NTNU

Norwegian University of
Science and Technology

Spurious activations of safety-instrumented systems

Mohammad Amin Ghanooni

Reliability, Availability, Maintainability and Safety (RAMS)
Submission date: September 2015
Supervisor: Mary Ann Lundteigen, IPK

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

NTNU
Norwegian University of
Science and Technology

Spurious activations of safety-instrumented systems

Mohammad Amin Ghanooni

2015

MASTER THESIS

Department of Production and Quality Engineering

Norwegian University of Science and Technology

Supervisor: Mary Ann Lundteigen

Preface

The work with this thesis has been carried out in the last semester of my Master's degree in Reliability, Availability, Maintainability and Safety (RAMS Engineering) at the Norwegian University of Science and Technology (NTNU). The title of the thesis is 'Spurious activations of safety-instrumented systems' and it is written under supervision of professor Mary Ann Lundteigen at the Department of Production and Quality Engineering.

I worked with maintenance management related topic in my specialization project. However, I decided to choose a topic within safety and reliability to improve my knowledge within this field as well. It is assumed that the reader has some basic knowledge about reliability of safety systems and is preferably familiar with the textbook System Reliability Theory: Models, Statistical Methods, and Applications by Rausand and Høyland (2004).

I appreciate Mary Ann for helping me with choosing this interesting topic which is going to be more applicable in practice in industry. We have had many informative and constructive conversations during the supervision process.

Trondheim,
September 2015

Mohammad Amin Ghanooni

Acronyms

CCF	Common cause failure
ESD	Emergency Shutdown
FMEA	Failure Mode and Effect analysis
FMEDA	Failure Mode Effect and Diagnostic Analysis
HIPPS	High Integrity Pressure Protection System
IEC	International Electrotechnical Commission
ISA	the international society for measurement and control
ISO	International Standards Organization
ISO/TR	International Standards Organization/Technical Report
OREDA	Offshore reliability data
PDS	Norwegian abbreviation of "reliability of computer-based safety systems"
PE	Programmable electronic
PFD	probability of failure on demand
SHH	Spurious high level alarm
SO	Spurious operation
SIF	Safety-instrumented function
SIS	Safety-instrumented system
SLL	Spurious low level alarm
STR	Spurious trip rate

Executive summary

Safety-instrumented systems (SIS) play an important role in many industry sectors including nuclear, aviation and oil & gas industry. SIS's are intended to detect the onset of hazardous events and eliminate or reduce the consequences to humans, the environment, and assets. However, the unnecessary safety may influence the production regularity and thereby impose unwanted costs on the end-user. On the other hand, it may lead to stress on components and systems and even hazardous events.

Spurious trip rate (STR) is introduced in industry to quantify the so-called unwanted safety. Several formulas are introduced to calculate STR which have been explained in this thesis. In order to understand the spurious concept better, failure classification in different standards and technical reports are described and discussed. Realizing the significance of dangerous and safe failure classification is crucial to understanding the spurious concept in this thesis. Therefore, the failure behavior of a temperature transmitter with respect to its effect on operation is qualitatively evaluated. Spurious activation may have consequences not only on SIS but also on other engaged equipment. This thesis provides several examples to better clarify this issue.

The β factor is the most contributing parameter to STR. This parameter is the mean fraction of all failures of an element that affects all the other elements of the system. Therefore, the methods to quantify this factor are introduced such as IEC 61508 model and Humphreys' method. Two of these methods which are based on similar ideas are described in-depth. However, all of these methods are developed to determine $\beta_{Dangerous}$ (beta-factor for dangerous failures). Therefore, it was essential to propose a new method to quantify β_{safe} (beta-factor for dangerous failures). This thesis develops a novel method to determine β_{safe}. Based on the available data, the method focuses on Humphreys' approach as a basis.

Although the new method was based on Humphreys, the corresponding proposed table of factors and weights was calibrated for IEC 61508 model, since both methods have been developed based on similar ideas. Flame detector was chosen to obtain β_{safe} based on the proposed approach as a case study.

The obtained factor-weight table in the proposed method is calibrated for the beta-factor range in both Humphreys' method and IEC 61508 model. Therefore, two tables are proposed based on the beta-factor range in above-mentioned methods. Besides, the results from the case study show that the difference between the obtained beta-factors from the two methods is due to the fact that each method incorporates a different beta-factor range. As a result, the SIS designer can choose a 'factor-weight' table based on their desired beta-factor range.

Chapter 1

1 Introduction

1.1 Background

Reliability is an important property of the safety instrumented system (SIS). A high SIS reliability is often achieved by high level of redundancy, which in turn may result in frequent spurious activations. The SIS is intended to provide the safety of the process. However spurious activation (unintended safety) may result in hazardous events (Lundteigen and Rausand, 2008) and high costs (Dang et al., 2015; Lundteigen and Rausand, 2008; Machleidt and Litz, 2011).

In order to understand the spurious activation concept better, it is essential to realize the 'dangerous and safe' failure classification and make a distinction between them. The influence of safe failures on the SIS availability has been discussed by reliability engineers, yet a firm conclusion has not been drawn.

Widely used standards such as IEC 61508 (2010) which is applicable to all kinds of industry, and IEC 61511 (2003) which is used for the process industry describe the above mentioned classification. IEC 61508 (2010) part 4 gives a clear definition of safe failure which is used as basis in this thesis for spurious activations. This Standard describes safe failure as a failure which results in spurious operation or increases the probability of the spurious operation of the safety function. This failure classification is described in ANSI/ISA-84.00.01 (2004); ISA-TR84.00.02 (2002); ISO/TR 12489 (2013); OREDA (2009); SINTEF (2013b) as well. Lundteigen and Rausand (2008) have classified spurious activation into three categories including spurious operation, spurious trip and spurious shut down to clarify the spurious trip concept.

Due to the consequences of spurious activations, it is essential to calculate spurious trip rate (STR). Different formulas are suggested in order to calculate STR in ISA-TR84.00.02 (2002); Lundteigen and Rausand (2008); SINTEF (2013b). Lundteigen and Rausand (2008) have proposed a new approach for STR calculation which includes β_{safe}. However the proposed formulas by ISA-TR84.00.02 (2002) and SINTEF (2013b) do not include β_{safe}. In other words, $\beta_{Dangerous}$ is considered to be same as β_{safe}. This leads to more conservative value for STR compared to the new formula introduced by Lundteigen and Rausand (2008). Spurious trip rates for different configurations using the above-mentioned formulas, show that the weight of beta-factor increases for configurations including redundancy; especially when M≥2 in a MooN configuration.

Hokstad and Rausand (2008) describe different models for determination of beta-factor. IEC 61508 (2010) and Humphreys (1987) have proposed methods for evaluating $\beta_{Dangerous}$ which is plant-specific. Unfortunately, there is no methodology for obtaining a value for β_{safe}. All methods described in Hokstad and Rausand (2008) are developed to

determine $\beta_{Dangerous}$. SINTEF (2015) has introduced check lists for equipment groups such as fire detectors to adjust the average estimated β values for specific equipment. These checklists are introduced for determining $\beta_{Dangerous}$. Therefore, there is a substantial need for proposal of a new approach to determine β_{safe}. This thesis addresses this need comprehensively.

1.2 Objectives

The objectives of this thesis are to:

1. study possible causes and categories of spurious activations of SIS.
2. discuss possible consequences of spurious SIS activations and elaborate on why it is important to reduce the frequency of such activations
3. perform and document a literature survey related to how to model and quantify the frequency of spurious SIS activations.
4. propose a new approach to determine the spurious activation frequency on the basis of item 3.
5. select a suitable case study (in agreement with the supervisors) and determine the frequency of spurious SIS activations for this system.
6. identify and describe topics within the Framework of this master's thesis that require further work.

The main objective of this thesis has been the determination of β_{safe} since it is the most contributing factor in STR calculation for redundant architectures. To achieve this goal, a suitable method was chosen based on the available data to determine the value of β_{safe}.

1.3 Limitations

The main focus in this thesis is SIS applications in the oil and gas industry and within the context of IEC 61508 and IEC 61511.

It was first decided to select the IEC model to determine β_{safe}. It was later found out this would not be possible due to an extensive model and lack of data. Therefore, Humphreys' method was chosen since it is based on a similar idea to IEC model and a suitable approach to obtain plant-specific beta.

The data selected for calibrating Humphreys' factor-weight table is taken from OREDA (2009). This data is collected from the population of 918 fire and gas detectors in 20 installations. According to Cooper et al. (1993), data selection is very critical with respect to failure mechanism categorization since they are dependent on component type, system type (e.g., standby or normally operating), and operating environment. Since flame detectors are studied in the case study, the following is assumed due to lack of concrete data:

- The component type is flame detector
- Detectors are normally operating
- Operating environment on all installations has been the same

The main argument for determining the weights for the sub-factors (defensive measures) is that there is not enough data with respect to CCFs. The only available data that is used in this thesis are from OREDA (2009). Howerver, OREDA (2009) does not define whether failures, in failure rate data table for fire and gas detectors, are independent or CCF. Therefore, it is assumed that the sum of failures include both independent and CCF. The data which are used in this thesis to derive the factor-weight table for the proposed method, are taken from failure mechanisms vs. failure modes table for fire and gas detectors. The figures in this table are percentages. Therefore, the distribution would be the same for both independent and CCFs.

The main argument for determining the weights against the sub-factors (defensive measures) is that there is not enough data with respect to CCFs. It has neither been possible to access expert judgments.

Furthermore, some decision-making has been done in order to define defensive measures against safe CCFs. This has been done according to available data in OREDA (2009) and defensive measures in Humphreys (1987). Since the defensive measures in Humphreys' method are introduced againt dangerous failure, these measures have been translated to safe failures.

1.4 Structure of the report

In Chapter 2, failure classifications based on different standards and technical reports are described. 'Dangerous and safe' failure classification is described specifically since realizing the significance of dangerous and safe failure classification is crucial to understanding the spurious concept in the next chapter. In Chapter 3, three categories of spurious activation including spurious operation, spurious trip and spurious shutdown are discussed. Chapter 4 describes consequences of spurious activation on SIS and other equipment using several examples. In Chapter 5, spurious trip rate formulas are introduced and explained. Chapter 6 describes the Humphreys' method and uses it as a basis for developing the proposed method. It also includes a case study using the proposed approach. Conclusions and recommendations for further work are provided in Chapter 7.

1.5 Approach

Possible causes and categories of spurious activations of SIS were studied through looking up the available literature. The concept of spurious activation is presented quite vaguely in throughout the literature. Thus, the focus in this thesis has been to clarify the concept by finding the best possible description of this idea.

Possible consequences of spurious SIS activations are elaborated on using several examples. The undesired effects of spurious activations are discussed and explained why it is important to reduce the frequency of such activations.

A literature survey related to how to model and quantify the frequency of spurious SIS activations was performed. There is no unique formula in order to calculate spurious

trip rate due to different interpretations of spurious activation concept. However, these formulas are compared to find out what is the most contributing factor to the frequency of spurious activation of SIS.

Since beta-factor is the most contributing factor to spurious activation frequency of architectures with redundancy, the new method is proposed to determine beta-factor with respect to safe failures. Based on the available data, the Humphreys' method was found to be the suitable method to develop the proposed method upon. However, the in-depth analysis of Humphreys' method was essential to be able to generate a factor-weight table to determine β_{safe}.

Flame detector is selected as case study to determine 'equipment specific' β_{safe} and a 2oo4 architecture was selected to determine the frequency of spurious SIS activations for this system. The generated table based on Humphreys' method was calibrated for IEC model beta-factor range. Next, the obtained β_{safe} values from both tables applied to the case study and compared.

In recommendations Section of this thesis, topics within the Framework of this master's thesis identified and described based on the findings through the thesis work process.

Chapter 2

2 Failure classification

2.1 Dangerous and Safe failure

In order to understand the spurious activation concept better, it is necessary to investigate failure classifications based on different literature, standards and handbooks.

Lundteigen and Rausand (2008) have proposed a classification of failure modes which encompasses both the IEC standards (IEC 61508 and IEC61511) and OREDA classification of failure modes. They highlight that OREDA, unlike IEC 61608 and IEC 61511, does not do the classification based on the consequence of failures. Critical failures are further classified as safe and dangerous. In order to compare the failures based on their effect on the equipment operation, a temperature transmitter is taken as an example and the failure modes are classified based on being danegrourous or safe.

The data in Fig. 2-1, is taken from exida (2012a). It is often impossible to know which failures are safe versus dangerous at the product level. Therefore the failure rate data for sensors is often generated using functional failure modes (Goble and Cheddie, 2004). Consequently, in order to investigate the failure behavior of a temperature transmitter

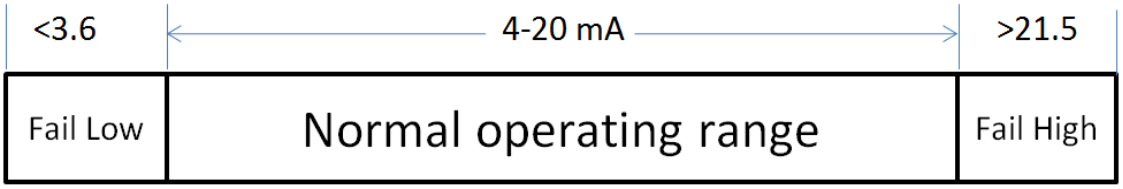

Fig. 2-1: A temperature transmitter normal and failure ranges

with respect to their effect on the operation, the following definitions are required:

Fail high output: failure that causes the output signal to go beyond the maximum output current (21.5 mA)

Fail low output: failure that causes the output signal to go below the minimum output current (3.6mA)

Fail output frozen: failure that makes the transmitter incapable of responding to a demand

Failure output drifting: failure that makes readings offset from the original calibrated state

Failure detected: failure that is detected by the internal diagnostics.

Failure of diagnostics: failure that is known as Annunciation Undetected; Failures within the transmitter that cause loss of diagnostics but do not affect the safety functionality.

Table 2-1: Distribution of dangerous and safe failures per each component of temperature transmitter

Affected component	Failure Mode	Failure Effect	
		Dangerous	Safe
Electronic circuit	Output Frozen	✓	
Sensor (scaled)	Output Low or Frozen	✓	
Sensor (Deformed)	Output high or low	✓	✓
Power supply	Output Low	✓	✓
Transmitter (left in test mode)	Output Frozen	✓	
Sensor seal	Output high or low	✓	✓
Diagnostics	No effect		

In Table 2-1, some failure modes may have both safe and dangerous effects. For example, a temperature transmitter failing high would be a safe failure, if the function normally takes the safe state on high process variable, while the transmitter failing high would be a dangerous failure in the event of a low process variable measurement.

In order to tackle CCFs, the following strategies are rendered useful (Goble and Cheddie, 2004):

- Diversity of redundant components
- Physical separation of redundant components
- Use of energize to trip vs. de-energize to trip systems
- Removal of systematic failures which are relevant to the inherent design of the system rather than random hardware failures
- Performing audits, assessments, and verifications
- Improvement of response time

The same element (Temperature transmitter) is taken as an example to look into effect of two conventional types of sensor elements which are used in the industry despite the emergence of the so-called smart sensors such as wireless sensors. The potential for systematic errors increases if the complexity of SIF increases (Gentile and Summers, 2006). Moreover with any new technology, there is the potential for many unknown failures. These two types of sensors are: Thermocouple and resistance temperature detectors (RTD).

Here factors and decisions influencing CCFs are investigated further:

- Operation and maintenance:

- Calibration errors
- Maintenance errors

Compared to resistance temperature detectors, thermocouples cannot be calibrated after use, since it results in misreading. Classifying an operator making a calibration error as a human error, would not be enough. It is required to look into the underlying human and organizational factors such as procedure quality and training level as well.

