location)	40%
Environmental control (internal and external)	35%
Operation, maintenance and modifications	25%

A checklist for PSVs has been suggested in Appendix A.1.4.

4.4 Fire and gas detectors

4.4.1 Point gas detectors

Functionality

Point gas detectors shall detect the presence of gas at specified concentration(s) and provide a signal to the F&G logic. Besides hydrocarbon gas, some H_2S, CO_2 and O_2 detectors are also included in the sample. The critical failure modes for gas detectors are somewhat difficult to consistently define since different classification schemes exist, but may include (ref. ISO 14224 [2006]); 'fail to function on demand' (FTF), 'no output' (NOO), 'low output (LOO) and 'wrong measurement' (WRM).

The table below lists the registered failure modes for the point gas detectors and the distribution of DU-failures and CCFs between the failure modes. In total, 59 failures were defined as DU failures for point gas detectors from the six operational reviews. This included a total population of 1341 point gas detectors.

Table 10 Registered failures for point gas detectors

Failure mode		Comment	DU-failures	CCFs
Fail to function / no output ("dead")	FTF NOO	None of these failures have been revealed by diagnostic, since it is dangerous *undetected* failures.	12	1 CCF event
Low output (incl. wrong/unsteady measurement)	LOO WRM		47	3 CCF events

The four registered CCFs registered involved the following failures:

- Ten DU failures (wrong measurement) were due to poor design of a detector type, so that all the detectors had to be replaced.
- Four DU failures (wrong measurement) were all detected at the same time by random observations (no alarm). The four detectors had frozen measurement and had to be replaced. Cause unknown.
- Two detectors of an old design (located in same area) were exposed to corrosive attack (unknown failure mode, but assumed FTF / NOO).
- One DU failure (and possible up to around ten additional DU-failures) was due to wrong calibration caused by failure in the test procedure.

Also, a number of systematic failures were observed with a potential of causing CCF events. Examples of such potential CCFs include:

- Some ten detectors were most likely subject to wrong calibration caused by operator error and/or failure in the test procedure.
- Four detectors did not function due to environmental influences causing dirty lenses. Two failures were revealed (by observations in CCR) one day and two failures were revealed (by observations in CCR) another day.
- For one gas detector a filter was clogged. Filter check was originally not part of the operator's maintenance procedures, and based on this event the maintenance procedures were updated. Clogged filter was not identified for other detectors of this type but could have affected other components.
- Two other detectors also failed due to clogged filters (another type of detector/filter).
- One detector did not function due to poor design of the mirror. Similar design of mirrors in other detectors could have resulted in a CCF.
- One failure was due to poor design of a steel filter on a type of H_2S detectors, resulting in excessive corrosion. No other failures due to corrosive steel filter were identified for the same detector type.
- One detector was found to be miss-calibrated. Could have affected other detectors due same procedures and/or maintenance personnel.

From the failure history we see that failures related to incorrect calibration and wrong measurements are important causes. Also, design related properties including location, and environmental influences seem to give significant contributions. Based on the number and distribution of the complete and the potential CCF events, a distribution between the three CCF categories has been made. Some CCF events have more than one single cause and have therefore been distributed between several CCF categories. Furthermore note that for several DU-failures, the underlying failure cause was unknown, so some subjective considerations have had to be made.

Table 11 Distribution of CCF categories for point gas detectors

CCF categories	Distribution
Design properties (incl. location)	35%
Environmental control (internal and external)	30%
Operation, maintenance and modifications	35%

A common checklist for point gas detectors and line gas detectors are given in Appendix A.2.1.

4.4.2 Line gas detectors

Line gas detectors shall detect the presence of gas in the sight line and provide a signal to the F&G logic. Critical failure modes are the same as for point gas detectors.

The table below lists the failure modes for the line gas detectors and the distribution of DU-failures and complete CCFs between the failure modes.

Table 12 Registered failures for Line gas detectors

Failure mode		Comment	DU-failures	CCFs
Fail to function / no output ("dead")	FTF NOO	Note that failures revealed during test where the detector does not respond upon gas could be either FTF/NOO or LOO.	6	1 CCF event
Low output (incl. wrong/unsteady measurement)	LOO		9	-

In total, 15 failures were defined as DU failures for line gas detectors from the six operational reviews. The total sample included 898 line gas detectors.

Only one CCF event was registered and involved several detectors (exact number unknown). The failure was due to wrong type of cabling (not intrinsically safe) and physical damage of this cable.

A number of systematic failures were observed with a potential of causing CCF events. Examples of such potential CCFs include:

- Three detectors located near each other did not respond upon testing on the same day (possible CCF, but cause unknown).
- One detector was incorrectly calibrated either during installation, modification or maintenance. Could have affected more detectors.
- One detector had a junction box filled with water; potential CCF due to either design and/or environmental influence. A rather high number of DD failures related to water or moist in junction boxes have been registered during the operational reviews. At one installation this was due to poor design and inadequate maintenance/inspection of the junction boxes; the water intrusions were due to decayed O-rings/plug on top of the junction boxes, and due to this it was focused on use of silicon instead of tightening up the plug on top of the junction boxes to reduce the extent of water intrusion.
- One detector was incorrectly mounted.
- Two detectors gave unsteady measurements on the same test. Cause unknown
- One detector failed due to wrong type of detector for the particular application.

Note that some of the potential CCFs have unknown failure modes and are not included in the failure mode table above.

For many of the DU-failures and some of the potential CCFs we were not able to classify them with respect to underlying failure cause. Therefore, the same distribution of CCF category as for point gas detectors (ref. Table 11) has been assumed. Also too limited data to estimate a separate beta-factor for line gas detectors has been available.

A common checklist for point gas detectors and line gas detectors are given in Appendix A.2.1.

4.4.3 Flame detectors

Flame detectors shall detect the presence of flame upon a demand and give a signal to the F&G logic.
As for gas detectors, the critical failure modes for flame detectors are somewhat difficult to consistently define since different classification schemes exist, but may include (ref. [ISO14224, 2006]); 'fail to function on demand' (FTF), 'no output' (NOO) and 'low output (LOO). It is however often difficult to distinguish between these failure modes from the operational data and the descriptions in the notifications.

In total, 23 failures were defined as DU failures for flame detectors from the six operational reviews. This included a total of 1780 detectors, thus implying a high reliability of such detectors.

In addition, 34 failures classified as DU were registered at one installation. These were all related to an old detector type of which all were replaced. The old detectors did not give any (diagnostic) alarm as they should, and failures were detected only upon tests or demands. These 34 DU-failures are not included. However, they could have been considered as a CCF due to poor design. Also, one DU burn-in failure has been removed from the data.

The CCFs registered involved the following failure:

- Four DU failures (failure of two components on two distinct facilities) were due to lack of competence concerning dipswitches, i.e. positions of the various dipswitches corresponding to the detection range of the detector.
- Two DU failures (located nearby) were due to loose wires, probably introduced during maintenance activities.
- Two DU failures were due to loose wires resulting in too low output of two detectors (electrical failure).

Some systematic failures were observed with a potential of causing CCF events. Examples of such potential CCFs include:

- Several detectors located near each other were exposed to snow and ice during winter. One DU failure was revealed.
- One DU failure was due to wrong/old type of detector not fit for the operation. Could have involved more detectors of similar make.
- One DU failure was due to a missing test after maintenance and modifications.
- One DU failure was due to water intrusion in the detector (condensation from water on the inside of the lens). May be related to both maintenance/operation and to poor design.
- Two DU failures were due to failure in electronics revealed within two weeks on two detectors located near each other.

Based on the limited number of observed CCFs we conclude that failures caused by maintenance and operation activities seem to play an important part. Design related properties (incl. location) also seem to have a relatively high influence, whereas environmental influences seem to be a somewhat more limited failure cause for flame detectors. Two CCF events were both due to loose wires but it is difficult to determine whether this is solely related to inadequate maintenance or also caused by poor design. These events have therefore been divided between the two CCF categories. Based on the number and distribution of the complete and the potential CCF events, a distribution between the three CCF categories has been suggested.

Table 12 Distribution of CCF categories for flame detectors

CCF categories	Distribution
Design properties (incl. location)	35%
Environmental control (internal and external)	25%
Operation, maintenance and modifications	40%

A separate checklist for flame detectors has not yet developed, basically due to inadequate data available. Rather, a common checklist for fire detectors is suggested, ref. Appendix A.2.2.

4.4.4 Smoke detectors

Smoke detectors shall detect the presence of smoke and send a signal to the F&G logic. As for flame detectors relevant failure modes are 'fail to function on demand' (FTF), 'no output' (NOO) and 'low output (LOO).

From the operational data it has been difficult to distinguish between these failure modes as the information from the notifications are rather limited. Most of the notifications do not contain any information beyond the fact that the detector has been replaced.

Based on a total population of some 3945 flame detectors, 41 failures were defined as DU failures for smoke detectors from the six operational reviews. It should be noted that 25 of these were revealed on the same installation. These detectors had limited diagnostics and did not give any alarm when they had failed.

Due to inadequate information given in the notifications and the fact that failed detectors have mainly been replaced it is difficult to estimate the β-value and to provide a distribution of CCF categories. It seems like improving diagnostic is an important measure in order to reduce the number of failures. Thus, the CCF category "Design" seems to be of high importance. Also environmental influences have caused some failures, in particular for detectors located in areas with polluted air. Areas exposed to pollution could e.g. be generator rooms. Not all situations with polluted optics have been revealed by diagnostic.

In total, five CCFs can be identified when looking into detectors located in the same room and which failed upon tests the same day. These CCF events involved the following failure:

- Four CCF events with two DU failures each.
- One CCF event with three DU failures.

Based on this the following rough distribution is suggested:

Table 13 Rough distribution of CCF categories for smoke detectors

CCF categories	Distribution
Design properties (incl. location)	40%
Environmental control (internal and external)	30%
Operation, maintenance and modifications	30%

A separate checklist for smoke detectors has not yet developed, basically due to inadequate data available. Rather, a common checklist for fire detectors is given, ref. Appendix A.2.2.

4.4.5 Heat detectors

Only one DU failure (on a facility with 94 heat detectors) has been revealed for heat detectors. The entire population of heat detectors only included some 200 detectors, hence limited operational experience with heat detectors have been available.

No separate checklists or β-value estimates have therefore been suggested for heat detectors but a common checklist for fire detectors is suggested, ref. Appendix A.2.2.

4.5 Process transmitters

4.5.1 Level transmitters

A level transmitter shall measure the level in a vessel or tank, and send a signal to the logic when the level is outside the set-point limits. Critical failure modes for process transmitters are not uniquely defined among the operators and installations, but may include 'fail to function on demand' (FTF), 'frozen measurement' (FRM), 'no measurement / out of range' (NOM), 'drifting measurement', 'erratic output' (ERO), 'low output' (LOO) and 'high output' (HIO).

The table below lists the assessed failure modes for the level transmitters and the distribution of DU-failures and CCF events between the failure modes.

Failure mode		DU-failures	CCFs
Fail to function / Frozen measurement / No measurement	FTF / FRM / NOM	7	No CCF events
Erratic output / Wrong measurement	ERO / WRM	41	3 CCF events
Drifting measurement	DRM	4	No CCF events

In total, 54 failures were defined as DU failures for level transmitters from the six operational reviews. The total population included 346 level transmitters.

The three registered CCFs involved:

- Nine DU failures (wrong measurement) were due to wrong measuring principle for the specific application, resulting in wrong level measurements (revealed randomly or on tests). It should be noted that many vessels have very challenging measurement conditions, and a suitable level measurement principle working for all operational situations may therefore be hard to find.
- Two DU failures (wrong measurement) were due to wrong data values in their data sheet.
- DU failures (wrong measurement) of two transmitters located near each other, both revealed at the same time (by observations in control room).

Several systematic failures were observed with a potential of causing CCF events. Examples of such potential CCFs include:

- Five transmitters were exposed to cold temperatures resulting in icing/hydrate of impulse lines. None of these however occurred at the same time.
- Three transmitter located on the same tank had similar problems (unknown cause). One transmitter has been replaced, but there was no information about replacement of the other transmitters.
- One transmitter failed due to incorrect mounting. If the same had occurred for other transmitters, e.g., due to same operational procedures or personnel, this could have resulted in a CCF.
- One transmitter was exposed to an electrical failure. This type of failure could also have influenced other transmitters, but only one failure was registered.

A main challenge with level transmitters is the fact that it is difficult to select the right type of measurement principle for the varying process conditions. Also, experience from operational reviews indicate that the correct understanding of the functionality and calibration/measurement issues related to level transmitters can be challenging. This can also be seen from the few observed CCFs and potential CCFs; the events often have more than one single cause and are often a combination of failures from the design phase and maintenance/operational challenges. Environmental influences also seem to be a contributor, but with a lower weight.

Table 14 Distribution of CCF categories for level transmitters

CCF categories	Distribution
Design properties (incl. location)	40%
Environmental control (internal and external)	25%
Operation, maintenance and modifications	35%

A checklist for process transmitters has not yet been developed

4.5.2 Pressure transmitters

Pressure transmitters shall measure the pressure in a vessel, tank or pipe segment, and send a signal to the logic when the pressure is outside the set-point limits. Possible failure modes are the same as for the level transmitters. However, it is difficult to distinguish between these failure modes from the operational data as the information from the notifications are rather limited.

In total, 44 failures were defined as DU failures for pressure transmitters from the six operational reviews. This was based on a total population of 917 pressure transmitters.

The four registered CCFs involved:

- Five DU failures (wrong measurement) were due to unclear measuring principles and incorrect calibration caused by some special challenges related to the measurement area and zero-point setting for these transmitters.
- Three DU failures were due to clogged tubing, two were detected on test on the same day and the third was detected on a test 2-3 weeks earlier. All three transmitters were located near each other. Probably the failure was due to internal environmental influences/contaminations.
- Two DU failures (wrong measurement) were detected casually as they both showed a lower value in the central control room than was displayed on the manometers. The cause of the failure is unknown.

- Three DU failures (wrong measurement) were due to incorrect set up of the measuring range for those transmitters; the measuring range set up was opposite to the intended.

Some examples of potential CCFs included:

- Four transmitters were exposed to cold temperatures resulting in icing/hydrate of impulse lines. These did not occur at the same time. One of them was due to an inadequate heating element.
- Four transmitters experienced clogged impulse lines due to crude, sand or settlings.
- One transmitter had frozen value due to a programming error. Could have affected more transmitters.

Based on the relatively few CCF events and potential CCFs a distribution of CCF categories has been suggested. From the events we see that operational/maintenance related problems related to set up and calibration play an important part as well as internal and external environmental challenges. Design related issues seem to have a somewhat lower influence.

Table 15 Distribution of CCF categories for pressure transmitters

CCF categories	Distribution
Design properties (incl. location)	25%
Environmental control (internal and external)	35%
Operation, maintenance and modifications	40%

A checklist for process transmitters has not yet been developed.

4.5.3 Temperature transmitters

Only three failures have been classified as DU for temperature transmitters, all of them conservatively assumed to be DU due to limited information concerning detection method or type of failure. The total population of temperature transmitters included 369 transmitters. Hence limited operational experience with temperature transmitters has been available and no separate β-value estimate has therefore been suggested.

4.5.4 Flow transmitters

11 DU failures have been revealed for flow transmitters based on a total population of 114 transmitters. Two CCF events were registered and involved:

- Four DU-failures were due to an incorrect assumption made during the design phase; the actual flow in the line was lower than assumed during design.
- Two DU-failures were due to unstable measurement at the same time caused by low temperatures.

Examples of potential CCFs include:

- One DU failure was due to wrong mounting of the transmitter. Could have affected more transmitters.
- One failure was conservatively classified as DU; the observed transmitter was still in "test modus" since last test, but it is uncertain if the detector would have functioned or not during a possible demand.

Due to the limited operational experience with temperature transmitters, no separate β-value estimate has been suggested.

4.6 Additional observations and measures from operational reviews

As seen from the above discussions several typical CCFs have been revealed during the failure reviews. It is worth noting that for some equipment groups, the experienced number of CCFs is higher than assumed from calculations in design. It is therefore important to focus on possible CCFs, to reveal their causes and to implement measures to reduce the probability of occurrences of CCFs.

Some general observations from the reviews related to CCFs are:

- Identification and classification of CCFs was sometimes challenging due to lack of details in many of the notifications. In particular there is often limited information in the notifications to enable a clear identification of failure cause and possible coupling factors. Lack of details in the notifications was however partly compensated by the expert panel discussions as part of the operational reviews where details underlying the notifications were discussed.
- For some equipment groups the total number of revealed CCFs was rather high compared to what can be expected from beta-factor values that are usually applied in reliability calculations.
- As for failure rates, the rate of CCFs are indeed facility specific. Identical CCF events were generally not observed across several facilities. This can probably also be related to the relatively limited number of available data on CCFs.

During the operational reviews, the following measures have been suggested to reduce the probability of CCFs and systematic failures:

- *Quality assurance of maintenance activities*: A typical failure type revealed on several of the facilities and for more than one equipment group, was related to incorrect mounting, incorrect set points, incorrect adjustment, etc. on previous test, maintenance activity or modification. Examples of such failures are incorrect mounting of valves and incorrect adjustments of detectors and transmitters. If such failures are revealed on the next test or PM, the component has in reality been non-functional during the entire test interval and thus gives a serious unavailability contribution. By improving the proof test procedures and the quality assurance of maintenance and test activities, this type of failure will become less frequent. Obviously training of operators to enhance their competency is another important measure.

- *Follow-up of level transmitters:* Unstable transmitters, incorrect measurements of transmitters and false alarms give process upsets and/or can lead to undesired events. Many of the failures on level transmitters were related to drifting due to variation in the density of the medium in the vessels under consideration. Unless regular calibration checks (checks of zero point) are performed, the zero point may have drifted such that the transmitter is unable to detect either LL or HH (depending on the direction of the drifting), which again may lead to a latent DU failure.
    - It is therefore important to regularly perform zero point checks in order to reduce the time where transmitters are not able to detect LL or HH.
    - In addition, it is recommended to evaluate which alarms (e.g. deviation alarms) that possibly could have been implemented.
    - Also, level transmitters with pancakes may be exposed to dirt, etc. from operation resulting in clogged drains / dirty pancakes. For exposed transmitters, regular draining against the pancakes is recommended to be performed.

  - Generally, it is also important to improve the operators general understanding of the level transmitters functionality and calibration attributes. For some type of level transmitters, such as e.g. radioactive transmitters, it has been observed that misunderstanding and lack of competency have caused several transmitter failures.

- *Avoidance of clogged impulse lines for pressure transmitters:* Several DU-failures registered for the pressure transmitters were related to clogged impulse lines, either due to dirt/settlings/hydrate or due to heating element failures. Thus it is important
  - To identify transmitters exposed to hydrate, either due to process vulnerabilities or from environmental influence, and to perform regular control of these transmitters exposed to dirt/icing.
  - To follow up heat tracing and heater elements or even categorize this type of equipment as safety critical and/or follow up the equipment as if it was safety critical.

- *Reduction of excessive response times of ESD, PSD and blowdown valves:* The number of DU failures related to excessive response times for ESD, PSD and blowdown valves is quite high, and indicates that some kind of systematic follow-up action should be defined. Excessive response times of valves are sometimes "corrected" by simply running the valves several times until it performs satisfactorily (and are then simply put back into operation again). This remedy is only provisional and will not remove the failure cause, which will again cause repeating failures. It is therefore important that the actual failure causes are identified (root cause analysis) and that risk reducing measures are implemented to prevent repeating failures. It is also important to have a clear understanding and knowledge of how the max/min response times are defined and the background for these limits.

- *Implementation of root cause analysis:* The notifications often give insufficient information about the direct causes and even more so the underlying causes of the failure. Then it is difficult to suggest and implement measures to avoid the failure from reoccurring or affecting other similar components. Improved failure cause investigation will contribute to reduce the number of repeating failures and also to reduce CCFs. Actually, the (root) causes should be identified and the correct measures be implemented before the component can resume "as good as new".

- *Improving calibration of detectors and transmitters:* Several failures have been related to incorrect calibration/adjustments of detectors and transmitters, either due to lack of competence, improper/incorrect test procedures or procedures not being followed. On one of the facilities, special training has been implemented where the focus has been placed on proper calibration of gas detectors, and it seems like this effort has resulted in less calibration errors on the facility. It is therefore recommended to implement more such training, especially for process transmitters. In addition the calibration procedures should be regularly evaluated.