As mentioned earlier, improving response time is one way to tackle CCFs (Goble and Cheddie, 2004). In the industry, one way to improve the response time of temperature sensors is to plate the sensor tip with silver or gold and by custom fitting the thermowell. However plating and force-fitting the sensor into the thermowell stresses the sensing element, causing calibration shift or premature failure of the sensor.

Environment stressors are considered as one of the main influencing factors for CCFs Fig. 3-5. Table 2-2 shows which element should be opted for in order to decrease the effect of environmental factor on the common cause.

Table 2-2: Sensitivity of different Temperature transmitter sensors to environmental stressors

Environment stressor	Thermocouple	Resistance temperature detectors
Vibration	✓	
Noise		✓
Heat	✓	
Humidity	✓	✓

- Design, implementation and installation

Plants sometimes apply a thermal compound in the sensor thermowell to improve the response time. Exposure to heat nevertheless can degrade the thermal compound which affects adversely the sensor's response time and may cause seizure of the sensor in the thermowell.

2.2 IEC 61508/61511 failure classification

It is worth clarifying different system failure modes. SIS can fail in two different ways: Dangerous and safe. IEC 61508 (2010) defines dangerous failures as those which prevent the system to perform its intended function on a real demand and have the potential to put the safety-related system in a hazardous or fail-to-function state. In contrast, safe failures are those which do not threat the ability of the safety system to perform its intended function. But the safety function is carried out without an actual demand; i.e. spurious operation. In IEC 61508 (2010) part 4 safe failure is described as follows:

Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) Results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or

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

Therefore, it can be concluded that the dangerous failures contribute to the system PFD_{avg}, while the safe failures contribute to the system STR.

The same definition can be found in IEC 61511 (2003). Safe failure is a type of failure, which does not have the potential to put the SIS in a hazardous or fail-to-function state. Besides that in IEC 61511 (2003) part 1, maximum allowable STR is one of the requirements in order to design a SIF. However, no methodology is given to calculate this rate.

2.3 OREDA failure classification

OREDA handbook includes reliability data collected from oil and gas installations. Failure causes in this handbook are categorized as follows:

- Design-related
- Fabrication/installation-related
- Operation/maintenance related
- Miscellaneous (includes causes which are not in the first three categories)

In OREDA, failure effects are critical, degraded and incipient (Lundteigen and Rausand, 2008).

- Critical: A critical failure is defined as a failure of an equipment unit which causes an immediate cessation of the ability to perform a required function. According to PDS method (SINTEF, 2013b) Required function may be interpreted in two ways:

1. The ability to activate on demand
2. The ability to maintain production when safe i.e. no demands

Therefore, it can be concluded that spurious activation belongs to this category as it leads to unavailability of the function or equipment. It is worth mentioning that dangerous failures belong to this category as they hinder the SIS from performing its required function. In other words, critical failures include both dangerous and safe failures. But among safe failures, spurious trips are accounted as critical.

- Degraded: i.e. some of the functions have failed but the fundamental functions are still present.
- Incipient: the onset of a degraded failure which develops into a degraded failure if no corrective action will be carried out.

2.4 ANSI/ISA 84.00.01 and ISA-TR84.00.02

ANSI/ISA 84.00.01 (ANSI/ISA-84.00.01, 2004) refers to the safe failure as false trip, nuisance trip, or spurious trip.

Mean time to a safe failure is referred to as Mean Time to Failure Spurious in ($MTTF_{spurious}$) in ISA-TR84.00.02 (2002) part 2. It is the estimated time between safe failures of a component or system. The modeling techniques discussed in ISA-TR84.00.02 (2002)-part 1, to evaluate the $MTTF_{spurious}$ for Safety Instrumented Functions are:

- Simplified equations, part 2
- Fault tree analysis in part 3
- Markov Analysis part 4
- Markov Analysis for logic solvers only part 5

The following table, adapted from the introduction part, specifically treats the application of simplified equations, fault tree analysis and Markov Analysis to SISs and makes comparison of their modeling capability.

Table 2-3: Comparison of system analysis techniques presented in ISATR84.00.02-2002

		Simplified Equations	Fault Tree Analysis	Markov Analysis
	Typical Systems Modeled	Simple SIF	SIF with complex relationships	SIF with complex relationships, time dependent requirements, or PE logic solvers
Attributes of Analysis Techniques	Handles different repair times for redundant elements	Not shown	Yes	Yes
	Handles diverse technology for redundant elements	Not shown	Yes	Yes
	Handles sequence dependent failures	No	Difficult	Yes
	Quantification technique	Simple math	Simple math or Boolean Algebra	Matrix algebra
	Provides graphics that allow easy visualization of failure paths	Practical for simple SIF	Yes	More difficult

2.5 PDS

PDS is the acronym for 'pålitelighet og tilgjengelighet av datamaskinbaserte sikringssystemer' which is the Norwegian abbreviation of 'reliability of computer-based safety systems'. The PDS method (SINTEF, 2013b) defines a spurious trip as a spurious activation of a single SIS element or of a SIF. (Norwegian for "Reliability and availability of computer based safety systems"). In the calculation of STR the PDS (SINTEF, 2013b) excludes the dangerous detected failures and considers only the spurious operation failures.

Same as IEC61508 (IEC 61508, 2010), the PDS method (SINTEF, 2013b) has considered the concept of safe and dangerous failures for classifying failure effects. In the sense that, these failures either affect the ability to perform on demand, or the ability to maintain the production when safe, they will be critical. On the contrary, the failures which do not affect the main function of the component are non-critical. Since spurious activation influences the production availability, it belongs to the critical classification of PDS method. The same applies to dangerous failures as they cause an immediate cessation of the ability to perform on demand.

2.6 ISO/TR 12489

As previously mentioned, there is a huge gap between safety and production in the industrial standardization. Higher level of safety does not necessarily mean higher production regularity. For example, improving safety without taking the production availability into consideration leads to architectures subject to spurious activations. Designing the safety systems should not only encompass the safety aspects but also spurious activation to achieve the best compromises. The ISO/TR 12489 (ISO/TR 12489, 2013) provides guidelines for evaluating the spurious failure frequencies in order to find good compromises between dangerous and spurious failure probabilities or frequencies. Therefore, the report aims at closing the gap by establishing a probabilistic approach, helping the reliability engineers to properly deal with the probabilistic modeling and calculations of any type of safety systems.

According to ISO/TR 12489 (ISO/TR 12489, 2013), a good balance between safety and production should be taken into consideration in the design phase, regardless of safety system type: mechanical or instrumented. This implies the higher probability of performing the safety function while the number of spurious activations is kept to a minimum.

In parallel with the other standards, ISO/TR 12489 (ISO/TR 12489, 2013) considers a safe state as a state of the process when safety is achieved . However, it pinpoints that the probability of hazardous event with regard to a safety function may increase with respect to safe state of another safety function. Therefore, the maximum allowable STR for the first function should consider the potential increased risk associated with the other function.

ISO/TR 12489 (ISO/TR 12489, 2013) has adopted the concept of safe and dangerous failures in failure classification as in IEC 61508 (IEC 61508, 2010) and PDS method (SINTEF, 2013b). This report has introduced the concepts of critical and non-critical failures as it was described in the previous section. Based on these concepts, safe failures are either critical or non-critical

- Critical safe failure: Initiate the related safety actions when this is not needed
- Non-critical safe failure: Basically increases the probability of success of the safety function

Therefore, spurious activation belongs to the critical category. Spurious failure is also mentioned as a failure which triggers an action in an untimely manner in ISO/TR 12489 i.e. triggered when not needed.

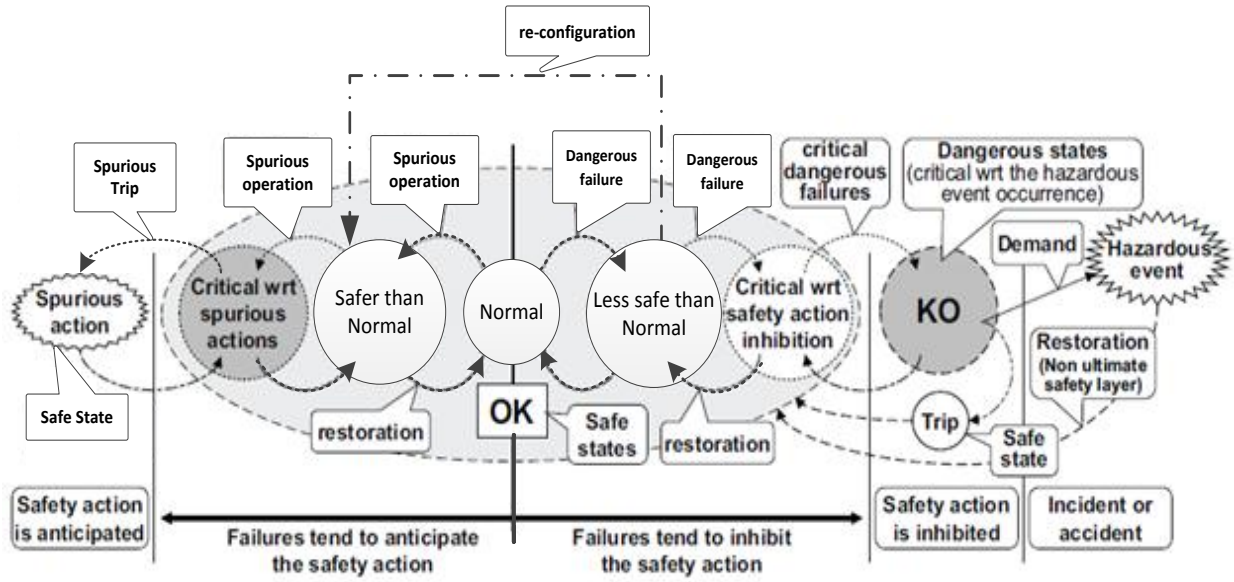

Fig. 2-2: States and failure classification for on-demand mode safety system

The technical report ISO/TR 12489 (2013) states that 'safer than nominal' class is safer from the safety function point of view but degraded from spurious activation point of view. Fig. 2-2 is the modified figure in ISO/TR 12489 (2013). In order to comprehend Fig. 2-2 better, a 2oo3 configuration is taken as an example. If one element has dangerous failure, then we end up with a 2oo2 configuration, as shown in Fig. 2-3. However, if re-configuration is implemented in the logic solver, then the architecture will be re-configured to 1oo2 voting. The new voting is safer than nominal since it is safer from the safety function point of view but degraded with respect to spurious activation. It is not a well described concept, though.

Reconfiguration has been added to Fig. 2-2. If a DD failure occurs, the SIS goes to 'less safe than normal' state. The SIS goes back to safe state using re-configuration.

Whenever spurious operation of one element occurs, it would be safer since fewer signals are required to go to safe state. However, in the 'safer than nominal' definition in (ISO/TR 12489, 2013) degraded has been mentioned with respect to spurious activation point of view. For example, if the spurious signal has been a false demand and one flag is set in the logic solver, so we have M-1 more signals to come to lead to ST. In

other words, there is one flag which we do not know whether it is true or false.

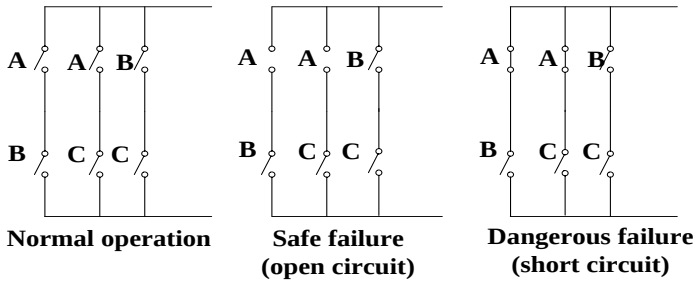

Fig. 2-3: Circuits for temperature transmitters with 2oo3 voting

Two concepts including dangerous failure and critical dangerous failure is introduced in ISO/TR 12489 (2013). It relies on OREDA interpretation of critical failure. A critical failure can be either critical to safety or to production. When it concerns the safety, the critical failure applies to dangerous failures. On the other hand, the critical failure applies to safe failures when it is critical to production. Critical dangerous failure is the last step that prevents the SIF from functioning.

Two terms are introduced with respect to spurious concept:

- critical safe failure
- spurious failure

If the SIF is spuriously activated, it is considered as critical safe failure. Lundteigen and Rausand (2008), call it spurious trip. Spurious failure is called spurious operation in the same article since it is at the element level.

2.7 ISO 14224

ISO 14224:2006 (ISO 14224, 2006) provides a comprehensive basis for the collection of reliability and maintenance data for equipment in all facilities and operations within the petroleum, natural gas and petrochemical industries during the operational life cycle of equipment. According to ISO 14224, the failure mechanisms are basically related to one of the following major categories of failure type:

- Mechanical failures
- Material failures
- Instrumentation failures
- Electrical failures
- External influence
- Miscellaneous

The above classification of failure types is rather coarse. Table 6-6 shows more detailed categorization of failure mechanisms based on the above-mentioned failure types which is recommended by ISO 14224 (ISO 14224, 2006).

Failure modes are categorized into three types in ISO 14224 (ISO 14224, 2006):

- Desired function is not obtained (e.g. failure to start)
- Specified function lost or outside acceptable operational limits (e.g. spurious stop, high output)
- Failure indication is present but no critical impact on equipment-unit function is found. (e.g. initial wear)

Chapter 3

3 Spurious Activation

A spurious operation is an activation of a SIS element without the presence of a specified process demand. Other names such as nuisance and false are also used instead of spurious activation in standards, technical reports, and articles. In the oil and gas industry, production loss is the main consequence of spurious activation but not degraded safety integrity. It can be the reason that both of the IEC standards (IEC 61508, 2010; IEC 61511, 2003) focus on functional safety. There is no focus on spurious activation in these standards, since production loss is relevant to operational integrity.

In both standards, there is almost nothing mentioned regarding spurious activation other than the name of the term itself. IEC 61508 (2010) part 1 considers developing a new safety function as a means to avoid the hazards due to spurious activation of a safety function. A good example for deployment of a new safety function deployment is the water measurement system in a water boiler onboard a vessel. In addition to the low and high level sensors for water level measurement in a water boiler, high-high and low-low sensors are built in as the redundant sensors. In this case, if spurious activation of a low level sensor makes the operator bypass the safety system due to loss of confidence in the system, low-low sensor will still be in place to prevent the hazards of the boiler and the boiler feed pump running dry.

Spurious activation can be categorized into the following three main types (Lundteigen and Rausand, 2008):

1) Spurious Operation
2) Spurious Trip
3) Spurious Shutdown

The dashed arrows in Fig. 3-1, show the link between these types. Spurious operation may lead to spurious trip, and spurious trip may lead to a spurious shutdown.

.

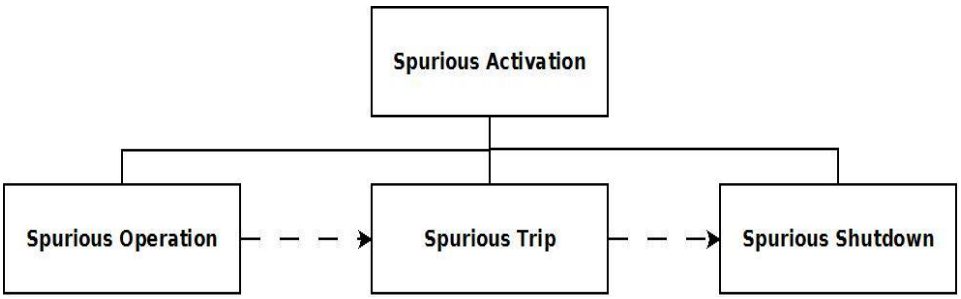

Fig. 3-1: Spurious activation types

In order to understand this concept more deeply, it is fair to investigate the causes for each type. It should be noted that controlling the factors which influence the rate of occurrence of spurious activation cannot be achieved, however it is possible to influence these factors indirectly (e.g., by a higher reliable element in a SIS).