- *Avoidance of water intrusion in junction boxes:* Water intrusion in junction boxes and instruments has been observed for several equipment types for some of the facilities. In particular, water intrusion into junction boxes of detectors has been a repeating issue. This results in reduced functionality (and detectable failures) of the associated equipment but has in some cases also caused DU failures. Water intrusion into junction boxes was on one of the facilities caused by decayed O-rings/plug on top of the boxes. It was then focused on use of silicon instead of tightening up the plug on top of the junction boxes to reduce the frequency of water intrusion. This measure may be relevant for other facilities with similar problems.

- *Detection of earth faults:* Several earth faults have been registered throughout the operational reviews, and the criticality classification of this type of failure has varied; if a dedicated earth fault alarm is given – the failure has been classified as safe, if a more "general" alarm has been given – the failure has been classified as dangerous. By "general" we here mean that the alarm is not addressable to a specific detector (only a common earth fault alarm for the entire loop is given) or a specific fault (e.g. earth fault). E.g. an earth fault on a single detector will typically give a common alarm and it is not necessarily straightforward to identify which detector (s) that has resulted in the alarm. Although being a type of detected failure, data from the reviews indicate that such "general" alarms have a tendency of sometimes being postponed before resolved (causing unavailability of some components). It is therefore important to have particular focus on earth fault alarms and to resolve them once they occur.

- *Inadequate actuator design:* Actuators for several types of valves have been replaced due to problems with the actuators, i.e. a cause that can usually be traced back to the design phase. A repeating cause seems to be that the actuators have been too weak (insufficient actuator force) for all relevant operational conditions or the material selection for the actuator has not been fit for purpose.

- *Increased focus on repair of detected failures*: During the operational reviews a lot of dangerous detected (DD) failures including CCFs related to DD failures have been revealed. The contribution from such failures is often taken to be negligible since DD failures are assumed repaired immediately or it is assumed that the system/process is shut down. Results from the operational reviews have revealed that this may not always be the case; such failures often remain unresolved for more than the "accepted" number of days (typically 5 days in the maintenance system). In other words, DD failures (and associated CCFs) can give a higher contribution to unavailability than assumed during design and it is therefore important to focus on resolving such failures within the specified time limits.

Based on the above discussion and the results presented in this chapter, it can easily be concluded that systematic failures and CCFs deserves more attention in the operational phase. With respect to CCFs reliability calculations imply that their contribution towards system unavailability is often significant if not even dominating in redundant configurations. However, SIL analysis performed during design is not sufficient to ensure control with the CCFs unless these failures are also followed up during operation. Nevertheless, the operational reviews have revealed that the attention and focus on CCFs and systematic failures are somewhat limited during operation. It is therefore important to increase the awareness of systematic failures and CCFs among maintenance and operating personnel and to ensure that defense measures are implemented to avoid such failures.

As part (and start) of this it is important that experienced failures are more thoroughly and detailed recorded in the maintenance system. In addition to detection method, failure mode, failure cause and failure consequence, CCFs should be given a separate CCF-code in the failure recording. One maintenance system for instance has a separate code called "common cause/mode failure" under the "failure mechanism" category. Increased use of the free text field is also important to facilitate a proper root cause analysis.

Another important observation from the operational reviews is the fact that the observed CCFs are usually plant specific and may be due to a particular design, a particular operating practice or specific environmental conditions. To reflect the effect of plant specific conditions and measures on the β-value, it is therefore beneficial to use CCF checklists, as given in IEC 61508, IEC 62061 and in Appendix A of this report.

5 CCF checklists to determine plant specific β-values

In this chapter we discuss the *equipment specific checklists* to determine plant specific β-values. The checklists developed as part of this project are based on the results from the operational reviews as discussed in chapter 4. The main purpose of these checklists is to:

- Classify and elucidate underlying factors that contribute to CCF
- Support decisions regarding possible defences or measures to reduce CCF, considering both root causes and coupling factors.
- Provide a method for adjusting generic β-values to incorporate facility specific conditions for different component types

5.1 Adjusting generic β-values

As discussed in this report, the experienced β-values from the operational reviews vary significantly between the facilities and depend on factors and conditions both related to design and to operation. The uncertainty related to these factors and conditions, and thus the uncertainty concerning the β-factor, will be largest at the start of a project and will decrease throughout later phases as more information and operational experience becomes available. This has been attempted illustrated in the below figure. It is then assumed that the operational experience is systematically evaluated and acted upon to reduce the occurrence of systematic failures as well as CCFs.

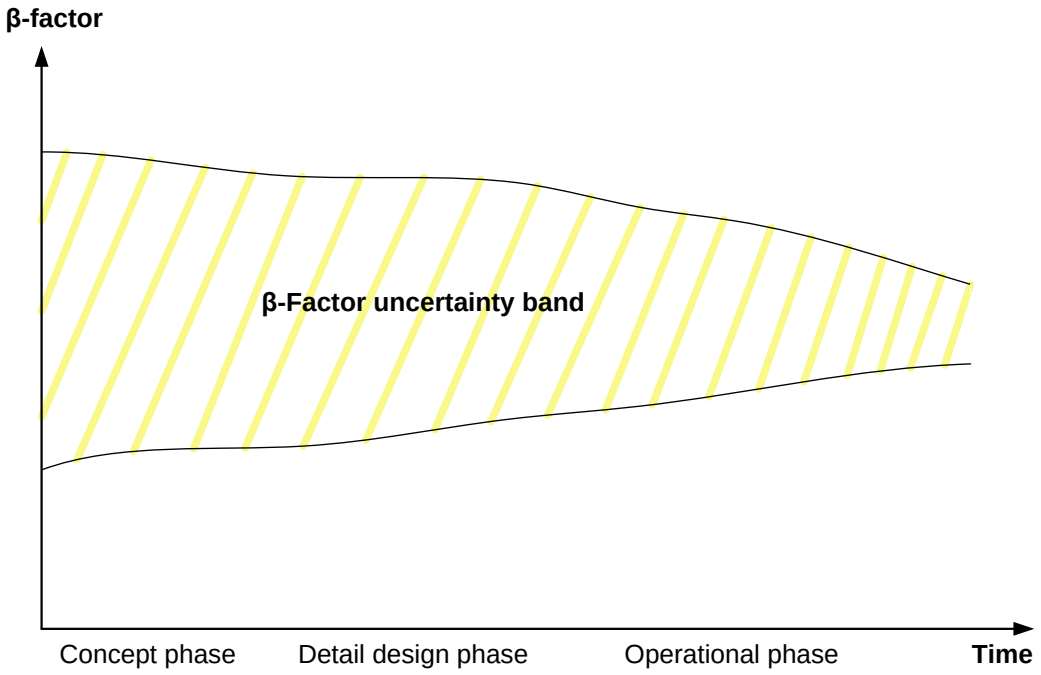


Figure 3: β-factor uncertainty as a function of time

Considering the above figure, the purpose of the checklists will be to utilize available information about relevant factors and conditions and thereby try to reduce the uncertainty related to the β-estimate. Typical applications of the checklists will be:

- During early design to determine plant specific beta-factor for early SIL calculations

- During detail design phase to revise the beta-factor based on additional knowledge about plant specific factors and conditions. The updated β-factors will typically be applied for SIL calculations and possibly for input to QRA.

- During operational phase to justify that the assumptions and for the plant-specific beta-factor are still valid (usually not done).

- During all phases to assess the likelihood of CCFs for a particular design and a foreseen operational regime. A checklist may also be used more qualitatively to identify vulnerabilities to common cause failures and to point at possible defences that, if implemented, will result in a reduction of the beta-factor.

During the operational phase information about CCFs may be collected and used to estimate the β-factor. However, since failures are infrequent and CCFs even more so, the amount of operational experience related to CCFs will be too limited to verify that the actual number of CCF is in line with the estimated beta-factor used in the SIL calculations. One option is to use a weighting procedure between the β-factor from design and the β experienced during operation (Bayes approach). In practice this implies that if for example the β-factor assumed in design was 10% for shutdown valves, and no CCFs have been experienced during the first 10 years of operation, then the β-factor can probably be somewhat reduced, but not to a zero level. It may be questioned whether such an update of the plant specific β-factor based on number of observed CCFs is at all relevant to perform during operation? As per today this is not done, but since it is actually required to verify the SIL requirements during operation, such a quantitative exercise should be considered.

5.2 CCF checklist format and categories

The equipment specific checklists are given in Appendix I.A.1.a)(1)A and have been developed based on experiences from the operational reviews as well as input from various literature discussed in chapter 3. The suggested checklist format is based on the following assumptions:

(i) Component specific CCF causes and couplings can be listed with basis in the review of reported failures: These are specific conditions known to affect the occurrence of CCFs (e.g. sand in the production flow, presence of ice and snow, same operators calibrating several transmitters, etc.). These causes and couplings are assumed to affect the beta-factor-value in some way.

(ii) Defences may be introduced to reduce the impact of specific CCF causes and couplings, but not to a zero level (for example, sand detectors, heat tracing of impulse lines, 3rd part control of work, etc.).

CCF causes, couplings and defences may vary between equipment groups. The general categorisation is discussed below (including some examples relevant for shutdown valves).

5.2.1 Classification of CCFs

Several schemes for classifying CCFs (or underlying coupling factors and root causes) can be found in the literature (ref. chapter 3). As discussed earlier in this report, CCFs and systematic failures are closely connected; basically all CCFs are systematic failures, but systematic failures can also affect one single component. Therefore, when classifying these CCFs, we will start with the failure classification scheme as proposed in the PDS method, see

Figure 4, and consider the systematic failures in particular.