3.1 Spurious Operation (SO)

Activation of a SIS in the absence of the specified demand is called spurious activation. For example, when the sun ray hits a flame detector which is not able to distinguish between false and real process demands, spurious operation is the result.

There are two main causes for spurious operation of a SIS, as shown in Fig. 3-2.

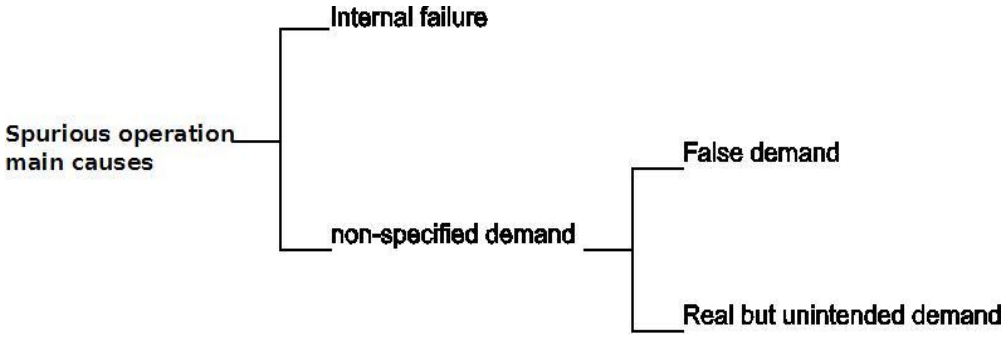

Fig. 3-2: Main causes of spurious operation

Spurious operation failures caused by internal failures, are considered safe failures, while all safe failures will not necessarily result in spurious operation.

The second cause, non-specified demand, can be categorized into two types of demands. It can be explained using a flame detector as an example. When the detector is hit by a sun ray and is activated, this is due to a false demand. On the other hand, when the detector responds to welding, a real but unintended demand is the source.

3.2 Spurious trip

ANSI/ISA-84.00.01 (2004) defines spurious trip as the shutdown of the process for reasons not associated with a problem in the process that the SIF is designed to protect (e.g., the trip due to a hardware or software fault). Alternative terms for spurious trip include nuisance trip and false shutdown.

For a SIS with MooN architecture, M elements or channels are necessary to realize the safety function. In a MooN architecture, SIS fails dangerously if N-M+1 elements fail. On the other hand, if M channels are operated spuriously, this will lead to spurious trip of SIF.

Other causes for spurious trips are (Lundteigen and Rausand, 2008):

- Loss of utilities
- DD failures

In oil and gas industry, some SIFs are supplied by hydraulic systems. For example, the leakage in the hydraulic system can lead to fail-safe-close of a safety valve or in the other words the spurious trip of SIF.

As a requirement in both IEC 61508 (2010) and IEC 61511 (2003), the SIS shall be designed to activate spuriously if DD failures hinder the SIF when it is demanded.

In Fig. 3-3, failure modes are categorized based on dangerous and safe failure modes, and their contribution to spurious trip is shown.

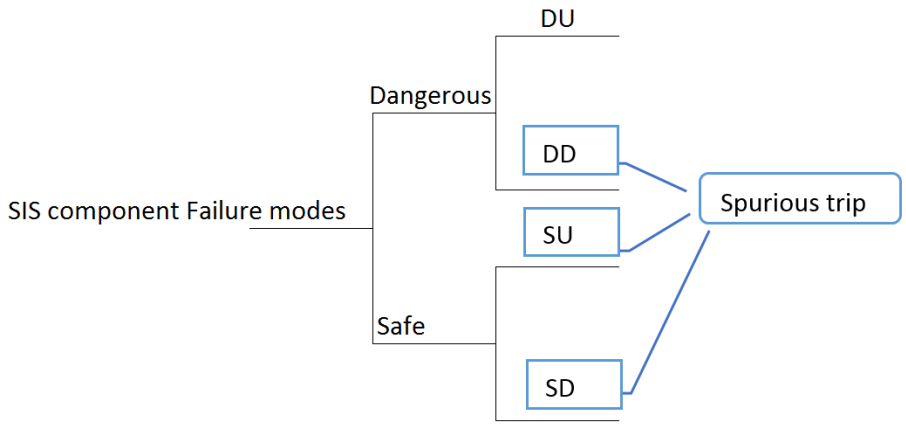

Fig. 3-3: Failure modes classification

As shown in Fig. 3-3 DU failure mode is not a contributor to spurious trip while DD failure mode in addition to safe failure modes can lead to spurious activation. Lundteigen and Rausand (2008) mention SIS configuration and operation philosophy as the factors which determine the number of DD failures which result in spurious trip of the SIS. The former relates to the number of DD failures which may spuriously activate the SIS. The latter applies when the presence of DD failures impede the SIF from functioning on demand. In this case, the system would be tripped manually or automatically.

For example, based on this operating philosophy, for a 1oo3 configuration, one DD failure leads to spurious activation of the SIS. While in a 2oo3 configuration, if the first failure occurs and repair action is initiated, and the element is not restored while the second failure occurs the SIS would be tripped to take the Equipment Under Control (EUC) to the safe state.

3.3 Spurious shutdown

The dashed arrows in Fig. 3-4, shows that the spurious trip may not necessarily lead to spurious shutdown. The spurious shutdown occurs whether the tripped SIF interacts with the process directly or leads to activation of other SIFs. However, the spurious shutdown is not only caused by SIS but also by spurious closure or stop of non-SIS equipment.

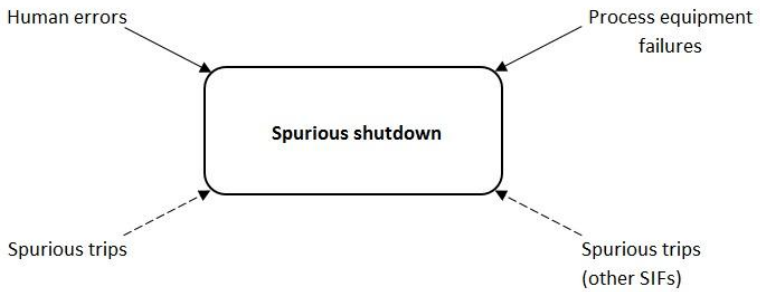

Fig. 3-4: Spurious shutdown causes

Human errors can be another cause for spurious shutdowns. The rate of such errors can be reduced by training and following the procedures. Further investigation of spurious shutdown further investigation is interesting since process start up and shutdown are frequently periods where chances of a hazardous event are high.

3.4 Classification of spurious activation faults

In order to reduce the spurious activation rate and consequently reduce the production loss, one should first establish which defenses and measures are required to reduce the probability of CCFs with respect to safe failures. Although it is not possible to directly eliminate or control influencing factors, it is plausible to control these factors through a set of decisions. Lundteigen and Rausand (2008) consider four sets of decisions and types of failures influenced by each decision:

1. Design, implementation and installation:
   - Random hardware SO failure
   - Response to false demands
   - DD failures
   - Systematic SO failure
   - CCFs
2. Competence and training:
   - Systematic SO failure
   - CCFs
3. Operation and maintenance

- Response to real but unintended demand
- Systematic SO failure
- CCFs

4. Environment:
    - Systematic SO failure
    - CCFs

Taking a look at the above classification shows that all these decisions are likely to influence safe CCFs. Hence it is essential to look into these decisions, and ask questions to address factors that affect the rate of spurious operation with respect to CCFs.

Fig. 3-5 which is adapted from Lundteigen and Rausand (2008) shows the decisions which influence spurious operation with respect to CCF for SISs.

In addition, all of the above-mentioned decisions may influence the systematic SO failures which lead to spurious operation (Lundteigen and Rausand, 2008). Systematic errors are a major source of CCF, and have the potential to disable redundant devices (Center for Chemical Process, 2010). They are not revealed by periodic testing due to non-physical nature (Rausand and Høyland, 2004). For example, it is possible to find out that the specifications of a valve actuator are chosen wrong. However, testing to determine whether the same valve actuator will close on demand is impossible.

The following are the systematic errors which have resulted in process safety incidents (Center for Chemical Process, 2010):

- Risk assessment errors
- Design errors
- Specification errors
- Unexpected operating environment impact
- Installation and commissioning errors
- Operator errors
- Maintenance errors
- Change management errors

In other words, there is a correlation between CCFs and Systematic failures, thus reduction of systematic failures has a major impact in reduction of CCFs.

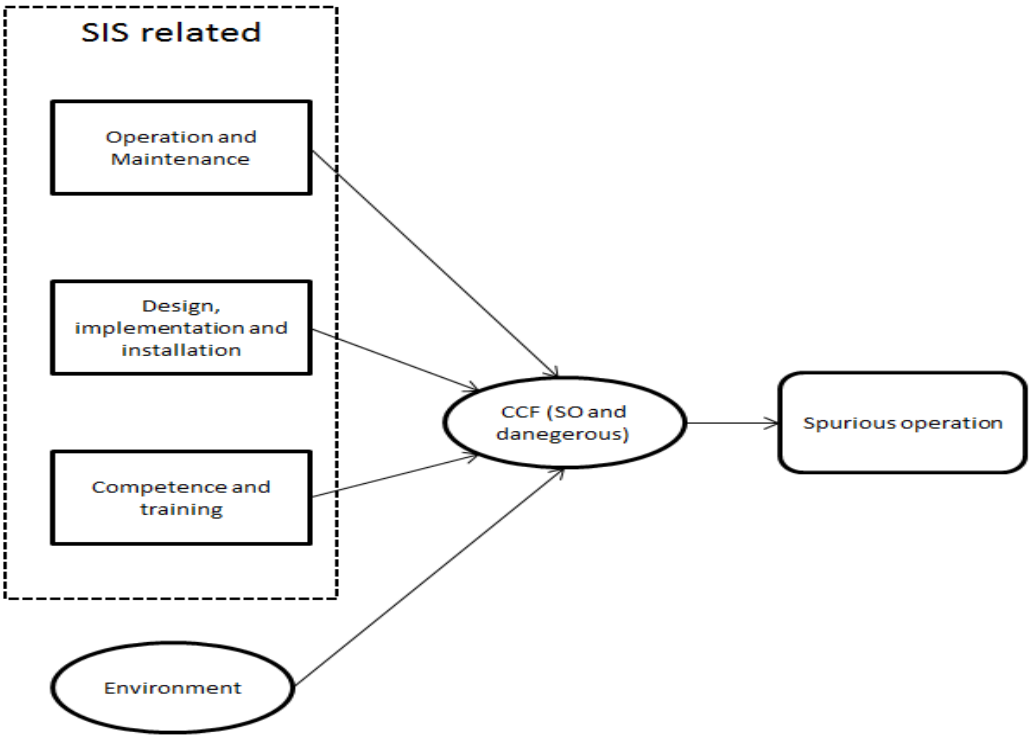

Fig. 3-5: Decisions influencing spurious operation with respect to CCF

A Bayesian network is developed to look deeper into the factors that contribute to β_{safe} as shown in Fig. 3-6. In contrast with Rahimi et al. (2011), environment is considered as

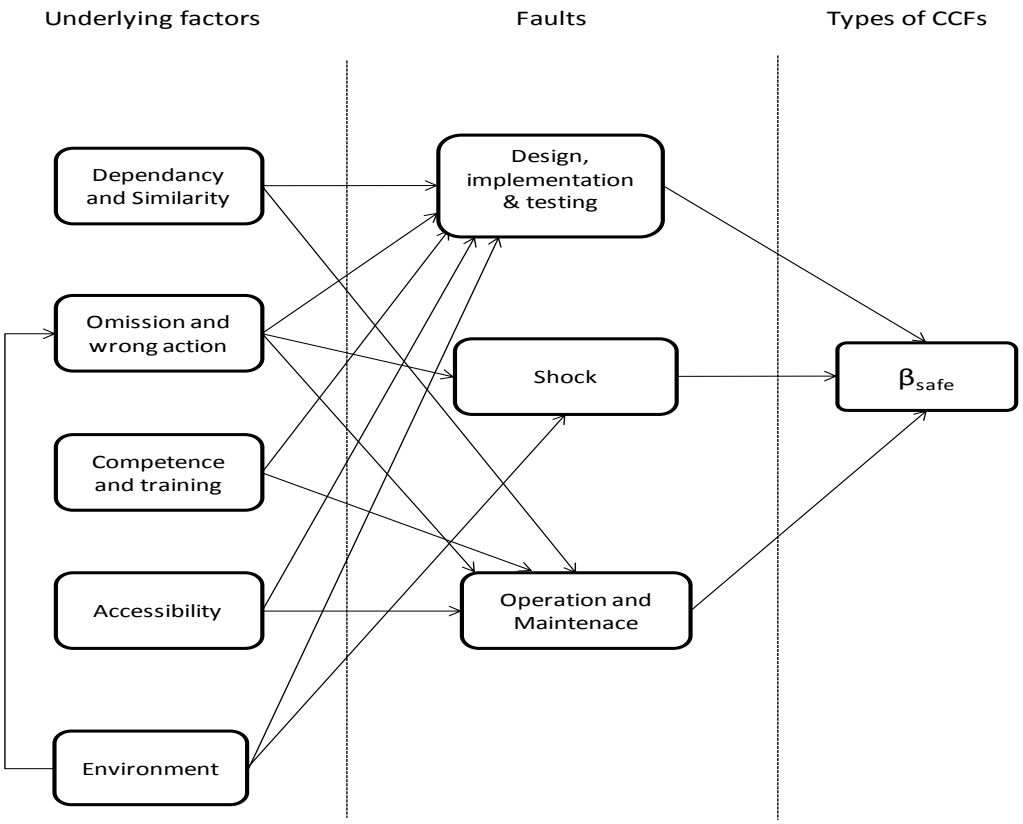

Fig. 3-6: Bayesian network showing the main factors influencing βsafe

an underlying factor. For example, not taking the corrosive environment into the design specification leads to premature failure of a component. Furthermore, environmental conditions like extreme weathers can lead to omission and wrong action. For example, working in hot and humid environment adversely affects the capability of maintenance personnel and may increase the human errors. Therefore, 'environment' is connected to 'omission and wrong action' with an arrow.

Accessibility can result in both the testing and operation and maintenance faults. For example, the correct tightening torque may not be applied to a diesel engine due to lack of space for the wrench movement. Or not good accessibility can lead to wrong testing or ignorance of some components which are not easy to reach.

Chapter 4

4 Consequences of spurious activation

Spurious activation often takes the EUC to a safe state due to 'fail-safe' design. For example, it leads to a false alarm or a spurious valve closure. However, safe failures may have some undesired effects. The following is a list of possible consequences:

- Frequent spurious activation may increase the likelihood of a hazardous event due to increased process demands on other equipment.
- Spurious shutdowns in a production assembly line can lead to more waste material and off-spec products. Lundteigen and Rausand (2008) mention that spurious activation of a SIS will normally lead to loss of production or low availability of the EUC.
- From the business point of view, a subsea compressor trip disturbs production regularity which is costly.
- Complications involved with spurious shut-down and start-up of a plant: According to Jin et al. (2011), it needs time and attention from operators and maintenance personnel to follow up spurious activations. Besides, human errors during restart of the EUC may lead to hazardous events.
- Reduced confidence in alarms
- Environmental emissions such as flaring beside production loss and process start-up complications according to PDS (SINTEF, 2013b)

Here, an example is described with two different scenarios in order to understand spurious activation consequences better:

Description of the system

On a vessel, which is propelled by a 2-stroke diesel main engine, lubrication system plays an important role beside other systems. One of the main elements of this system is the lubricating oil backwash filter. There are two types of backwash filter: Manual and Auto. In auto backwash filters, when the pressure difference across the filters increases, an indication of filter getting clogged is displayed, and the auto system cuts-off the filter and opens the bypass. The auto wash takes place and the dirty oil drains into a sludge tank. On the other hand, in the manual type, the backwash is carried out by the engineer or watch keeper while the pressure difference across the filter exceeds a predefined value. Main engine's control system monitors the oil pressure difference across these filters using two SISs: Low oil pressure and too low oil pressure SIS. Automatic start of a stand-by pump prevents the oil pressure to drop below the shut-down limit.

Scenario 1

Spurious activation of SIS in response to too low oil pressure SIS leads to realizing of safety function i.e. shutdown of the main engine. This can lead to several hazardous events based on the location of the vessel. For example, the vessel can run ashore or in an extreme weather in the middle of the sea, it can capsize if the main engine is not back into operation in time, or collide with another vessel.

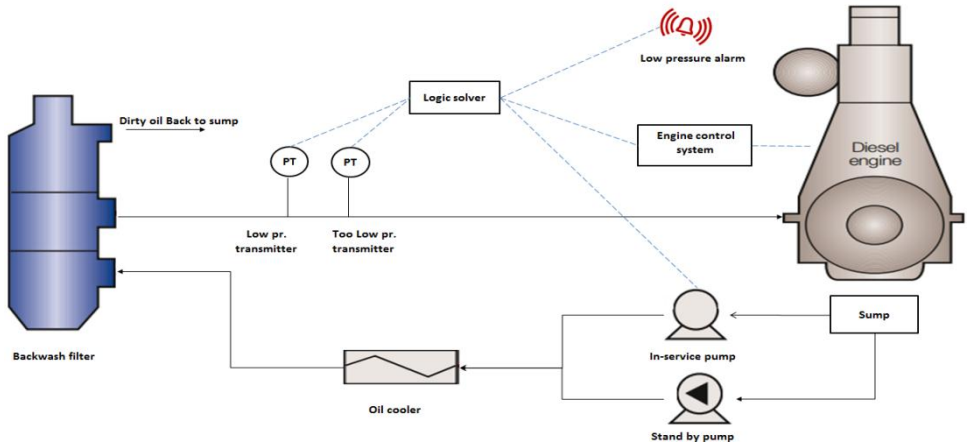

Fig. 4-1: Simplified schematic diagram of Main engine lubrication system on a vessel

Scenario 2

Low oil pressure alarm is spuriously activated several times. This has led to loss of confidence in the alarm, so the operator has bypassed it. There are two possibilities here:

1. Dangerous failure of too low level SIS, in case of oil pressure drop from low level to too low level, leads to seizure of the running engine:
    a. If the stand-by pump does not start to compensate for the too low pressure.
    b. The engine is not shut down manually.
2. Spurious activation of too low oil pressure which is the same as scenario 1

4.1 Spurious activation effect on P-F interval

The concept of P-F curves was introduced by Moubray (Moubray, 1997) to describe the processes of some gradual failures. Rausand and Høyland (2004) introduce P-F interval approach as inspection and replacement policy which is commonly used in reliability centered maintenance. Two points on this diagram are worthwhile to be investigated further. The first point which is called potential failure or point 'P' on the diagram, which is the point where failure becomes detectable. From this point onwards, the degradation accelerates, until it leads to functional failure, shown as point 'F' in Fig. 4-2.

According to Guo et al. (2014) offshore pipeline failures can also be described using P-F curves, for example pipeline failure due to wave and flow induced vibration.

This model is suitable for equipment which are exposed to random shocks (Rausand and Høyland, 2004). P-F interval in the real world is not deterministic but stochastic i.e. point 'P' and point 'F' both can vary over a large range. Therefore, T_p and T_f are random variables. The following are the reasons behind it (Castanier and Rausand, 2006):

- Different pipes have different failure times which depend on the quality of materials, type of coating and the thickness of wall
- Corrosiveness and erosiveness of the internal fluid

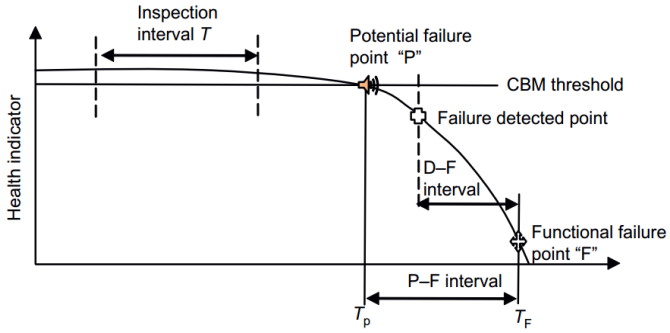

Fig. 4-2: P-F interval graphical representation

In addition to above mentioned parameters that affect T_p and T_f values, stresses due to spurious activation of SIS on the EUC and the SIS itself should be also considered. In a practical but not scientific article, Panikkar (2014) highlights spurious trip effect on piping and equipment, especially when the piping is in the P-F interval. In this interval, the equipment is in the wear-out period. In other words, it is a period when the equipment approaches the end of its lifetime. Spurious operation can give stress to the equipment and as a result, deteriorate both the SIS and the EUC. For example, sudden pressure build-up in the upstream side of a pipeline due to spurious closure of shut down valve which gives a shock to the pipeline can accelerate the failure mechanism.

4.2 Design and spurious activation

Electrical circuit breakers are used to interrupt power circuit under normal conditions or to interrupt this circuit under fault or emergency conditions in order to prevent hazard prevention and mitigation in the process industry. Circuit breakers switch and protect medium and high voltage distribution systems by interrupting fault or short-circuit currents. Circuit breakers are used to switch and protect low and medium-voltage motors as well. Energize-to-trip signal from the safety logic solver is used to operate the circuit breaker to initiate shutdown of a large electric motor. Two goals are achieved if energizing the tripping coil is applied for fail-safe design:

1. Reduction in weight as well as risk reduction due to less generated heat
2. Reduction in STR

If the circuit breakers are designed on de-energize-to-trip principal, a continuously energized electromagnet is needed to hold the breaker contacts closed against the tripping spring. It is both not feasible since the coil would be too large and extra heat is generated. Energize-to-trip design is especially applicable for medium-voltage circuit breakers (Grattan and Nicholson, 2010). This type of design leads to process uptime since an external source of energy trips the circuit breaker in case of a fault in the circuit although loss of tripping signal itself can lead to hazardous events. However according to Grattan and Nicholson (2010) a battery bank as redundant back-up power is used in the event of a main AC power failure.

In oil and gas industry, an ESD (Emergency Shutdown) is typically designed as normally

energized i.e. de-energize-to-trip. It results in high safety integrity. However, increased spurious trips are expected. In fire and gas systems (F&G), spurious trip can have dangerous results. For example, spurious activation of a water deluge system inside a compartment on board a vessel can cause damage to equipment and can be hazardous to personnel. In other words, the electrical equipment contact with water causes the mal-operation of dynamic positioning system of a vessel, or the personnel may get electrified. Therefore, it is common to design an FGS as energize-to-trip.

Over-current protection is a fundamental requirement to reduce hazards associated with power distribution system. To protect the system, overcurrent relays are used to isolate the faulted line or equipment. However, overcurrent occurs in normal operating condition too. Lotfifard, Faiz and Kezunovic (2012) mention induction motors and transformers as two main sources for generating overcurrent under normal operating conditions.

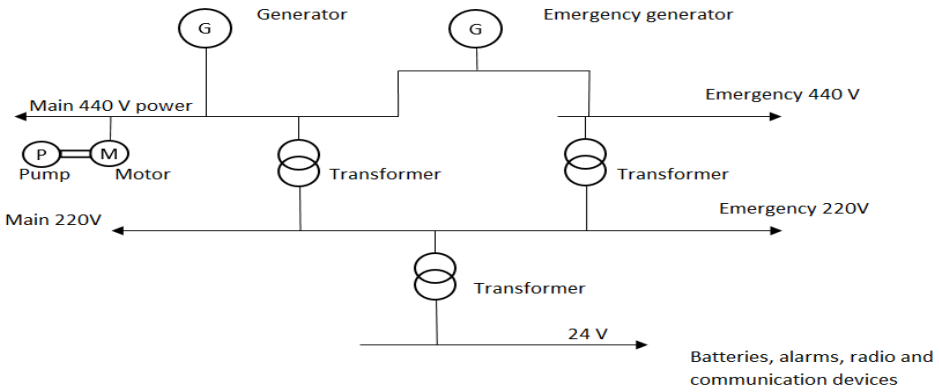

Fig. 4-3: Simplified diagram for electrical distribution system of a ship

When a transformer is energized, an inrush current is expected. The inrush current could reach values as high as 25 times full-load current and will decay with time until a normal exciting current value is reached. Starting of a large induction motor leads to a current typically 5–6 times the rated current and is damped out after a few cycles. As a result, overcurrent relay may be activated spuriously in response to overcurrent in the electrical circuit while it is not due to non-fault event. Fig. 4-3 shows a simplified diagram for electrical distribution system of a ship. In case of the failure of the main power system on board a vessel, an emergency power system is present. Spurious activation of 440V to 220V transformer or 220V to 24V transformer may lead to hazardous events. For example, the former can lead to unavailability of emergency lighting which can consequently cause personal injury due to falling off stairs. The unavailability of communication system because of spurious activation of the latter may lead to a collision.

In oil and gas industry three-phase induction motors are largely used to drive gas compressors, sea water injection pumps and oil exporting pumps (ISO/TR 12489,

2013). Therefore, spurious activation of the induction motor relay, in response to the overcurrent which is generated by the induction motor starting, may disturb the production start-up phase.

In order to prevent spurious activation of over-current relays in response to overcurrent, time delay is applied to initiate relay trip command. On the other hand, the relay sensitivity is reduced due to this imposed delay during the fault. Therefore, the electrical equipment will be damaged for staying in the fault state, though a short time. Lotfifard, Faiz and Kezunovic (2012) have proposed a method to rectify this problem. Based on their idea, the relay should have two time-current characteristic, fast and slow. The slow characteristic which is the same as the time delay approach for normal operating conditions and the fast characteristic, which does not have such a delay and detects non-fault mode. For detailed description of the proposed method, please refer to (Lotfifard et al., 2012).

An electricity distribution company, which provides the electricity for an industrial region, would be obliged to pay the penalty to the customer in case of spurious activation of a transformer's protection relay which has led to blackout.

In the following security system, Fig. 4-4, which is deployed for the buildings' escape doors, smart card reader is used to access these doors in off hours. The reader interfaces with a PC for its processing requirements. Apart from the processing segment, which its elements are not shown and described here, the communication of data is carried out between the card reader and the following:

- Door sensor
- Door lock
- Exit button
- Fire alarm

The door sensor is programmed to open the lock during business hours. For entry into buildings during off hours, specific clearance codes are programmed into a cardholder's record so that the individuals who are authorized can access these doors. Exit button is integrated into this system to be used during off hours while the door sensor does not function. The door security system is programmed to open automatically upon activation of the fire alarm system. Although it can help with faster evacuation, it provides access to the persons who are not authorized to enter the building. The unwanted granted access probability increases upon spurious activation of fire alarm system. This can pose a theft or sabotage risk to the properties in the building especially during off hours.

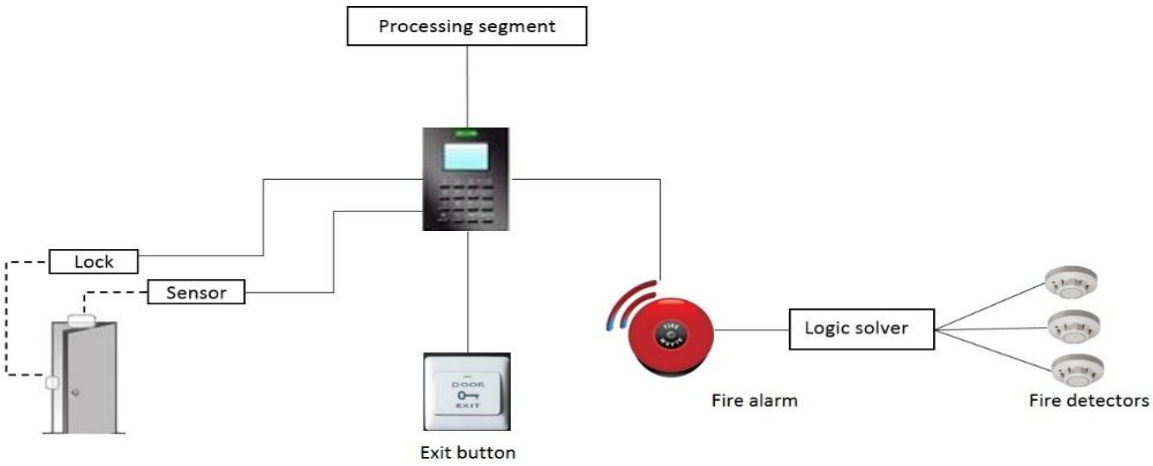

Fig. 4-4: Security system of a building

Chapter 5

5 Quantification of spurious activations

5.1 Spurious Trip Rate calculation

Apart from getting an insight into why spurious activations occur, modeling and quantifying of spurious SIS activations are important factors to be accounted for when selecting SIS design.

There are different approaches in order to calculate STR:

- Simplified formulas
- PDS method
- ISA approach

As previously mentioned, spurious activation is of little concern to IEC 61508 (IEC 61508, 2010) and IEC 61511 (IEC 61511, 2003), and thereby no or vague requirements related to spurious activations are provided. IEC 61508 has no requirements while IEC 61511 mentions maximum STR without giving more details on how the rate should be modeled and calculated.

Lundteigen and Rausand (2008) define STR as the mean number of spurious activations of the SIF per time unit while PDS (SINTEF, 2013b) defines STR as the expected number of spurious activations of the SIS per time unit. In other words, in PDS method spurious activation of a SIS leads to spurious trip. Since there is no unique interpretation of the spurious trip concept, comparing the results of STR calculations does not seem an easy task due to different assumptions underlying different formulas.

As discussed in Section 2, three new definitions related to spurious activation are introduced (Lundteigen and Rausand, 2008); spurious operation, spurious trip, and spurious shutdown. These definitions are rendered essential in order to calculate the STR.

Lundteigen and Rausand (2008) have proposed an approach that has leaded to new formula for calculating STR. Based on three main causes of spurious trips, which are spurious operation, dangerous detected failures and loss of utilities, new formulas are introduced.

Lundteigen and Rausand (2008) point out that their proposed formula (5.1) underestimates spurious trip rate slightly, for a KooN structure when $k \geq 3$.

$$STR_j^{koon} = n(1-\beta_j^{SO})\lambda_{SO,j}\left[\sum_{m=k-1}^{n-1}\binom{n-1}{m}p^m(1-p)^{n-1-m}\right]+\beta_j^{SO}\lambda_{SO,j} \quad (5.1)$$

The above formula has two parts: The first part accounts for the independent failures while the latter cater to CCFs. The probability that an element in SIS will have a SO-failure in the restoration interval is approximated to be:

$$p = (1-\beta_j^{SO})\lambda_{SO,j}\mathrm{MDT} \quad (5.2)$$

It is possible to simplify formula (5.1). However, two arguments can be given regarding the approximation. The first is the argument in this thesis while the second one is based on Lundteigen and Rausand (2008); Rausand (2014).