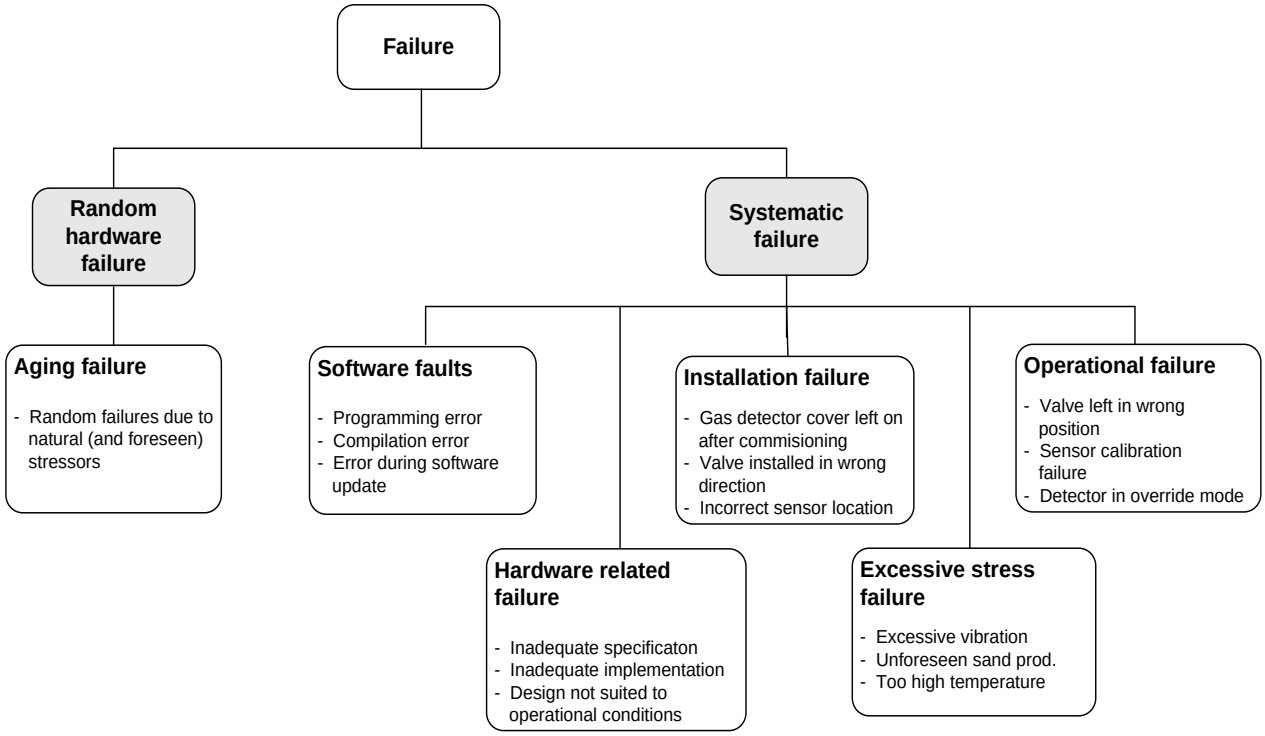


Figure 4: PDS failure classification by cause of failure, [Hauge et.al. 2013].

Software faults and hardware failures are both related to *design properties* of the component and since the equipment groups covered in this report are mainly hardware related (logic solvers not included as a separate equipment group) software faults are not included as a category on its own (but as a sub-category).

Operational failures and installation failures include human errors performed during operation, testing/ maintenance and repair, as well as during commissioning, installation and modifications. Such failures can materialise once (or close in time to) being introduced, but may often remain inherent in the system for a long period and materialise during an actual demand.

Excessive stress failures occur when stresses or conditions *beyond* the design specification are placed upon the component. Hence these failures are related to both the external as well as the internal environmental conditions that a component is exposed to.

Based on the above, the following CCF categories and sub-categories (examples – not a complete list) have been suggested:

- *Design properties*
  - Component specification and manufacturing
  - Material selection
  - Complexity
  - Associated utility systems
  - Location and separation
  - Software / logic
  - Prior use

- *Environmental control (external and internal)*:
  - Climate and temperatures; Ice, snow, fog, rain, sea spray, etc.
  - Variability in climatic conditions
  - Sand, dirt, hydrates and deposits
  - Corrosion and erosion

- *Operation, maintenance and modifications*
  - Installation commonalities; personnel, procedures and routines
  - Latent failures introduced during commissioning, installation and modifications
  - Maintainability and HMI
  - Procedures and routines
  - Personnel competency and training
  - Operator errors (of omission and commission)
  - Maintenance commonalities; personnel, procedures and routines.
  - Management of change

Note that installation/commissioning and modifications here have been included as part of the operational phase. Relatively few CCF events related to these phases were identified and hence they have not been included as separate categories.

It should also be noted that a failure introduced during operation, maintenance or modification may be caused by some inadequate design (i.e. underlying cause). Hence, the categories introduced above are not always mutually exclusive. However, when classifying CCFs in Chapter 4, we have generally considered the phase in which the failure has been introduced.

5.2.2 Classification of defences against CCF

Defences are measures or strategies that may prevent or reduce the likelihood of an associated cause or coupling to come into force. Examples can be separation of components, use of sand-traps, use of diverse technology and performance of root cause analysis to prevent future failures.

Defences may be split into the two main categories of "soft" *training/documentation/analysis* measures and "hard" *physical/technical/operational* measures. Soft and hard measures often "come in pair" as for example a root-cause analysis may have to be followed up with some technical measures like removal of ice or better insulation of the component. The two main categories can be further broken down, exemplified by the list below (not a complete list):

Examples of *training/documentation/analysis* defences are:

- Training, experience and competence
  - Technical equipment/system competence
  - SIS equipment and process specific courses
  - Simulator training

- Design related reviews:
  - Design analyses and reviews (w.r.t. sizing, material selection, actuator capacity, response time, etc.)
  - Process analyses (w.r.t. temperatures, pressure, flow, keeping tight in closed position, etc.)
  - Environmental and location analyses

- Operational follow-up and analyses:
  - Root cause analyses / analyses to identify systematic and common/shared failure causes
  - Design analyses and reviews (w.r.t. sizing, material selection, actuator capacity, response time, etc.)
  - Analyses to improve testing/maintenance and to identify measures to reduce systematic failures and CCFs
  - Handling of changes and modifications
  - Audits and reviews to validate the quality of testing/maintenance

Examples of *physical/technical/operational* defences are:

- Operational and maintenance measures
  - Cleaning
  - Lubrication
  - Draining
  - Adjustment checks
  - Removing ice, snow, etc.
  - Monitoring and inspection
  - Check of heat tracing / heaters
  - Maintenance staffing and scheduling (staggered testing, staff diversity)

- Design and functionality measures
  - Fit for purpose
  - Diversity
  - Changes/improvements of design / functionality
  - Improved technology
    - Improved materials
    - Increased diagnostics

- Physical and layout measures
  - Separation / Segregation
  - Enclosure
  - Insulation
  - Heat tracing / heaters

5.2.3 Description of checklist columns

The CCF-checklists include a set of columns that are explained below. Some of the columns relate to topics, figures, or issues that have been pre-set with basis in the operational reviews, while others relate to aspects that must be judged by the user of the checklist.

CCF category as discussed in section 5.2.1. These are pre-set categories.

Weights (in %) which are based on results from the operational reviews. Here, each CCF category and sub-category is given a certain weight based on the distributions referred in chapter 4 (i.e. from the actually observed data). For each equipment group the weights of each of the three CCF categories add up to 100%.

Relevance which is an assessment related to the relevance of the associated CCF statement or question, and is to be judged by the user of the checklist. There are three different options to select among:

- *Y*es: The question/statement is considered relevant and can be answered at the given point in time of filling in the checklist
- *Pre*mature: The question/statement is considered relevant but cannot be answered at the given point in time of filling in the checklist (e.g. questions related to operational follow-up is difficult to answer in the design phase). The *generic predefined weight* is then applied in the β-factor estimation
- *NA*: The checklist question/statement is not considered relevant for the design or installation under consideration. Hence the generic weight of the CCF category is subtracted in the β-factor estimation.

Defences related to the specific CCF sub-category under consideration, i.e. measures or strategies to prevent or reduce the likelihood of a CCF to occur. These are pre-set and based on a general consideration and classification of defences that apply to the Petroleum industry.

Efficiency (Eff) is a scaling comparable to the scaling used for potential CCFs in [NUREG/CR-6268 2007], with one added level. The following scaling factors are suggested:

- 3.0: *No* measure is implemented resulting in a "penalty" of a factor 3.
- 1.0: Measures are implemented but are judged to have a *Low* (or average) efficiency that does not go beyond what is considered average/current CCF protection standard in the industry.
- 0.5: Measures beyond average protection have been implemented, but the effect of the measure is considered *Medium* (or limited) or it has not been documented that the foreseen effects have been achieved.
- 0.1: Measures have been taken, and it has been documented that the measures have a *High* (and positive) effect on the issue in question.

The value used is selected by the user of the checklist but a default of 1.0 is assumed.

Modification factor (Mod Factor) is the product of the efficiency factor assigned to each defence and the weight related to the specific CCF statement/question. By summing up the modification factors for each CCF statement/question, an aggregated modification factor is obtained. This is further illustrated in the example in the next section.

The three CCF categories have – for each equipment type - been assigned a basic weight based on experiences and classification of CCFs - and potential CCFs failure causes from the operational reviews (ref. section 4.3 – 4.5). For each CCF category a number of equipment specific check list questions (or statements) have been suggested. The weight of each "question" is again based on findings from the operational reviews (and some expert judgements) and is also related to the particular failure modes observed for the components under consideration. E.g. for shutdown valves it is observed that closing time is often a problem. Hence, the associated CCF questions are assigned a relatively high weight in the checklist for shutdown valves.

The relevance and weight of each of the CCF categories and sub-categories obviously vary between the equipment groups. Also we see that some questions may apply for several equipment groups. For example measures related to improved root cause analysis and training, staffing and scheduling will typically be relevant for several equipment groups. As a result, several of the checklist questions are similar for different equipment groups. However, even if the questions are the same, the answers may be different and/or the specific CCF question or associated defence may be considered irrelevant for the components under

consideration. E.g. diversity may have been applied for a particular transmitter type (e.g. level transmitters) but not for pressure transmitters. Nevertheless, the user of the checklist has to assess the relevance of the checklist question according to the scheme described above.

The defences related to each of the CCF questions have been predefined in the checklist whereas the users themselves shall evaluate the efficiency of the defences according to the scheme described above. Default efficiencies are however filled in but can be adjusted. This is important in order to ensure that the users of the checklists take into account all relevant previous experiences (from other similar facilities, systems, components, etc.) and possible defence measures in the assessment.

5.2.4 Checklist example for shutdown valves

Below is given an example of a checklist (for shutdown valves) and how it could be filled in. The user has to fill in the relevant column with 'Y', 'Pre' or 'NA' (shown in green in the below table) and also re-evaluate the defaulted efficiency factors (default in red, re-evaluated in green). The modification factors are automatically calculated.