1) To get a spurious trip in a KooN configuration, k elements out of n elements should be spuriously operated. It can be argued that the following formula can give a more reasonable output, since the spurious operation of n-k remaining elements has no impact on the spurious trip of the SIS. There is a finite probability that independent failures could occur in all channels of a multi-channel system so that all channels will be simultaneously in a failed state. In other words, independent failures are assumed to occur randomly with time. Therefore the probability of such failures affecting parallel channels at the same time is low compared to the probability of a single channel failing. Therefore formula (5.1) may be approximated to formula (5.3).

$$STR_j^{koon} = n(1-\beta_j^{SO})\lambda_{SO,j}\left[\binom{n-1}{k-1}p^{k-1}(1-p)^{n-k}\right]+\beta_j^{SO}\lambda_{SO,j} \quad (5.3)$$

2) Formula (5.1) is based on binomial distribution and thereby probability theory. It means that the item either fails or continues to function while the probability that several items fail at the same time exist regardless of CCFs. For example, in a 2oo4 configuration, the SIS will have spurious trip if at least two items will be spuriously operated. In the meanwhile, when the first element fails and the maintenance (repair) personnel get into the site, 2 of 3 remaining elements may fail simultaneously while the first element is being repaired. Therefore all the probabilities should be added together to gain the correct value for the STR.

Rausand (2014) has approximated the sum in formula (5.1) by the first term based on the fact that $p^{m+1} \ll p^m$ since p is a very small number. Therefore the formula will be as follows:

$$STR_j^{koon} = n(1-\beta_j^{SO})\lambda_{SO,j}\left[\binom{n-1}{k-1} p^{k-1}(1-p)^{n-k}\right] + \beta_j^{SO}\lambda_{SO,j} \quad (5.4)$$

It can be easily seen that both formula (5.3) and formula (5.4) are same. Therefore, both arguments are correct.

Rausand (2014) has applied another approximation in formula (5.4). Since p is very small, then $(1-p) \approx 1$, so the formula can be approximated by:

$$STR_j^{koon} = n(1-\beta_j^{SO})\lambda_{SO,j}\left[\binom{n-1}{k-1} p^{k-1}\right] + \beta_j^{SO}\lambda_{SO,j} \quad (5.5)$$

There are two other STR's which can be added to formula (5.5) in case of loss of utilities or false demands. Since the contribution of these rates are negligible compared to CCF contribution, these rates are not mentioned here, please refer to Lundteigen and Rausand (2008).

In the simplified STR formula by Lundteigen and Rausand (2008) in Table 5-1, the following items are disregarded since their contribution to STR compared to CCF is low:

- False demands, non-intended demands, loss of utilities and systematic failures
- Independent failures occurring during the MDT

Table 5-1: Spurious trip formulas used by different approaches (Lundteigen and Rausand, 2008)

Configuration	Approach		
	New	PDS	ISA
1oo1	$\lambda_{SO} + \lambda_{DD}$	λ_{SO}	$\lambda_S + \lambda_{DD}$
1oo2	$(2-\beta^{SO})\lambda_{SO} + \beta^{DD}\lambda_{DD}$	$2\lambda_{SO}$	$2(\lambda_S + \lambda_{DD}) + \beta^D(\lambda_S + \lambda_{DD})$
1oo3	$(3-2\beta^{SO})\lambda_{SO} + \beta^{DD}\lambda_{DD}$	$3\lambda_{SO}$	$3(\lambda_S + \lambda_{DD}) + \beta^D(\lambda_S + \lambda_{DD})$
2oo3	$\beta^{SO}\lambda_{SO} + \beta^{DD}\lambda_{DD}$	$2.4\beta^D\lambda_{SO}$	$\beta^D(\lambda_S + \lambda_{DD})$
2oo4	$\beta^{SO}\lambda_{SO} + \beta^{DD}\lambda_{DD}$	$4\beta^D\lambda_{SO}$	$\beta^D(\lambda_S + \lambda_{DD})$

ISA-TR84.00.02 (2002) and PDS (SINTEF, 2013b) use $\beta_{Dangerous}$ instead of β_{Safe}. ISA-TR84.00.02 (2002) includes both safe detected and safe undetected failures in their formulas. It is assumed here that λ_{SO} and λ_{safe} are same to be able to compare the formulas in case study Section.

The new approach proposed by Lundteigen and Rausand (2008), assumes that a CCF will affect all channels simultaneously. Therefore, the simplified formula in Table 5-1 is

same for all koon configurations provided that k≥2. ISA has made the same assumption as Lundteigen and Rausand (2008). However, configuration factor is used in PDS (SINTEF, 2013b) to cater for CCFs in configurations other than 1oo2.

PDS (SINTEF, 2013b) uses multiple beta-factor model (MBF), which is a specially designed model, for CCF modeling. The contribution of CCFs in a koon configuration is estimated as $C_{koon}\beta$, where β is the fraction of CCFs among two components and C_{koon} is a correction factor for koon configurations. Therefore, the beta-factor which is used in PDS (SINTEF, 2013b) is different from the standard β in the beta-factor model. For example, for a 2oo4 the correction factor is 2.4, as shown in Table 5-1.

5.2 Total spurious trip rate

Total spurious trip may be calculated as following by adding spurious trips rates formulae proposed by Lundteigen and Rausand (2008):

$$STR_{Total}^{koon} = STR_{1,j}^{koon} + STR_{2,j}^{koon} + STR_{3,j}^{koon} + STR_{4,j}^{koon} \quad (5.6)$$

The indexes in the formula are as follows:

1: refers to spurious trip due to internal failures

2: refers to spurious trip due to false demands

3: refers to spurious trip due to DD failures

4: refers to spurious trip due to loss of utilities

During one of the supervision sessions, an issue was discussed regarding total rate for spurious trips of a SIS. As it is seen in above-mentioned formula there is no term which shows the combination of DD-failures and spurious operations which may lead to spurious trips.

Since the nature of causes for dangerous detected failures and spurious operations are different and consequently, the effect on the EUC will be different. A 2oo3 configuration for too low level transmitters of a water boiler on board a vessel can easily reveal this fact. According to Lundteigen and Rausand (2008), a KooN configuration will fail if at least (n-k+1) of the n elements fail to performs the safety function. On the other hand to have a spurious trip, k of n elements should be spuriously operated. Based on this fact, let's consider the following scenario for a 2oo3 configuration to clarify it better:

Scenario

One of the transmitters gets a DD-failure i.e. it does not perform the intended safety function when it is called for. Simultaneously another transmitter gets spuriously operated due to internal failure and sends a signal showing that the level in the boiler is

low, and necessary actions on the checklist should be performed. This scenario does not lead to either loss of the safety function or the spurious trip of the SIS which is boiler's burner shut-down.

It may also be argued that there is an interaction between spurious operation and dangerous failures as previously discussed in Section 4.1. In the P-F interval, the equipment is in the wear-out period and frequent spurious operation can give stresses to the equipment and as a result, deteriorate both the SIS and the EUC. For example, the deterioration of an ESD valve due to shocks which is induced by spurious operations can cause the valve spindle bending and a probable seizure of the valve in the long run. Therefore, this argument is not valid either to add another term to the formula, since the cause of DD-failure of the ESD valve is seizure of the spindle and the frequent spurious activation has an indirect impact on DD-failure.

5.3 β factor

One way to improve the reliability of SIS is by introducing redundancy. However, CCFs may emerge which inflict a serious threat to the reliability of the SIS and thereby affecting the gained reliability (Rahimi et al., 2011).

Hokstad and Rausand (2008), have described several models for modeling CCFs; among which is the most commonly used, the well-known beta-factor model. Some industries have focused on development of CCF models and collection of data related to CCF such as Nuclear power industry (NUREG-75/014, 1975) and Norwegian offshore industry (SINTEF, 2013b).

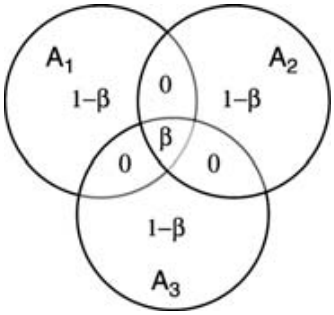

Fig. 5-1: Fractions of different multiplicities of failures for a system with three identical channels when using the beta-factor model (Hokstad and Rausand, 2008)

In order to discuss the beta-factor role in calculating the STR, it is worth describing what β really means. Hokstad and Rausand (2008) consider a system with n identical channels. Given that a specific channel has failed, this failure will, with probability β, cause all the n channels to fail, and with probability (1-β), just involve the given channel. The system will then have a CCF rate $\lambda_C = \beta\lambda$, where all n channels fail. In addition, each channel has a rate of independent failures, $\lambda_I = (1-\beta)\lambda$. The total failure rate of a channel may be written as $\lambda = \lambda_I + \lambda_C$. In other words, the parameter β can be interpreted as the mean fraction of all failures of a channel that also affect all the other channels of the

system.

It should be considered that in the beta-factor model, the multiplicity of the failure event is either 1 or *n*. The intermediate values of the multiplicity are not applicable. This is illustrated in Fig. 5-1 for a system of three identical channels, where A_i denotes failure of channel *i*.

Considering the proposed formulas in Table 5-1, it can be concluded that the β factor starts to show higher weight in STR while the redundancy starts to increase in the SIS configuration. Therefore, it is essential to determine the value of β, since it is the most contributing factor to STR. As a result, it is decided to focus on the methods that beta-factor value can be determined.

Since the original beta-factor was defined for identical channels with the same constant failure rate λ, another approach is proposed to deal with systems with diversified channels. The proposed approach is to define β as a percentage of the geometric average of the failure rates of various channels of the system (Hokstad and Rausand, 2008).

According to Hokstad and Rausand (2008), there are several methods for choosing a more 'correct' beta-factor compared with the estimated β based on generic data. These methods are based on the actual system's susceptibility to possible causes of CCF events.

Beta-factor is influenced by the defenses against CCF events which are implemented in a plant (Hokstad and Rausand, 2008). Therefore β estimates based on generic data are of limited value. There are several methods for choosing a more 'correct' beta-factor compared with the estimated β based on generic data. According to Hokstad and Rausand (2008), these methods are based on the actual system's susceptibility to possible causes of CCF events and are as follows:

- IEC model for determining beta-factor
- Humphreys' method
- Partial beta factor model
- Unified partial model

These methods are designed to determine 'plant specific' β*'s.* However, it should be noted that all these methods were developed to determine 'dangerous beta-factor'.

In IEC61508 (IEC 61508, 2010), part 6, a single "plant specific" can be determined for each of the channel groups of the SIS by using the provided checklist. For more information on other methods, please refer to Hokstad and Rausand (2008). Since a SIS consists of three different parts including input elements, logic solvers and final elements, application specific β-values must be calculated for each part separately.

To estimate β, 37 questions are addressed with regard to following factors:

- Separation/segregation
- Diversity/redundancy
- Complexity/design/application/maturity/experience
- Assessment/analysis and feedback of data
- Procedures/human interface
- Competence/training/safety culture
- Environmental control
- Environmental testing

5.3.1 IEC model for determining beta-factor

These questions should be evaluated for each type of elements of the safety system as mentioned earlier. Taking a look at the above-mentioned factors explains why these areas are focused for estimating the β factor in IEC61508(IEC 61508, 2010), part 6. These factors are defenses which are established against the occurrence of CCFs. Since we intend to reduce the probability of failure due to CCFs, these questions are addressed and evaluated in order to estimate the value of the β-factor.

In the table provided in IEC61508 standard, scoring the PE (logic subsystem) is carried out in a separate column compared to sensors and final elements which are scored in another column. Sensors/final elements and PE (logic subsystem) are then assigned X_i and Y_i scores related to question no. i using engineering judgment, where X_i and Y_i are added. is selected if diagnostic testing leads to improvement against CCFs and Y_i is selected if not. The ratio X_i/Y_i represents the contribution of diagnostic testing as a defense against CCF related to question no. i. Total scores are then calculated using provided formulas in the standard based on whether the diagnostic tests are included or not. Taking into account the diagnostic tests, a factor Z is incorporated into the formula, based on the frequency and coverage of diagnostic test using Tables D.2 and D.3 in IEC 61508 (2010) part 6, to calculate the total score. Finally, Table D.4 in IEC 61508 (2010) part 6 is used to give the estimate of β, using the calculated total score for logic subsystem or sensor/final element.

The value of the beta factor is selected based on engineering judgment. Many owner/operators use a beta factor between 0.1% and 5.0% when good engineering practices like IEC 61508 or IEC 61511 are applied in the design, installation, inspection, and maintenance practices. The beta factor can be substantially higher if good engineering practices are not followed (Center for Chemical Process, 2010).

This checklist will be just useful when it concerns the estimation of β-factor for dangerous detected or dangerous undetected failures. Unfortunately, there is not any similar checklist which helps us with estimation of β-factor for safe failures.

5.3.2 Humphreys' method for determining beta-factor

The Humphreys' method is one of the first methods to determine a plant specific β. It should be noted that the model introduced in IEC 61508 (2010), part 6, annex D is

based on similar idea in Humphreys (1987). In this master thesis, it is decided to use Humphreys' method to introduce a new approach for reducing spurious trip frequency by the dominant factor β.

In addition, it should be noted that SINTEF (2015) has provided equipment specific checklists in order to determine plant specific beta-factor values. However, these checklists are developed for dangerous failure and do not include safe failures.

Humphrey (1987) mentions that fraction of β can be represented by if two or more identical units are used in a redundant channel:

$$\beta = \frac{\lambda_C}{\lambda_I + \lambda_C} \tag{5.7}$$

λ_C and λ_I are CCF rate and independent failure rate respectively.

However, Humphreys (1987) points out that assigning a value to the beta-factor is not an easy task in many practical applications. For example, Humphreys (1987) states that the following wide range introduced in 'Guidance on the safe use of programmable electronic system' document, issued by the health and safety executive, is due to difficulty in assigning a value to the beta-factor.

Identical channel redundancy: 0.03 to 0.3

Diverse channel redundancy: 0.001 to 0.1

Humphreys (1987) argues that this approach in the above-mentioned document is subjective and can be critical in the practice, since a wide range is suggested and then a typical value from these two ranges will be chosen based on the degree of diversity. Therefore a method is suggested by Humphreys (1987) which uses objective criteria to give a value to beta-factor that is defensible in the assessment. Besides, this method can be used as guidance in design i.e. what measures should be adopted to achieve a desired beta factor. The procedure for numerical value allocation to the sub-factors in Humphreys and Jenkins (1991) shows that the beta-factors which correspond to columns 'a' and 'e' are adopted from 'Guidance on the safe use of programmable electronic system' document'. Humphreys (1987) has used the 'Min' and 'Max' of above-mentioned ranges i.e. 0.001 and 0.3 which correspond to column 'e' (best possible β) and column 'a' (worst possible β) respectively.

Humphreys' β factor table can be used in two ways:

1. One may evaluate the existing defensive measures to obtain the value of β factor.
2. One may ask what measures must be taken to achieve a certain β factor.

The first measure will be applied in Section 0 for the case study. It means that each defensive measure is evaluated and a weight is given accordingly to obtain β_{safe}.

5.4 STL and STR

In order to understand the STL concept better, it is wise to take a look at SIL and compare these two approaches.

Safety integrity is a fundamental concept in IEC 61508 (2010) part 4 and is defined as follows:

The probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a specified period of time.

The aim with hazard and risk analysis is to allocate risk reduction to protective functions used to reduce the process risk below risk acceptance criteria (Center for Chemical Process, 2010). This allocated risk reduction is related to its safety integrity level. The risk reduction and integrity level establish a benchmark for the design and management practices used throughout the PIF life. The SIL is in turn defined by the PFD and classified into four discrete levels called safety integrity levels (SIL)(Rausand and Høyland, 2004). An SIL has to be assigned to each safety instrumented function (SIF). The safety integrity level is assigned to safety instrumented functions, and not to the SIS, that may comprise several safety instrumented functions.