Table 16 Example of filled-in CCF checklist for shutdown valves

CCF category	*Weight*	*Relevance*	*Defences*		*Mod. Factor*
Design properties	**45 %**	**Y/Pre/NA**	**Description of defence**	**Eff.**	
Valves within the same equipment group are of the same type (make, manufacturer, material selection, etc.).	10 %	Y	Has the design been reviewed with the purpose of revealing common vulnerabilities, associated with sizing, material selection, location and so on, and are defences implemented to reduce common vulnerabilities (separation, diversity)	1.0 (L)	0.1
Response times (max/min) are critical for the successful performance of the valves.	15 %	Y	Have design reviews been carried out with the purpose of identifying possible design constraints in view of response time requirements?	1.0 (L)	0.15
Inadequate actuator force can cause the valve not to close upon particular process conditions, such as e.g. low pressures.	5 %	Y	Has it been verified by analyses (and possibly testing) that there is sufficient actuator force to close the valve under all foreseeable process conditions and/or has extra sizing/ dimensioning of actuator, etc. been implemented to ensure that the valve will function under all foreseeable process conditions??	0.1 (H)	0.005
Failure of common utility systems, such as accumulators, hydraulic-, or pneumatic systems can result in valves failing to close.	5 %	NA	Has it been confirmed that the associated utility systems have sufficient capacity, and are procedures in place to ensure that as well as the individual valve actuators?	1.0 (L)	0
Valves are required to keep leak tight in closed position.	5%	Y	Are condition monitoring or other operational measures implemented to prevent too high leakage rates in closed position?	1.0 (L)	0.05
Whether the design can be considered fit for purpose is considered an issue for the particular application.	5 %	Y	Is any operational experience related to the specific valve type available, or is prior-use experience available for the valve and relevant for the current application?	0.5 (M)	0.025
Subtotal modification factor for 'Design properties':					0.33 (33 %)
Environmental Control (external & internal)	**20 %**	**Y/Pre/NA**	**Description of defence**	**Eff.**	
The valves are exposed to an internal environment such as dirt, sand, hydrates, etc. with a potential to affect valve performance.	3 %	Y	Has specific procedures for control of sand, dirt, hydrate formation, etc. been implemented, including procedures for cleaning and lubrication of valves?	1.0 (L)	0.03
As above	4 %	Y	Have physical measures for control of internal environmental influences such as sand traps, inhibitors, etc. been implemented?	0.5 (M)	0.02
The valves are exposed to snow, temperature changes, icing conditions, sea spray, etc., possibly affecting valve performance?	3 %	Y	Are procedures for removing ice, build-up of snow, control of hydraulic oil viscosity, etc. during periods with cold temperatures in place and implemented (including procedures to check that e.g. heat tracing is functioning / is on)?	0.5 (M)	0.015
As above	4 %	Y	Are valves exposed to snow, ice, sea spray, cold temperatures equipped with separate weather protection/ isolation/ heat tracing?	0.5 (M)	0.02
The valves are subject to a corrosive environment (internal and/or external) that can affect valve performance.	3 %	Y	Are inspection procedures and associated acceptance criteria in place for controlling and preventing corrosion?	0.5 (M)	0.015
As above	3 %	Y	Have physical measures for control of the corrosive environment been implemented such as material choice, corrosion inhibitor, etc.?	1.0 (M)	0.03
Subtotal modification factor for 'Environmental control':					0.13 (13 %)

Operation, maintenance & modifications	35 %	Y/Pre/NA	Description of defence	Eff.	
The valves are periodically tested and maintained according to a predefined maintenance program.	3 %	Y	Are test- and maintenance procedures readily available, made familiar among the maintenance personnel, and are they kept continuously updated throughout the operational phase?	0.5 (L)	0.015
As above	3 %	Y	Are there routines/procedures in place to periodically review and if necessary adjust the frequency of functional testing for the valves in light of registered failure history and experienced failure causes?	3.0 (N)	0.09
As above	4%	Y	Do the maintenance personnel always check for similar failures on other valves, if a failure is revealed during testing or operation?	0.5 (L)	0.02
Results from periodic testing and maintenance are logged into some kind of electronic (or written) maintenance system.	5 %	Y	Have the maintenance operators been given particular training with respect to understanding the valves functionality, critical failure modes and registering maintenance notifications in order to give a good description of e.g. failure cause, detection method and failure modes?	1.0 (L)	0.05
As above	5 %	Pre	Are maintenance notifications regularly gone through in order to reveal repeating valve failures, to compare results for all relevant valves across the facility, and to initiate and perform root cause analysis in order to identify measures to remove these failure causes?	1.0 (L)	0.05
In case of a valve failure during testing or operation it may be a relevant measure to run the valve again until it functions.	5 %	Pre	If a valve has to be run several times to function satisfactorily (e.g. close fast enough), are then additional measure (lubrication, cleaning, finding the root cause) always put in place in order to prevent this from happening again?	1.0 (L)	0.05
Wrong tuning of bleed off valve and/or weaknesses in the bleed-of arrangement / control block may result in valve failing to close or closing too slow.	5 %	Pre	Are operational measures implemented to ensure that the bleed-off arrangement is correctly tuned and (if relevant) periodically calibrated towards required closing times?	1.0 (L)	0.05
Adding new valves or valve modifications, including changes to valve performance requirements may become relevant during the operational phase	5 %	Y	Are there procedures for independent checks after valve modifications, valve adjustments and adjustments of closing/opening time?	0.1 (H)	0.005
Subtotal modification factor for 'Operation, maintenance & modifications':					0.33 (33 %)
Aggregated modification factor					0.79 (79 %)

From the example checklist we see that the estimated modification factor is 0.79. Then if the generic β-factor for shutdown valves is 12 %, the updated β-value becomes 12 % · 0.79 = 9.5 % based on the evaluation of the checklist questions.

Note that some issues related to the category "operation, maintenance and modifications" have not been evaluated (i.e. "Pre"). In such case the checklist can be reviewed at a later stage when more information is available. Such an update should then preferably include a re-evaluation of all checklist questions.

6 Concluding remarks

Reliability calculations basically involve two main activities:

1. Establish the mathematical/statistical model of the given system including CCF analyses, by use of e.g. analytical formulas, reliability block diagrams, fault trees, Markov models or simulation techniques.
2. Establish the value of variables and parameters to be used as input to the reliability model, typically from OREDA [2009], the PDS data handbook [2013], company specific databases or vendor certificates.

Significant research efforts have traditionally been put into activity 1, both in academia, through textbooks, standards and guidelines, e.g. exemplified through the newly released ISO/TR 12489 [2013] which gives a thorough description of different reliability modelling and calculation techniques.

Major initiatives are also ongoing for data collection in the petroleum industry, in particular through the OREDA project and the RNNP project where relatively high level failure data for different barrier elements are collected.

When comparing the *uncertainty* related to the choice of reliability modelling technique versus the choice of reliability data, some general observations can be made based on SINTEFs own experiences:

- The choice of modelling techniques, e.g. using a simulation model instead of analytical formulas, may in some cases affect the estimated unavailability; usually by just a few percent but sometimes up to 30-40 % (e.g. if the analytical formulas do not take into considerations important time dependencies)
- The reliability data applied may often vary with more than one decade for a given piece of equipment, sometimes up to two decades, when comparing e.g. vendor certificate data with generic/historic data based on operational experiences.

It therefore seems fair to conclude that even more efforts should be put into the *right choice of reliability data*, as this aspect per today is associated with far more uncertainty than the modelling itself.

Reliability data includes two important parameters; (1) failure rates for single components and (2) CCF rates for redundant components. The latter is typically represented by the β-factor, which can be interpreted as the fraction of failures that cause more than one component to fail in a redundant configuration. In the PDS project, much work has been done to obtain generic failure rates for single components based on operational experience from offshore and onshore facilities, ref. PDS data handbook [2013]. Values for the β-factor have also been suggested, but they are generally based on expert judgements and figures from the nuclear industry, rather than actual operational data from the petroleum industry. Since the reliability of systems that employ redundancy is highly influenced by CCFs, it is important to obtain more realistic data for such failures relevant for the petroleum industry. In this report, results from such a project are presented; data from operational reviews on six offshore and onshore installations have been used to study the occurrence of safety critical failures and CCFs in particular.

Based on a review of some 12000 maintenance notifications, the most typical CCF causes and their relative importance have been presented and discussed. The new knowledge has been used as basis for developing equipment specific checklists, targeted to address the most important CCFs for each equipment type. Also, the data has been applied to estimate new β-factors for selected equipment groups. A major conclusion is that

the observed β-values based on operational experience are significantly higher than what has traditionally been assumed in design calculations for all equipment types under consideration. It can therefore be concluded that more effort should be put into systematically analysing and reducing the extent of CCFs (and systematic failures).

It should also be emphasised that the estimated βs are based on average values and vary significantly between the installations. On some installations no CCF events have been observed for certain equipment groups, whereas on other installations a very high frequency of CCFs has been observed for certain equipment. It is therefore important to adjust the generic (or average) estimates of β, based on installation specific conditions.

References

Amendola A., 1989. Classification of multiple related failures. In A. Amendola (ed), Common Cause Failure Analysis in Probabilistic Safety Assessment. Kluwer Ac. Pub.

Brand P.V., 1996. A pragmatic approach to dependent failures assessment for standard systems. AEA Technology plc.

Hauge S., et al 2013. Reliability Prediction Method for Safety Instrumented Systems. PDS Method Handbook 2013.

Hokstad P., 2004. A Generalisation of the Beta Factor Model. In Probabilistic Safety Assessment and Management Eds.: C. Spitzer, U. Schmocker & V.N. Dang, Springer 2004. Proceedings from PSAM7-ESREL '04.

Hokstad P. and Rausand M., Common Cause Failure Modelling: Status and Trends, pp 621-640. In Handbook of Performability Engineering. Editor: Krishna B. Misra. Springer 2008.

Hokstad P., Maria A. & Tomis P., 2006. Estimation of Common Cause Factors from Systems with Different Numbers of Channels. IEEE Transactions on Reliability, Vol. 55, No. 1, pp 18-25.

Håbrekke S., et al 2013. Reliability Data for Safety Instrumented Systems. PDS Data Handbook 2013.