In a non-scientific but practical white paper, Houtermans (2006) mentions that process availability is of almost no interest in the existing functional safety standards like IEC 61508 and IEC 61511. When spurious trips are addressed in the industry, the economic aspects and therefore the financial loss associated with the spurious trip is of interest for the stakeholders in industry. However, unexpected shutdown causes a lot of serious safety problems especially process plants like refineries, chemical plants, etc. since these plants run nowadays for a couple of years continuously.

Houtermans (2006) proposes STL for safety functions carried out by safety systems to express economic loss associated with it. For safety systems, STL is directly related to Probability of Fail Safe (PFS), just like SIL is directly related to Probability of Failure on Demand (PFD). He highlights that an end-user prefers safety functions that offer both sufficient safety availability and process availability. As a result, he proposes a new concept which defines performance levels for spurious trips that is called Spurious Trip Level (STL). This measure gives end-users an attribute that helps them define the desired process availability of safety functions according to him.

In other words, the STL is a measurement of how often the safety function is carried out without a demand from the process. As shown in Table 5-2, quantitative requirements are attributed to different STLs and are expressed as probability of safe. PFS (Probability of fail-safe) is the probability that the safety function causes a spurious trip because of an internal failure of the safety function. Houtermans (2006) considers only

the spurious trip due to internal failures while spurious activation can be due to other causes like false demands or loss of containment as described in Lundteigen and Rausand (2010).

Table 5-2: Spurious trip levels

STL	Probability of Fail Safe per year (PFS)	Spurious trip costs in USD (example of an end-user)
X	$\geq 10^{-(x+1)}$ to $<10^{-x}$	…
…	…	…
5	$\geq 10^{-6}$ to $<10^{-5}$	Over 500k and USD 1M
4	$\geq 10^{-5}$ to $<10^{-4}$	Between 200k and USD 500k
3	$\geq 10^{-4}$ to $<10^{-3}$	Between 100k and USD 200k
2	$\geq 10^{-3}$ to $<10^{-2}$	Between 50k and 100k
1	$\geq 10^{-2}$ to $<10^{-1}$	Between 10k and 50k
0	>0 to $\leq 10^{-1}$	Between 0 and 10k

Table 5-2 shows that the lower the probability of spurious trips, the higher the STL. On the other hand, the STL represents asset loss due to an internal failure of a function. The more financial damage the function can cause due to a spurious trip the higher the STL level of the function should be.

The 3rd column of Table 5-2, shows an example of how a company can calibrate its spurious trip levels, depending on which level of financial loss they can or are willing to tolerate. For example, the end-user demands from the suppliers and system integrators STL 3 for the SIS if the financial loss due to spurious trip is estimated to be between 100k and USD 200k. Rausand (2014) criticizes the STL approach and argues that the

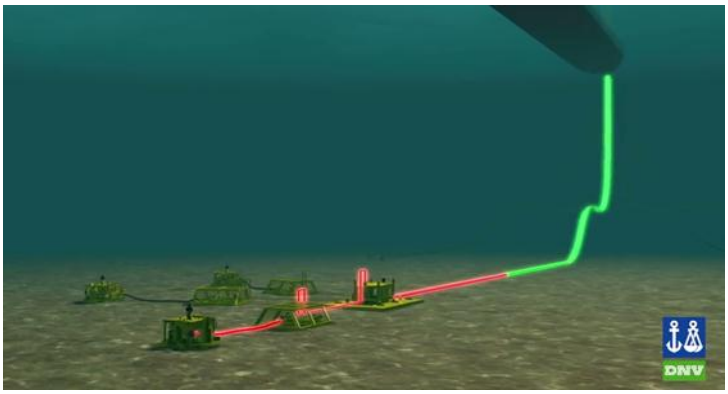

Fig. 5-2: Sub-sea system pipeline

levels are only based on financial loss while other aspects such as safety issue are excluded but he does not elaborate it further.

In order to explain some safety aspects of spurious activation, a spurious closure of a

valve and its consequences in the subsea system is explained. In the subsea system, it is sometimes required that a topside valve such as a riser ESD valve to be closed before the X-mas tree valves on the ocean floor. Similarly, if a hydrate plug or other form of blockage occurs inside the pipeline, product flow would be constrained or even stopped. Pressure from hydrate plug to the topside valve remains low. Pressures upstream from the plug would rise to full shut-in pressure.

The same condition occurs, if for example, subsea isolation valve spuriously closes. There may be no risk with respect to created high pressure in the pipeline due to built-in HIPPS (High Integrity Pressure Protection System) on the pipeline. However, the demand on the safety system causes the logic controllers in HIPPS to trigger the HIPPS valves to close. As a result, internal pressure from the HIPPS valves to the topside never rises above the set pressure. This demand is created on another safety system (HIPPS) that is meant to protect the pipeline. The economic issue is important but potential safety issue can be discussed as well.

Taking the above-mentioned example into account, the STL approach considers only the spurious trip of the isolation valve (PFS) and does not consider the demand on the other safety system (HIPPS). For example the HIPPS may fail on the demand introduces risks on the EUC. One of the advantages of using HIPPS in the subsea is that derated pipelines, i.e. thickness of the wall or other properties reduced, may be used resulting in reduction in the weight considerably. In case of using derated pipeline, the rupture of the pipeline on the low pressure side can be expected. Though, it is also possible that the pipeline with higher thickness which is in its P-F interval to fail due to the shock that is received by the sudden pressure build-up as was discussed in Section 4.1. Besides that, startup and shutdown are the most critical phases of industrial plants. A spurious trip may cause the plant to go through the shutdown and startup again. When the trip occurs, it takes place unexpectedly, people might panic, take the wrong decisions, all with its own consequences. Then a startup needs to happen again. So, besides the financial issues, a lot of safety issues are associated with spurious trips that are not considered in this approach.

Chapter 6

6 Proposed method for determining β_{safe}

6.1 Approach for deriving the method

The proposed approach here is based on beta-factor. As previously discussed in Section 5.3, it is essential to determine the value of β, since it is the most contributing factor to STR. As a result, it is decided to propose an approach to determine the beta-factor. The Humphreys' method is chosen here since the check list in IEC 61508 is very extensive and there are many factors to consider such as diagnostic tests. Besides, there is no data is available to score X and Y which were explained in Section 5.3.1.

This chapter explains the new approach and the new approach has been built on an in-depth analysis of Humphreys' method. The following steps have been done:

1. In-depth analysis of Humphreys' method is carried out.
2. Relevant data from OREDA is selected.
3. Failure mechanisms leading to spurious failure mode identified.
4. Root causes for safe failures identified and discussed.
5. The relationship between root causes and failure mechanisms discussed.
6. Defensive measures against spurious CCFs identified and discussed.
7. Defensives measures weighed against failure mechanisms.
8. New Humphreys' table based on proposed method generated

6.2 Analysis of Humphreys' method

The first step in the Humphreys' method is to introduce a number of factors and sub-factors relevant to common-mode failure. In order to achieve this goal, Humphreys (1987) has used the common mode failure classification in (Bourne et al., 1981). Bourne et al. (1981) classifies common mode failures under four main categories:

- Design
- Construction
- Procedural
- Environmental

Humphreys has reduced these categories to three in (Humphreys, 1987). Sub-categories of construction are 'manufacture' and 'installation and commissioning' (Bourne et al., 1981). The 'Construction' category is perhaps merged into the 'design' category. 'Procedural' has been also replaced by 'operation'. The final main categories (factors) in (Humphreys, 1987) are then as follows:

- Design
- Operation
- Environment

In this thesis, the same main categories are considered for introducing a method for determining equipment specific β_{safe}.

Humphreys (1987) proposes some defensive measures (sub-factors) for each category as shown in Table 6-1. Each defensive measure is described in Appendix A.

Table 6-1: Main categories and defensive measures in Humphreys' method

Main category (factor)	Defensive measure (sub-factor)
Design	separation
	similarity
	complexity
	analysis
Operation	procedures
	training
Environment	control
	tests

Each sub-factor is then classified into five categories from 'a' to 'e' as it is shown in Table 6-4. Numerical values are allocated using the following procedure:

- The sum of column 'a' should correspond to β=0.3 which represents the worst case scenario.
- The sum of column 'e' should correspond to β=0.001 which represents the best case scenario.
- A divisor of 50000 is then chosen to allow for the convenience of whole number. It means that the sum of column 'a' should be 15000 and the sum of column 'e' should be '50' to achieve the target values for β. However the sum of column 'a' is 15100 and the sum of column 'e' is 51 in Table 6-4.
- Column 'a' and 'e' is then filled based on the above mentioned assumptions and expert judgment to find 'a' and 'e' values for each sub-factor.
- The 'a' and 'e' values for each sub-factor were then fitted into the formula (6.1)

$$Y = Ae^{BX} \tag{6.1}$$

The introduced method in Humphreys (1987) has been developed through some iterations. It means that the weighting factors were modified by further discussion among reliability engineers and the original values in columns 'a' to 'e' were not fitted into formula (6.1). According to Humphreys (1987), the final changes to fit the values

into formula (6.1) made little difference to the calculated β i.e. the final β is fairly insensitive to changes in the values in column 'a' to 'e'. However, it should be agreed upon that the difference between columns 'a' and 'b' are quite large (Humphreys, 1987). The large difference between these two columns may be a good reason for reliability engineers to have chosen the exponential function for fitting the values.

The last step in the above mentioned procedure is vaguely stated in Humphreys (1987) without any further explanation. Therefore, it is investigated further here in order to find out how the values in columns 'b', 'c' and 'd' are found by fitting values from columns 'a' and 'e' into formula (6.1).

There are only three items available in order to find the values in corresponding columns:

- Values in column 'a' for each sub-factor (Table 6-2)
- Values in column 'e' for each sub-factor (Table 6-2)
- Formula (6.1) in Humphreys (1987) for finding values in column 'b', 'c' and 'd'

Humphreys (1987) does not mention what each parameter means in formula (6.1). No values are defined for 'X', constant 'A' and constant 'B' in Humphreys (1987). Through further investigation, it is found out that X values are simply integers 1 to 5, while Y values are the allocated weights to each sub-factor. Since we have five weights for each sub-factor, it is proposed here to assign values X=1,2,…,5 to weights e, d,…, a, as shown in Table 6-2. It should be noted that 'e' takes the value of 1, while 'a' takes the value of 5, since 'a' is the worst case scenario and 'e' is the best case scenario. Besides, according to Humphreys (1987), formula (6.1) is acceptable in terms of experience; however no theoretical justification exists behind it.

Table 6-2: Available values for exponential regression

Sub-factor	Weight				
	a	b	c	d	e
	x= 5	x= 4	x= 3	x= 2	x= 1
Separation	2400				8
Similarity	1750				6
Complexity	1750				6
Analysis	1750				6
Procedures	3000				10
Training	1500				5
Control	1750				6
Tests	1200				4

In order to find constants 'A' and 'B' in formula (6.1), the 'Trendline' tool within the plotting environment in Microsoft Excel is used. Next, exponential regression is carried out using x=5 and x=1 and their corresponding values for each sub-factor in columns 'a'

and ‘e’. The exponential function for each curve is then obtained as shown in Fig. 6-1. Since ‘similarity’, ‘complexity’, ‘analysis’ and ‘control’ have identical ‘a’ and ‘e’ values so they overlap in Fig. 6-1. The application specific β can be determined by summing up the chosen weights for all eight sub-factors and then dividing by 50000 (Humphreys, 1987). Assuming that the suggested formula is acceptable, the same formula can be used in developing a similar table for determining β_{safe}.

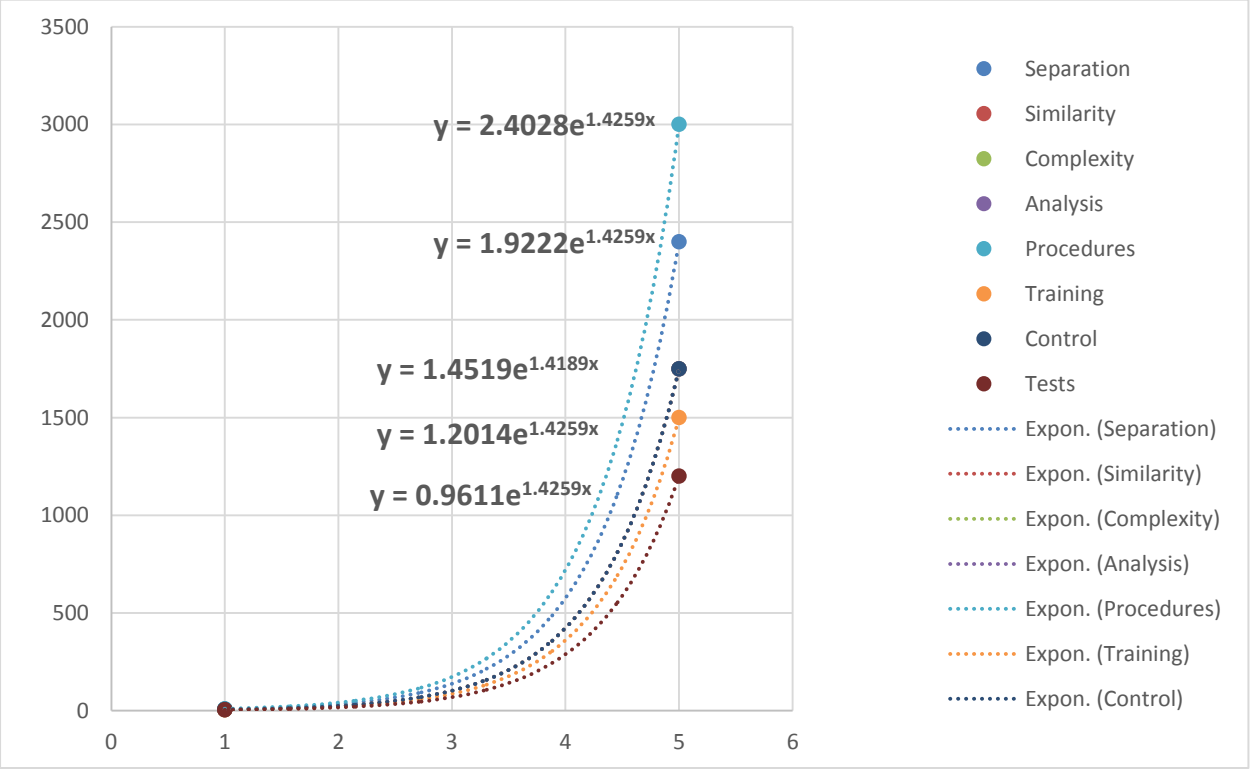

Fig. 6-1: Fitted trends for sub-factors using values in columns 'a' and 'e' in Humphreys (1987)

Constants ‘A’ and ‘B’ are obtained through the exponential regression using a linear model by ‘data analysis’ tool in Microsoft Excel. In order to carry out this regression, ‘y’ values should be log transformed, as shown in step 1 of Fig. 6-2. Therefore, formula (6.1) will be equivalent to formula (6.2) by taking the natural log of both sides of the equation :

$$\ln y = \ln A + Bx \qquad (6.2)$$

Formula (6.2) has the form of a linear regression model as shown in (6.3).

$$y' = A' + Bx + \varepsilon \qquad (6.3)$$

Formula (6.3) is the linear regression model which Microsoft Excel uses to obtain the values for constants ‘A’ and ‘B’. The last term (ε) in formula (6.3) is the error term and is

not discussed here, since it lies outside the scope of this thesis. As mentioned previously, there are only two values (observations) available for each sub-factor i.e. the starting point and the end point. Therefore any type of curve can be fitted into these two points on the graph. However exponential regression is used here in order to remain consistent with Humphreys (1987).