Humpreys RA 1987. Assigning a numerical value to the beta factor common cause evaluation. Reliability '87. Proceedings paper 2C.

Håbrekke S., et al 2013. Reliability Data for Safety Instrumented Systems. PDS Data Handbook 2013.

IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva: International Electrotechnical Commission. 2010

ISO 14224 (2006). Petroleum, petrochemical and gas industries—collection and exchange of reliability and maintenance data for equipment

ISO/TR 12489. Petroleum, petrochemical and natural gas industries – Reliability modelling and calculation of safety systems. Ver. 01, 2013

NEA 2004. International Common Cause failure data exchange. Number NEA/CSNI/R(2004)4. Nuclear Energy Agency

NEA 2012. International Common Cause Data Exchange (ICDE) General Coding Guidelines
- Updated Version Nuclear Safety NEA/CSNI/R(2011)12. OECD Nuclear Energy Agency (NEA): 106.

NEA, N. E. A. (2014). "OECD/NEA International Common Cause Data Exchange (ICDE) Project." http://www.oecd-nea.org/jointproj/icde.html, 2014.

NUREG/CR-4780, Vol. 1 (1988). A. Mosleh, K.N. Fleming, G.W. Parry, H.M. Paula, D.H. Worledge, D.M. Rasmuson. Procedures for Treating Common Cause Failures in Safety and Reliability Studies.

NUREG/CR-5485, (1998). Guidelines on modeling common-cause failures in probabilistic risk assessment. US Nuclear Regulatory Commission. A. Mosleh, D.M. Rasmuson, F.M. Marshall. Washington, DC.: Nuclear Regulatory Commission.

NUREG/CR-6268, Rev.1 US Nuclear Regulatory Commission (2007). T.E. Wierman, D.M. Rasmuson, A. Mosleh. Common-cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding.

OREDA participants, OREDA; Offshore Reliability Data Handbook, Volume 1 – topside data and Volume 2 – subsea data. 5th edition, 2009.

Parry, G.W. 1991. Common cause failure analysis: a critique and some suggestions. Reliability Engineering and System Safety 34, 309–326.

Paula, H. M., D. J. Campbell, and D. M. Rasmuson 1991. Qualitative cause-defense matrices; engineering tools to support the analysis and prevention of common cause failures. Reliability Engineering and System Safety 34(3), 389–415.

Petroleumstilsynet, Risikonivå i petroleumsvirksomheten. Hovedrapport, utviklingstrekk 2013, norsk sokkel, Rev. 2, April 2014

SKI 1992, CCF analysis of high redundancy systems, safety/relief valve data analysis and reference BWR application. SKI Technical Report 91:6, Stockholm.

Smith, A.M., Watson, I.A. 1980. Common cause failures—a dilemma in perspective. Reliability Engineering 1.

Zitrou A, Bedford T. 2003. Foundations of the UPM common cause model. In: Bedford T, Gelder PH. van, eds. Safety and Reliability. Balkema, ESREL 2003; 1769–1775.

Appendix

A Equipment specific checklists

A.1 Valves

A.1.1 Shutdown valves – topside ESD and PSD valves incl. riser ESD valves

CCF category	*Weight*	*Relevance*	*Defences*		*Mod. Factor*
Design properties	**45 %**	**Y/Pre/NA**	**Description of defence**	**Eff.**	
Valves within the same equipment group are of the same type (make, manufacturer, material selection, etc.).	10 %		Has the design been reviewed with the purpose of revealing common vulnerabilities, associated with sizing, material selection, location and so on, and are defences implemented to reduce common vulnerabilities (separation, diversity)	1.0 (L)	
Response times (max/min) are critical for the successful performance of the valves.	15 %		Have design reviews been carried out with the purpose of identifying possible design constraints in view of response time requirements?	1.0 (L)	
Inadequate actuator force can cause the valve not to close upon particular process conditions, such as e.g. low pressures.	5 %		Has it been verified by analyses (and possibly testing) that there is sufficient actuator force to close the valve under all foreseeable process conditions and/or has extra sizing/ dimensioning of actuator, etc. been implemented to ensure that the valve will function under all foreseeable process conditions??	1.0 (L)	
Failure of common utility systems, such as hydraulic-, or pneumatic systems can result in valves failing to close.	5 %		Has it been confirmed that the associated utility systems have sufficient capacity, and are procedures in place to ensure this throughout the plant lifetime as well as monitoring of the individual valve accumulators (if relevant)?	1.0 (L)	
Valves are required to keep leak tight in closed position.	5%		Are condition monitoring or other operational measures implemented to prevent too high leakage rates in closed position?	1.0 (L)	
Whether the design can be considered fit for purpose is considered an issue for the particular application.	5 %		Is any operational experience related to the specific valve type available, or is prior-use experience available for the valve and relevant for the current application?	1.0 (L)	
Subtotal modification factor for 'Design properties':					
Environmental Control (external & internal)	**20 %**	**Y/Pre/NA**	**Description of defence**	**Eff.**	
The valves are exposed to an internal environment such as dirt, sand, hydrates, etc. with a potential to affect valve performance.	3 %		Has specific procedures for control of sand, dirt, hydrate formation, etc. been implemented, including procedures for cleaning and lubrication of valves?	1.0 (L)	
As above	4 %		Have physical measures for control of internal environmental influences such as sand traps, inhibitors, etc. been implemented?	1.0 (L)	
The valves are exposed to snow, temperature changes, icing conditions, sea spray, etc., possibly affecting valve performance?	3 %		Are procedures for removing ice, build-up of snow, control of hydraulic oil viscosity, etc. during periods with cold temperatures in place and implemented (including procedures to check that e.g. heat tracing is functioning / is on)?	1.0 (L)	

As above	4 %		Are valves exposed to snow, ice, sea spray, cold temperatures equipped with separate weather protection/ isolation/ heat tracing?	1.0 (L)
The valves including actuators are subject to a corrosive environment (internal and/or external) that can affect valve performance.	3 %		Are inspection procedures and associated acceptance criteria in place for controlling and preventing corrosion?	1.0 (L)
As above	3 %		Have physical measures for control of the corrosive environment been implemented such as material choice, corrosion inhibitor, etc.?	1.0 (M)
Subtotal modification factor for 'Environmental control':				

Operation, maintenance & modifications	**35 %**	**Y/Pre/NA**	**Description of defence**	**Eff.**
The valves are periodically tested and maintained according to a predefined maintenance program.	3 %		Are test- and maintenance procedures readily available, made familiar among the maintenance personnel, and are they kept continuously updated throughout the operational phase?	1.0 (L)
As above	3 %		Are there routines/procedures in place to periodically review and if necessary adjust the frequency of functional testing for the valves in light of registered failure history and experienced failure causes?	1.0 (L)
As above	4%		Do the maintenance personnel always check for similar failures on other valves, if a failure is revealed during testing or operation?	1.0 (L)
Results from periodic testing and maintenance are logged into some kind of electronic (or written) maintenance system.	5 %		Have the maintenance operators been given particular training with respect to understanding the valves functionality, critical failure modes and registering maintenance notifications in order to give a good description of e.g. failure cause, detection method and failure modes?	1.0 (L)
As above	5 %		Are maintenance notifications regularly gone through in order to reveal repeating valve failures, to compare results for all relevant valves across the facility, and to initiate and perform root cause analysis in order to identify measures to remove these failure causes?	1.0 (L)
In case of a valve failure during testing or operation it may be a relevant measure to run the valve again until it functions.	5 %		If a valve has to be run several times to function satisfactorily (e.g. close fast enough), are then additional measure (lubrication, cleaning, finding the root cause) always put in place in order to prevent this from happening again?	1.0 (L)
Wrong tuning of bleed off valve and/or weaknesses in the bleed-of arrangement / control block may result in valve failing to close or closing too slow.	5 %		Are operational measures implemented to ensure that the bleed-off arrangement is correctly tuned and (if relevant) periodically calibrated towards required closing times?	1.0 (L)
Adding new valves or valve modifications, including changes to valve performance requirements may become relevant during the operational phase	5 %		Are there procedures for independent checks after valve modifications, valve adjustments and adjustments of closing/opening time?	1.0 (L)
Subtotal modification factor for 'Operation, maintenance & modifications':				

Aggregated modification factor

A.1.2 Blowdown valves

CCF category	*Weight*	*Relevance*	*Defences*		*Mod. Factor*
Design properties (incl. location)	**40 %**	**Y/Pre/NA**	**Description of defence**	**Eff.**	
Blowdown valves within the same equipment group are of the same type (make, manufacturer, material selection, etc.).	10 %		Has the design been reviewed with the purpose of revealing common vulnerabilities, associated with sizing, material selection, location and so on, and are defences implemented to reduce common vulnerabilities (separation, diversity)	1.0 (L)	
Opening times (max/min) are critical for the successful performance of the valves.	5 %		Have design reviews been carried out with the purpose of identifying possible design constraints in view of response time requirements?	1.0 (L)	
There is sequential blowdown on the facility.	5 %		Has it been verified by analyses (and possibly testing) that there is sufficient capacity in associated utility systems to ensure adequate sequential blowdown and has the blowdown logic been sufficiently verified?	1.0 (L)	
Failure of common utility systems, such as hydraulic-, or pneumatic systems can result in valves failing to open.	5 %		Has it been confirmed that the associated utility systems have sufficient capacity, and are procedures in place to ensure this throughout the lifetime of the plant?	1.0 (L)	
Some blowdown valves are depending on accumulators for successful opening.	5 %		Are procedures implemented for monitoring of accumulators to reveal leakages and ensure sufficient accumulator force?	1.0 (L)	
The blowdown valves must operate under varying pressure conditions	5 %		Has it been verified through analysis (and possibly testing) that the valves will open under all relevant pressure conditions?	1.0 (L)	
Whether the design can be considered fit for purpose is considered an issue for the particular application.	5 %		Is any operational experience related to the specific valve type available, or is prior-use experience available for the valve and relevant for the current application?	1.0 (L)	
Subtotal modification factor for 'Design properties':					
Environmental Control (external & internal)	**25 %**	**Y/Pre/NA**	**Description of defence**	**Eff.**	
The valves are vulnerable to internal hydrates/icing with a potential to affect valve performance.	5 %		Has specific procedures for control of hydrate formation been implemented, and/or are physical measures such as heating, heat tracing or insulation installed to prevent hydrate formation?	1.0 (L)	
The valves are exposed to snow, temperature changes, icing conditions, sea spray, etc., possibly affecting valve performance?	5 %		Are procedures for removing ice, build-up of snow, control of hydraulic oil viscosity, etc. during periods with cold temperatures in place and implemented (including procedures to check that e.g. heat tracing is functioning / is on)?	1.0 (L)	
As above	5 %		Are valves exposed to snow, ice, sea spray, cold temperatures equipped with separate weather protection/ isolation/ heat tracing?	1.0 (L)	
The valves including actuators are subject to a corrosive environment (internal and/or external) that can affect valve performance.	5 %		Are inspection procedures and associated acceptance criteria in place for controlling and preventing corrosion?	1.0 (L)	
As above	5 %		Have physical measures for control of the corrosive environment been implemented such as material choice, corrosion inhibitor, etc.?	1.0 (M)	
Subtotal modification factor for 'Environmental control':					