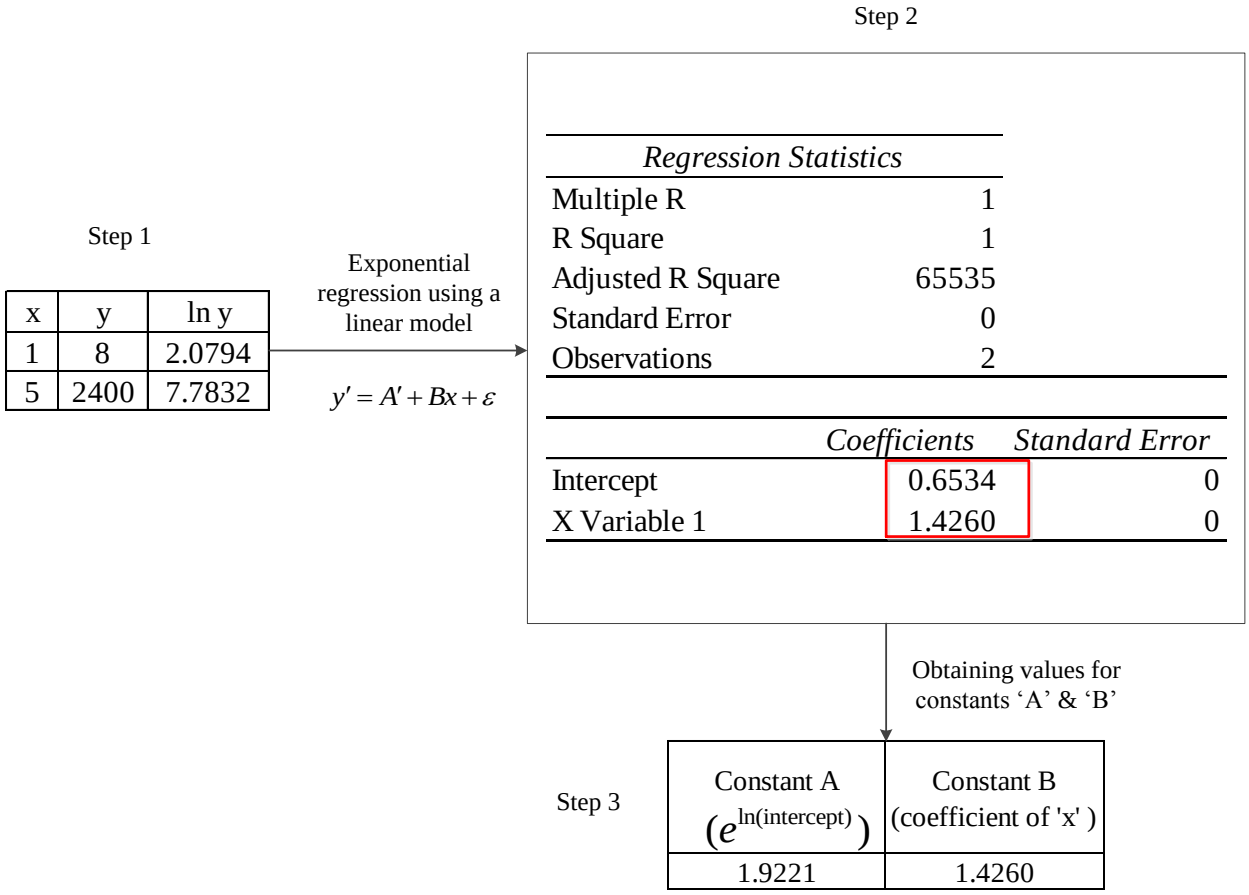

Fig. 6-2: Exponential regression using a linear model to obtain constants 'A' & 'B' in 'Y=Ae^{BX}'

Step 2 in Fig. 6-2, shows the data obtained through regression analysis by Microsoft Excel. Since constants 'A' and 'B' are required, only relevant data are shown here. Therefore, the required data are 'intercept' and 'X variable' coefficients. 'Intercept' is the first term on the right hand side of (6.2) hence, ln A=0.6534.

Constant 'A' is then obtained by taking exponents of both sides, as shown in step 3 of Fig. 6-2. Constant B is the same as coefficient of the x variable in step 2 of Fig. 6-2.

Having defined the values for constants 'A' and 'B' and variable 'x', one can simply calculate the values in columns 'b', 'c' & 'd' using formula (6.1), The obtained 'Y' values for each sub-factor are shown in red in Table 6-3. However, the values in columns 'b', 'c' and 'd' are slightly different in Humphreys (1987) with the ones in Table 6-3 .

Table 6-3: Finding values for columns 'b', 'c' & 'd' in Humhreys' factors and weights table

Factor	Sub-factor	Weight					$Y=Ae^{BX}$	
		a (x=5)	b (x=4)	c (x=3)	d (x=2)	e (x=1)	Constant A	Constant B
Design	Separation	**2400**	**577**	**139**	**33**	**8**	**1.9222**	**1.4259**
	Similarity	**1750**	**423**	**102**	**25**	**6**	**1.4519**	**1.4189**
	Complexity	**1750**	**423**	**102**	**25**	**6**	**1.4519**	**1.4189**
	Analysis	**1750**	**423**	**102**	**25**	**6**	**1.4519**	**1.4189**
Operation	Procedures	**3000**	**721**	**173**	**42**	**10**	**2.4028**	**1.4259**
	Training	**1500**	**360**	**87**	**21**	**5**	**1.2014**	**1.4259**
Environment	Control	**1750**	**423**	**102**	**25**	**6**	**1.4519**	**1.4189**
	Tests	**1200**	**288**	**69**	**17**	**4**	**0.9611**	**1.4259**

Table 6-4 shows the same values in factor-weight table in Humphreys (1987). It seems that the experts or reliability engineers have rounded off the calculated values in columns 'b', 'c' and 'd' in Table 6-4 to have a multiple of five in these three columns. Table 6-4 is considered as the basis for the proposed method in Section 6.3 for determining β_{safe} since it is same as the factor-weight table in Humphreys (1987).

Table 6-4: Completed version of factors and weights of Humphreys' method

Factor	Sub-factor	Weight					$Y=Ae^{BX}$	
		a (x=5)	b (x=4)	c (x=3)	d (x=2)	e (x=1)	Constant A	Constant B
Design	Separation	**2400**	**580**	**140**	**35**	**8**	**1.9738**	**1.4215**
	Similarity	**1750**	**425**	**100**	**25**	**6**	**1.4502**	**1.4184**
	Complexity	**1750**	**425**	**100**	**25**	**6**	**1.4502**	**1.4184**
	Analysis	**1750**	**425**	**100**	**25**	**6**	**1.4502**	**1.4184**
Operation	Procedures	**3000**	**720**	**175**	**40**	**10**	**2.3608**	**1.4298**
	Training	**1500**	**360**	**90**	**20**	**5**	**1.1871**	**1.4298**
Environment	Control	**1750**	**425**	**100**	**25**	**6**	**1.4502**	**1.4184**
	Tests	**1200**	**290**	**70**	**15**	**4**	**0.9137**	**1.4369**

Table 6-4 is the completed version of the existing table in (Humphreys, 1987). In order to obtain the values for constants 'A' and 'B' for each sub-factor, the same procedure to obtain these constants' values in formula (6.1) is carried out. The procedure steps are shown in Fig. 6-3 for separation sub-factor.

The same has been done for the seven remaining sub-factors, and values of constants 'A' and 'B' are then entered in Table 6-4.

The rounded values in Table 6-4 are slightly different with the weights in Table 6-3. Therefore, the new data for each sub-factor is still a successful fit in exponential

regression. In addition, the goodness-of-fit can be evaluated by R-squared. R-squared is the statistical measure which shows how successful the fit is to a set of data. R-squared can take on any value between 0 and 1. Values closer to 1 indicate a greater proportion of variance is accounted for by the model (web.maths.unsw.edu.au, 2015). As an example, this value is obtained through the regression analysis for the separation sub-factor in Fig. 6-3. The R-squared value of 0.9999 for separation sub-factor means that the fit explains 99.99% of the total variation in the data about the average. This is resulted from the fact that the weights for each sub-factor in columns 'b', 'c' and 'd' are already calculated using an exponential function.

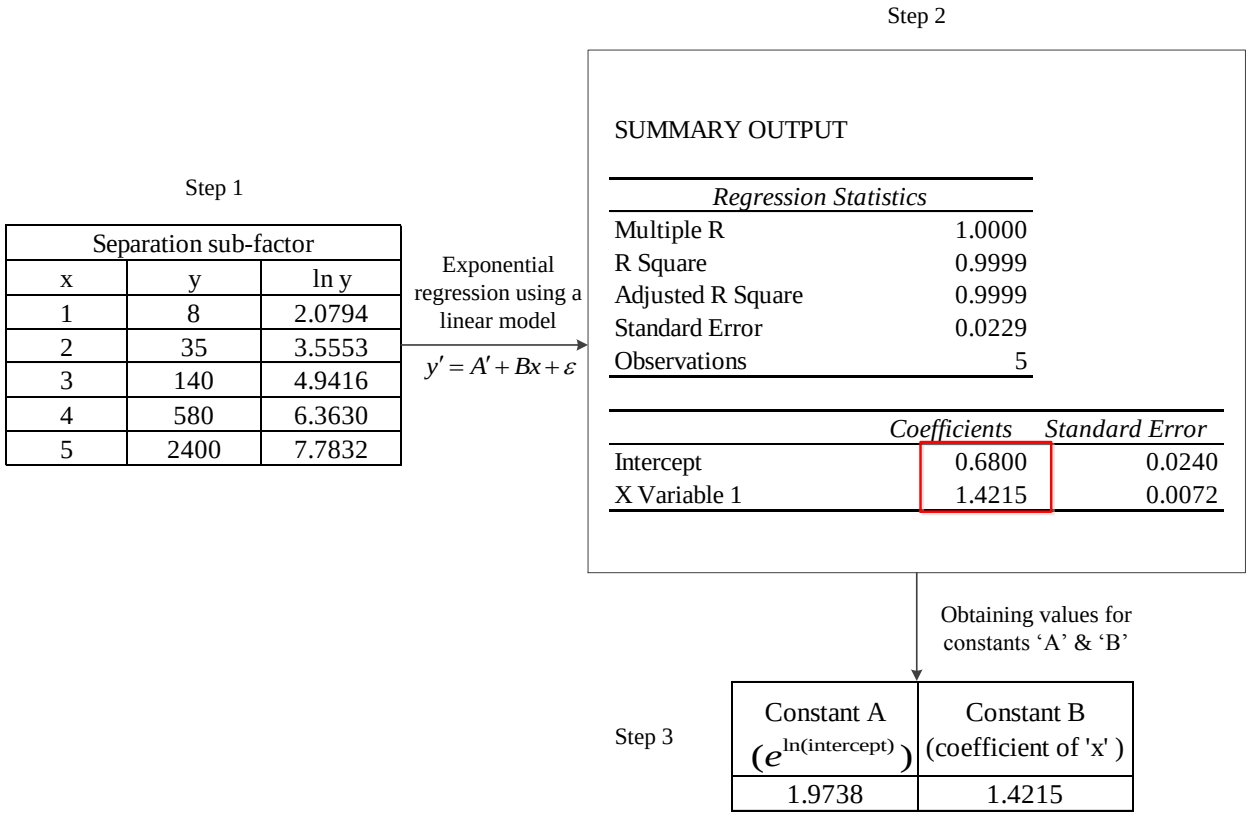

Fig. 6-3: Exponential regression using a linear model to obtain constants 'A' & 'B' in 'Y=Ae^{BX}' for separation sub-factor

The trends for all sub-factors are shown in Fig. 6-4. Values for B are almost constant in all of the curves while the values for A in each curve vary from 0.9137 to 2.3608. It can be seen in Fig. 6-4 that all of the curves are similar in their general forms.

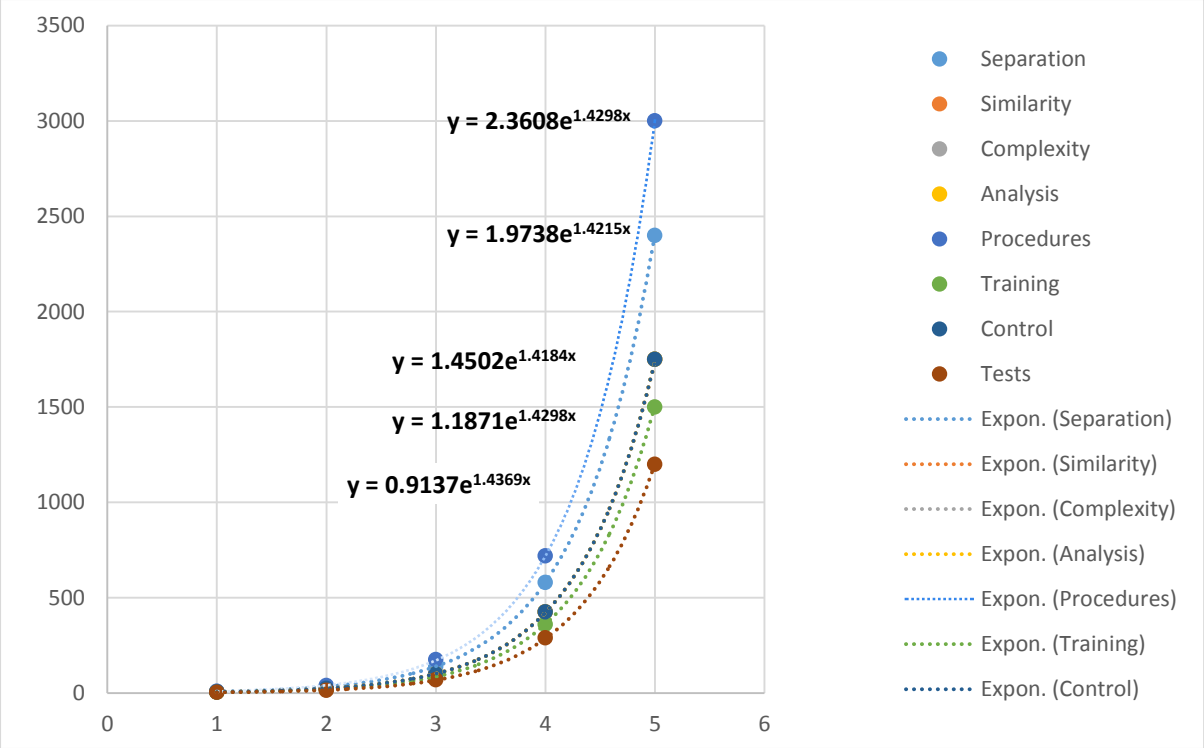

Fig. 6-4: Fitted trends for sub-factors with corresponding functions in Humphreys' method

The curves for 'similarity', 'complexity', 'analysis' and control have similar 'a' to 'e' values and therefore overlap in Fig. 6-4.

6.3 Generating new table to determine β_{safe}

6.3.1 Basis for using Humphreys' method to determine βsafe

In (Bourne et al., 1981), the common mode failures are classified by cause of failures. In other words, if recommendations are to be made for a common mode failure prevention policy, it is essential that all failure causes can be identified. According toISO 14224 (2006), failure causes (root causes) are:

- design-related causes
- fabrication/installation related causes
- operation/maintenance related causes
- management related causes
- miscellaneous

Bourne et al. (1981) introduce almost similar categories to classify common mode failures based on the common mode failure causes. Design, operation and environment related causes are assumed to be the root causes that initiate a failure in (Humphreys, 1987). Humphreys has used the CCF concept in Bourne et al. (1981) to develop Table 6-4. Weights for each sub-factor are obtained base on the failure cause (root cause) in Humphreys (1987). Eight defensive measures are then weighed in terms of the degree of reduction in causes related to design, procedure and environment. For

example, if the 'separation' sub-factor influences the design related causes significantly, the weight 'e' (best case) is selected for it. On the other hand, the weight 'a' is chosen in case of slight effect on the failure cause.