Operation, maintenance & modifications	35 %	Y/Pre/NA	Description of defence	Eff.
The valves are periodically tested and maintained according to a predefined maintenance program.	3 %		Are test- and maintenance procedures readily available, made familiar among the maintenance personnel, and are they kept continuously updated throughout the operational phase?	1.0 (L)
As above	3 %		Are there routines/procedures in place to periodically review and if necessary adjust the frequency of functional testing for the valves in light of registered failure history and experienced failure causes?	1.0 (L)
As above	4%		Do the maintenance personnel always check for similar failures on other valves, if a failure is revealed during testing or operation?	1.0 (L)
Results from periodic testing and maintenance are logged into some kind of electronic (or written) maintenance system.	5 %		Have the maintenance operators been given particular training with respect to understanding the valves functionality, critical failure modes and registering maintenance notifications in order to give a good description of e.g. failure cause, detection method and failure modes?	1.0 (L)
As above	5 %		Are maintenance notifications regularly gone through in order to reveal repeating valve failures, to compare results for all relevant valves across the facility, and to initiate and perform root cause analysis in order to identify measures to remove these failure causes?	1.0 (L)
In case of a valve failure during testing or operation it may be a relevant measure to run the valve again until it functions.	5 %		If a valve has to be run several times to function satisfactorily (e.g. open fast enough), are then additional measure (lubrication, cleaning, finding the root cause) always put in place in order to prevent this from happening again?	1.0 (L)
Failure of common utility systems, such as a pneumatic air supply system, may result in valves failing to open or opening too slow.	5 %		Operational measures such as e.g. periodic inspection and maintenance are implemented to ensure that common utility systems necessary for operating the blowdown valves are always functioning.	1.0 (L)
Adding new valves or valve modifications, including changes to valve performance requirements may become relevant during the operational phase	5 %		Are there procedures for independent checks after valve modifications, valve adjustments and adjustments of closing/opening time?	1.0 (L)
Subtotal modification factor for 'Operation, maintenance & modifications':				

Aggregated modification factor

A.1.3 Fire dampers

CCF category	*Weight*	*Relevance*	*Defences*	*Mod. Factor*
Design properties (incl. location)	**50 %**	**Y/Pre/NA**	**Description of defence**	**Eff.**
Dampers within the same equipment group are of the same *type* (make, manufacturer, material selection, etc.).	10 %		Has the design been reviewed with the purpose of revealing common vulnerabilities, associated with sizing, material selection, etc., and are defences implemented to reduce common vulnerabilities?	1.0 (L)
Dampers protecting the same room/area are located in the *immediate vicinity* of each other.	10 %		Has the layout been reviewed with the purpose of revealing common vulnerabilities associated with location, and are defences implemented to reduce such vulnerabilities (separation, diversity)?	1.0 (L)
Response times (max/min) are critical for the successful performance of the dampers.	5 %		Have design reviews been carried out with the purpose of identifying possible design constraints in view of response time requirements?	1.0 (L)
Inadequate actuator force or actuator design can cause the damper not to close or close too slow upon particular weather conditions (ice, snow, wind, etc.).	15 %		Has it been verified by analyses (and possibly testing) that there is sufficient actuator force to close the damper under all foreseeable weather conditions, and/or has extra sizing/ dimensioning of actuator, etc. been implemented to ensure that the damper will function under all foreseeable conditions?	1.0 (L)
Whether the design of damper and actuator can be considered fit for purpose is considered an issue for the particular application.	10 %		Is any operational experience related to the specific damper type available, or is prior-use experience available for the damper and relevant for the current application?	1.0 (L)
Subtotal modification factor for 'Design properties':				

Environmental Control (external & internal)	**15 %**	**Y/Pre/NA**	**Description of defence**	**Eff.**
The dampers may be exposed to external and internal influences such as dirt and sand, etc. with a potential to affect damper performance.	5 %		Has specific procedures for control of sand, dirt, etc. been implemented, including procedures for cleaning and lubrication of valves?	1.0 (L)
The dampers are exposed to snow, temperature changes, icing conditions, sea spray, etc., possibly affecting their performance?	5 %		Are procedures for removing ice, build-up of snow, etc. during periods with cold temperatures in place and implemented, and/or are physical measures such as weather protection, heating, heat tracing or insulation installed to protects against harsh environment?	1.0 (L)
The dampers including actuators are subject to a corrosive environment (internal and/or external) that can affect their performance.	5 %		Are inspection procedures and associated acceptance criteria in place for controlling and preventing corrosion, and/or have physical measures for control of the corrosive environment been implemented such as material choice, etc.?	1.0 (L)
Subtotal modification factor for 'Environmental control':				

Operation, maintenance & modifications	35 %	Y/Pre/NA	Description of defence	Eff.
The dampers are periodically tested and maintained according to a predefined maintenance program.	3 %		Are test- and maintenance procedures readily available, made familiar among the maintenance personnel, and are they kept continuously updated throughout the operational phase?	1.0 (L)
As above	3 %		Are there routines/procedures in place to periodically review and if necessary adjust the frequency of functional testing for the dampers in light of registered failure history and experienced failure causes?	1.0 (L)
As above	4 %		Do the maintenance personnel always check for similar failures on other fire dampers, if a failure is revealed during testing or operation?	1.0 (L)
Results from periodic testing and maintenance are logged into some kind of electronic (or written) maintenance system.	5 %		Have the maintenance operators been given particular training with respect to understanding the fire dampers' functionality, critical failure modes and registering maintenance notifications in order to give a good description of e.g. failure cause, detection method and failure modes?	1.0 (L)
As above	5 %		Are maintenance notifications regularly gone through in order to reveal repeating damper failures, to compare results for all relevant dampers across the facility, and to initiate and perform root cause analysis in order to identify measures to remove these failure causes?	1.0 (L)
In case of a damper failure during testing or operation it may be a relevant measure to run the damper again until it functions.	5 %		If a damper has to be run several times to function satisfactorily (e.g. close fast enough), are then additional measure (lubrication, cleaning, finding the root cause) always put in place in order to prevent this from happening again?	1.0 (L)
Maintainability of and access to the dampers is considered a relevant issue.	5%		Is the access to the dampers good enough to perform maintenance activities in an easy manner, and/or has any measures been implemented in order to increase the maintainability?	
Adding new dampers or damper modifications may become relevant during the operational phase	5 %		Are there procedures for independent checks after damper modifications, damper adjustments and adjustments of closing times?	1.0 (L)
Subtotal modification factor for 'Operation, maintenance & modifications':				

Aggregated modification factor

A.1.4 Pressure Safety Valves (PSV)

CCF category	*Weight*	*Relevance*	*Defences*		*Mod. Factor*
Design properties (incl. location)	**40 %**	**Y/Pre/NA**	**Description of defence**	**Eff.**	
PSVs within the same equipment group are of the same *type* (make, manufacturer, material selection, etc.).	10 %		Has the design been reviewed with the purpose of revealing common vulnerabilities, associated with sizing, material selection, etc., and are defences implemented to reduce common vulnerabilities?	1.0 (L)	
PSVs protecting the same vessel are located in the *immediate vicinity* of each other.	10 %		Have measures been implemented to reduce the effect of vulnerabilities due to common location (separation, diversity, etc.)?	1.0 (L)	
A pilot valve is required to operate the PSV successfully.	15 %		Have design reviews and/or analyses been carried out to ensure that the selected pilot valves are fit for purpose and/or are other measures implemented to ensure high availability of pilot valves and pilot lines?	1.0 (L)	
Whether the design can be considered fit for purpose is considered an issue for the particular application.	5 %		Is any operational experience related to the specific valve type available, or is prior-use experience available for the valve and relevant for the current application?	1.0 (L)	
Subtotal modification factor for 'Design properties':					
Environmental Control (external & internal)	**35 %**	**Y/Pre/NA**	**Description of defence**	**Eff.**	
The valves are vulnerable to internal hydrates/icing with a potential to affect valve performance.	5 %		Has specific procedures for control of hydrate formation been implemented, and/or are physical measures such as heating, heat tracing or insulation installed to prevent hydrate formation?	1.0 (L)	
The valves are exposed to snow, temperature changes, icing conditions, sea spray, etc., possibly affecting valve performance?	5 %		Are procedures for removing ice, build-up of snow, control of hydraulic oil viscosity, etc. during periods with cold temperatures in place and implemented (including procedures to check that e.g. heat tracing is functioning / is on) and/or are physical measures such as weather protection, heating, heat tracing or insulation installed to protects against harsh environment?	1.0 (L)	
The pilot lines may be subject to freezing or plugging.	10 %		Are physical or procedural measures implemented to avoid freezing or plugging of impulse lines?	1.0 (L)	
The valves are subject to internal or external influences such as sand or dirt that can affect their performance.	7 %		Are procedural measures implemented to avoid and control possible congestion of dirt/sand and/or are physical measures implemented to avoid such influences?	1.0 (L)	
The valves are subject to a corrosive environment (internal and/or external) that can affect their performance.	8 %		Are inspection procedures and associated acceptance criteria in place for controlling and preventing corrosion, and/or have physical measures for control of the corrosive environment been implemented such as material choice, weather protection, etc.?	1.0 (L)	
Subtotal modification factor for 'Environmental control':					

Operation, maintenance & modifications	25 %	Y/Pre/NA	Description of defence	Eff.
The valves are periodically tested and maintained according to a predefined maintenance program.	3 %		Are test- and maintenance procedures readily available, made familiar among the maintenance personnel, and are they kept continuously updated throughout the operational phase?	1.0 (L)
As above	3 %		Are there routines/procedures in place to periodically review and if necessary adjust the frequency of functional testing for the valves in light of registered failure history and experienced failure causes?	1.0 (L)
As above	4%		Do the maintenance personnel always check for similar failures on other valves, if a failure is revealed during testing or operation?	1.0 (L)
Results from periodic testing and maintenance are logged into some kind of electronic (or written) maintenance system.	4 %		Have the maintenance operators been given particular training with respect to understanding the valves functionality, critical failure modes and registering maintenance notifications in order to give a good description of e.g. failure cause, detection method and failure modes?	1.0 (L)
As above	3 %		Are maintenance notifications regularly gone through in order to reveal repeating valve failures, to compare results for all relevant valves across the facility, and to initiate and perform root cause analysis in order to identify measures to remove these failure causes?	1.0 (L)
Incorrect adjustment of set point may cause malfunction of the PSV	4 %		Have measures been implemented to avoid incorrect adjustment of PSV set point such as special training of operators and/or particular tools for calibration?	1.0 (L)
Adding new valves or valve modifications, including changes to valve performance requirements may become relevant during the operational phase	4 %		Are there procedures for independent checks after valve modifications, valve change outs and/or valve adjustments?	1.0 (L)
Subtotal modification factor for 'Operation, maintenance & modifications':				

Aggregated modification factor

A.2 Fire and gas detectors

A.2.1 Point and line gas detectors

CCF category	*Weight*	*Relevance*	*Defences*		*Mod. Factor*
Design properties (incl. location)	**35 %**	**Y/Pre/NA**	**Description of defence**	**Eff.**	
The applied gas detectors are of the same type (make, manufacturer, material selection, etc.).	10 %		Has the design been reviewed with the purpose of revealing common vulnerabilities and are defences implemented to reduce the effect of any such common vulnerabilities (separation, diversity, etc.)	1.0 (L)	
The detectors contain specific parts that highly influence the reliability of the detectors.	10 %		Has specific analyses been performed or measures been implemented to ensure that the reliability of *particularly critical parts* such as filters, lenses, mirrors, junction boxes etc. are good.	1.0 (L)	
Location/layout of redundant detectors is critical in order to ensure optimal detection.	5 %		Has separate analyses/simulations been conducted to verify that (voted) detectors are located such that they will detect gas, even for moderate releases, taking into consideration ventilation conditions, wind, etc.?	1.0 (L)	
The gas detector is delivered with a specified diagnostic coverage factor	5 %		Has it has been verified and documented by analysis (and/or prior use) that the gas detector fulfils the "promised" diagnostic coverage		
Whether the design can be considered fit for purpose is considered an issue for the particular application.	5 %		Is any operational experience related to the specific detector type available, or is prior-use experience available for the detector and relevant for the current application?	1.0 (L)	
Subtotal modification factor for 'Design properties':					
Environmental Control (external & internal)	**30 %**	**Y/Pre/NA**	**Description of defence**	**Eff.**	
The detectors are exposed to snow, rain, fog, icing conditions, sea spray, etc., possibly affecting detector performance?	10 %		Are procedures for removing ice, snow, cleaning lenses/mirrors, avoiding water intrusion, etc. during periods with harsh weather, in place and implemented, and/or are other physical measures installed to protect against harsh environment (e.g. use of silicone to avoid water intrusion into junction boxes, etc.)?	1.0 (L)	
The detectors are subject to external influences such as polluted air, exhaust, sand, dirt, etc. which may influence the performance of the detectors.	10 %		Are procedural measures implemented to avoid and control possible influences from a polluted environment and/or are physical measures implemented to avoid such influences?	1.0 (L)	
The detectors are subject to an external corrosive environment that can affect their performance.	10 %		Are inspection and maintenance procedures in place for controlling and preventing corrosion, and/or have physical measures for control of the corrosive environment been implemented such as material choice, weather protection, etc.?	1.0 (L)	
Subtotal modification factor for 'Environmental control':					

Operation, maintenance & modifications	35 %	Y/Pre/NA	Description of defence	Eff.
The detectors are periodically tested and maintained according to a predefined maintenance program.	3 %		Are test- and maintenance procedures readily available, made familiar among the maintenance personnel, and are they kept continuously updated throughout the operational phase?	1.0 (L)
As above	3 %		Are there routines/procedures in place to periodically review and if necessary adjust the frequency of functional testing for the detectors in light of registered failure history and experienced failure causes?	1.0 (L)
As above	3%		Do the maintenance personnel always check for similar failures on other detectors, if a failure is revealed during testing or operation?	1.0 (L)
Results from periodic testing and maintenance are logged into some kind of electronic (or written) maintenance system.	3 %		Have the maintenance operators been given particular training with respect to understanding the detectors' functionality, critical failure modes and registering maintenance notifications in order to give a good description of e.g. failure cause, detection method and failure modes?	1.0 (L)
As above	3 %		Are maintenance notifications regularly gone through in order to reveal repeating detector failures, to compare results for all relevant detectors across the facility, and to initiate and perform root cause analysis in order to identify measures to remove these failure causes?	1.0 (L)
Incorrect calibration and/or adjustment of zero point may cause malfunction of the gas detectors	10 %		Have measures been implemented to avoid incorrect calibration / zero point adjustment such as special training of operators, 3rd party checks, high quality procedures and/or particular tools for calibration?	1.0 (L)
Incorrect calibration may cause the detector not to respond to all type of relevant gases in the different areas (e.g. laser-based line gas detectors in weather exposed areas)	5 %		Have measures been implemented to ensure that the gas detectors respond to all different gases / gas-compositions in the area?	1.0 (L)
Adding new detectors or replacement of detectors may become relevant during the operational phase	5 %		Are there (management of change) procedures in place for independent checks after detector replacements and modifications, e.g. related to exhaustive testing of updated logic and voting configurations?	1.0 (L)
Subtotal modification factor for 'Operation, maintenance & modifications':				

Aggregated modification factor

A.2.2 Fire detectors (incl. flame, smoke and heat)

CCF category	*Weight*	*Relevance*	*Defences*		*Mod. Factor*
Design properties (incl. location)	**35 %**	**Y/Pre/NA**	**Description of defence**	**Eff.**	
The applied fire detectors are of the same type (make, manufacturer, material selection, etc.).	10 %		Has the design been reviewed with the purpose of revealing common vulnerabilities and are defences implemented to reduce the effect of any such common vulnerabilities (separation, diversity, etc.)	1.0 (L)	
The fire detectors contain specific parts that highly influence the reliability of the detectors.	5 %		Has specific analyses been performed or measures been implemented to ensure that the reliability of *particularly critical parts* such as filters, lenses, sensors, junction boxes etc. are good.	1.0 (L)	
Location/layout of redundant detectors is critical in order to ensure optimal detection.	5 %		Has separate analyses/simulations been conducted to verify that (voted) detectors are located such that they will detect gas, even for moderate releases, taking into consideration ventilation conditions, wind, etc.?	1.0 (L)	
The fire detector is delivered with a specified diagnostic coverage factor	10 %		Has it has been verified and documented by analysis (and/or prior use) that the fire detector fulfils the "promised" diagnostic coverage		
Whether the design can be considered fit for purpose is considered an issue for the particular application.	5 %		Is any operational experience related to the specific valve type available, or is prior-use experience available for the valve and relevant for the current application?	1.0 (L)	
Subtotal modification factor for 'Design properties':					
Environmental Control (external & internal)	**30 %**	**Y/Pre/NA**	**Description of defence**	**Eff.**	
The detectors are exposed to snow, rain, fog, icing conditions, sea spray, etc., possibly affecting detector performance?	10 %		Are procedures for removing ice, snow, cleaning lenses/mirrors, avoiding water intrusion, etc. during periods with harsh weather, in place and implemented, and/or are other physical measures installed to protect against harsh environment (e.g. use of silicone to avoid water intrusion into junction boxes, etc.)?	1.0 (L)	
The detectors are subject to external influences such as polluted air, exhaust, sand, dirt, etc. which may influence the performance of the detectors.	10 %		Are procedural measures implemented to avoid and control possible influences from a polluted environment and/or are physical measures implemented to avoid such influences?	1.0 (L)	
The detectors are subject to an external corrosive environment that can affect their performance.	10 %		Are inspection and maintenance procedures in place for controlling and preventing corrosion, and/or have physical measures for control of the corrosive environment been implemented such as material choice, weather protection, etc.?	1.0 (L)	
Subtotal modification factor for 'Environmental control':					

Operation, maintenance & modifications	35 %	Y/Pre/NA	Description of defence	Eff.
The detectors are periodically tested and maintained according to a predefined maintenance program.	3 %		Are test- and maintenance procedures readily available, made familiar among the maintenance personnel, and are they kept continuously updated throughout the operational phase?	1.0 (L)
As above	3 %		Are there routines/procedures in place to periodically review and if necessary adjust the frequency of functional testing for the detectors in light of registered failure history and experienced failure causes?	1.0 (L)
As above	3%		Do the maintenance personnel always check for similar failures on other detectors, if a failure is revealed during testing or operation?	1.0 (L)
Results from periodic testing and maintenance are logged into some kind of electronic (or written) maintenance system.	3 %		Have the maintenance operators been given particular training with respect to understanding the detectors' functionality, critical failure modes and registering maintenance notifications in order to give a good description of e.g. failure cause, detection method and failure modes?	1.0 (L)
As above	3 %		Are maintenance notifications regularly gone through in order to reveal repeating detector failures, to compare results for all relevant detectors across the facility, and to initiate and perform root cause analysis in order to identify measures to remove these failure causes?	1.0 (L)
Incorrect calibration and/or adjustment of zero point may cause malfunction of the fire detectors	15 %		Have measures been implemented to avoid incorrect calibration / zero point adjustment such as special training of operators, 3rd party checks, high quality procedures and/or particular tools for calibration?	1.0 (L)
Adding new detectors or replacement of detectors may become relevant during the operational phase	5 %		Are there (management of change) procedures in place for independent checks after detector replacements and modifications, e.g. related to exhaustive testing of updated logic and voting configurations?	1.0 (L)
Subtotal modification factor for 'Operation, maintenance & modifications':				

Aggregated modification factor

Technology for a better society

www.sintef.no