The data which is used for developing a table to determine β_{safe} is taken from failure mechanism versus failure mode table for fire and gas detectors in OREDA (2009). According to SINTEF (2015), the observed β-values are different from installation to installation. For example, an installation registers all DU failures of fire dampers as CCF. It means that a high rate of CCF events can be observed for this certain equipment group while this value is lower on another installation since they use different criteria for CCF evaluation. Therefore, it is necessary to adjust the average estimates of β. To fulfill this task, the equipment specific CCF checklists have been developed by SINTEF (2015). As a result, the data for fire and gas detectors (equipment group) are used to determine β_{safe} in this thesis.

The proposed method in this thesis, is based on the common failure mechanism concept in Cooper et al. (1993). Cooper et al. (1993) state that failure mechanisms are documented in maintenance record databases, but there is a lack of sufficient information about failure description. As a result, the root causes can be interpreted differently by different people. Therefore, they have used failure mechanisms to establish a closer relationship with root causes of component failures. In other words, they have focused on common cause failure mechanisms instead of root cause analysis according to Lundteigen and Rausand (2007). Cooper et al. (1993) argue that it is difficult to determine root causes due to insufficient information about failure description. Therefore, it is more efficient to introduce defenses against common failure mechanisms rather than CCFs.

In developing a method to determine β_{safe}, the failure mechanisms which lead to spurious activation of the equipment are identified using OREDA (2009) and ISO 14224 (2006). Using failure mechanisms in the proposed method in this thesis does not mean that failure causes (root causes) are the same as failure mechanisms. ISO 14224 (2006) points out that failure mechanism describes the apparent observed cause of failure, while failure cause describes the underlying or 'root' cause of failure. Therefore, failure mechanism should not be confused with failure cause.

A common failure mechanism defense approach is presented in this thesis using the common failure mechanism concept by Cooper et al. (1993) as well as Humphreys' method (1987). Instead of scoring the sub-factors against the root causes (design, operation and environment), each sub-factor can be weighed against the failure mechanisms which correlate to the root causes. For example, vibration, looseness and instrument failure are the failure mechanisms which can be influenced by separation sub-factor, and they are related to design.

6.3.2 Development of the proposed method to determine β_{safe}

A flowchart is suggested to provide the steps for generating the corresponding weights

against each sub-factor. Fig. 6-5 shows steps for producing a corresponding Humphreys' table (Table 6-4) (Microsoft Excel, 2010)

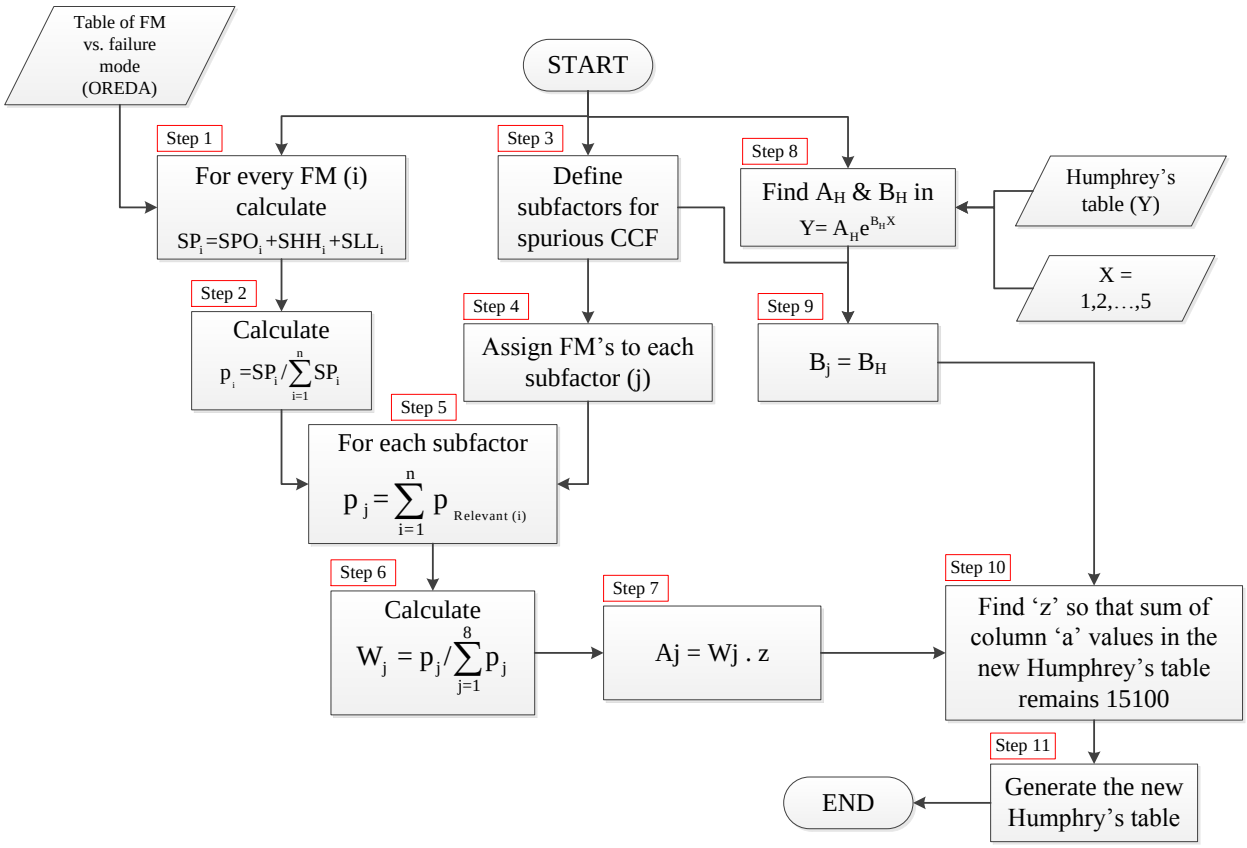

Fig. 6-5: Flowchart for generation of new Humphreys' table for determining βsafe

The following is a description of the steps for generating the new Humphrey's table in order to determine β_{safe}:

Step 1)

The percentage of total spurious failure for each failure mechanism is calculated by adding up percentages of SO, SHH and SLL failure

$$SP_i = SPO_i + SHH_i + SLL_i \quad (6.4)$$

where *'i'* represents each failure mechanism.

Three failure modes are introduced for spurious failure of fire and gas detectors in OREDA (2009) and ISO 14224 (2006) which include:

- SO: Spurious operation e.g. false alarm
- SHH: Spurious high level alarm e.g. 60% of lower explosion limit (LEL)
- SLL: Spurious low level alarm e.g. 20% of lower explosion limit (LEL)

Step 2)

Each obtained value in Step 1) is divided by sum of all the obtained values in the same step as shown in Table 6-5.

$$p_i = SP_i / \sum_{i=1}^{n} SP_i \quad (6.5)$$

Formula (6.5) calculates the percentage of total number of spurious failures per failure mechanism.

Total number of spurious failures including SPO, SHH and SLL are 30 in OREDA (2009). For example, for contamination failure mechanism in Table 6-5, '17' means that 17% of the 30 spurious failures are related to contamination.

Table 6-5: Distribution of spurious failure modes per failure mechanism in percent

Failure mechanisms (FM)	Failure modes			Sum of spurious	Percentage per FM
	SO	SHH	SLL	$SP_i = SPO_i + SHH_i + SLL_i$	$p_i = SP_i / \sum_{i=1}^{n} SP_i$
Contamination	0.97	0.32	0.32	1.61	17
External influence - general	0.97		0.32	1.29	13
Instrument failure - general	0.32	1.3	0.65	2.27	23
Looseness	0.32			0.32	3
Misc. External influence	0.32			0.32	3
Misc. general	0.32			0.32	3
Out of adjustment	0.97	1.3	0.65	2.92	30
Vibration	0.65			0.65	7
Sum of each column	4.84	2.92	1.94	9.7	100

The distribution of each failure mechanism which lead to different spurious failure modes including SPO, SLL and SHH is shown in Fig. 6-6.

Steps 3)

In order to define defensive measures (sub-factor), which influence spurious CCF, the first measure is to identify failure mechanisms. That is to say failure mechanisms, which lead to spurious failures, should be recognized. Based on failure data in OREDA (2009) and Table B.2-Failure mechanism in ISO 14224 (2006), the failure mechanisms which lead to spurious failure of fire and gas detectors are shown in Table 6-6. Next, the defensive measures which may influence those failure mechanisms are defined. In the proposed approach in this thesis, all eight defensive measures in Humphreys (1987) are

considered relevant to reduce spurious CCFs based on the identified failure mechanisms in Table 6-6.

Table 6-6: Failure mechanisms lead to spurious failure of fire and gas detectors

Failure mechanism	Subdivision of failure mechanism	Description of failure	Spurious Failure Modes		
			SO	SHH	SLL
External influence	Contamination	Gas detector head contaminated	✓	✓	✓
	General	Failure caused by some external events or substances outside the boundary (but no further details are known)	✓		✓
	Misc. external influence	Foreign objects, environmental influence from neighboring systems (false demand)	✓		
Instrument failure	General	Failure related to instrumentation but no details known	✓	✓	✓
	Out of adjustment	Calibration error, parameter drift	✓	✓	✓
Mechanical failure	Looseness	Disconnection, loose items	✓		
	Vibration	Abnormal vibration	✓		
Miscellaneous	General	Failure mechanism that does not fall into one of the categories above (real but not intended demand)	✓		

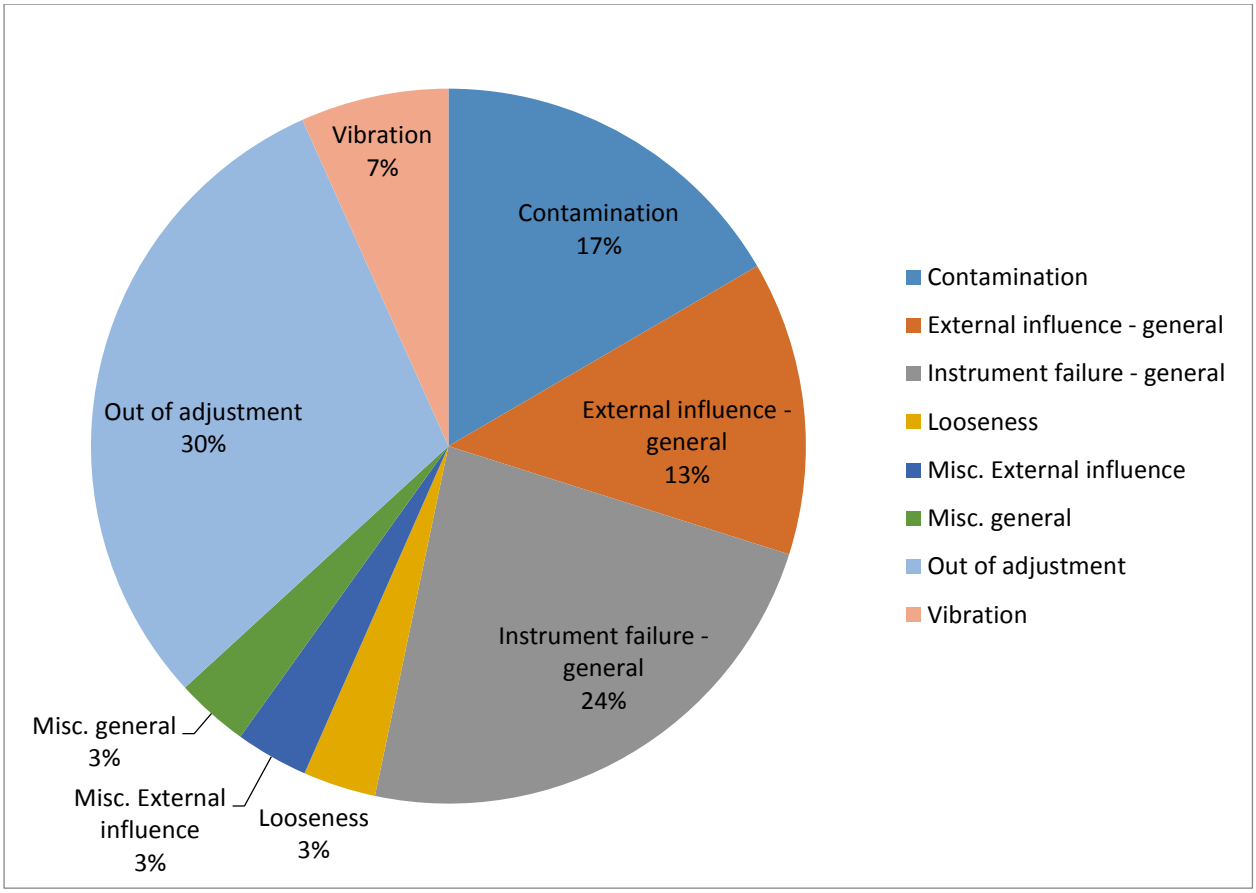

Fig. 6-6: Distribution of different failure mechanisms which lead to spurious failure for fire and gas detectors

Step 4)

During this step, failure mechanisms leading to spurious failures are identified and selected for each defensive measure (sub-factor). This is shown in Table 6-7.

Step 5)

For each sub-factor in Table 6-8, the relevant p_i's from step 2 are summed up to give the total influence of failure mechanisms:

$$p_j = \sum_{i=1}^{n} p_{\text{Relevant (i)}} \qquad (6.6)$$

Here, subscript 'Relevant' means that only the percentages of failures mechanisms which are influenced by each sub-factor (j) are added together.

Step 6)

The weight for each sub-factor is obtained by

$$W_j = p_j / \sum_{j=1}^{8} p_j \quad (6.7)$$

Where each obtained value in Step 5) is divided by the sum of all the values in the same step as shown in Table 6-8.

Table 6-7: Rationales for assigning failure mechanisms to each sub-factor

Factors	sub-factors	Failure mechanisms influenced by each sub-factor	Rationales
Design	Separation	1) Vibration 2) Looseness 3) Instrument failure - General	1) Vibration due to devices' interconnection 2) more likely due to increased No. of components inside a device or an enclosure. 3) adverse effect of one component on the other one. Exp. The heat generated by a component adjacent to heat detectors leads to spurious
	Similarity	1) Instrument failure -general 2) Misc. general (false demands)	1) Diversity reduces the potential for dependent failure by minimizing common mode failure. 2) similarity in design without correct specification. Using flame detectors in an area mostly exposed to
	Analysis	1) Instrument failure -general 2) Misc. general (false demands)	Safety analysis in the design phase prevents: 1) maufacturing error such as defective material, poor quality etc. 2) Helps with identification of false demans
	Complexity	1) Out of adjustment	As the complexity of the SIF increases, the potential for systematic errors increases due to the combination of failures. Exp. Software bug leads to out of adjustment.
Operation	Procedures	1) External influence - general (real but not intended demand) 2) Contamination 3) Out of adjustment	1) Not specified in the procedure. Exp. It is not mentioned that welding activates flame detectors. 2) Contamination of sensors due to lack of correct procedure 3) Miscalibration of sensors due to wrong procedures or high number of operator's actions.
	Training	1) Looseness 2) Contamination 3) Out of adjustment	1) Untrained personnel applies wrong torque while tightening bolts 2) Lack of competence leads to poisoning of the sensors. 3) Misclalibration of sensors due to lack of competence
Environment	Control	1) External influence - general (real but not intended demand) 2) Contamination 3) Out of adjustment	1) Poor isolation and control of environment allows for abnormal operation and unnecessary demands. 2 & 3) Environmental control restricts the access of the personnel, thereby less human interaction
	Test	1) Vibration 2) contamination	Environmental test reveal: 1) shock, vibration, radiation etc. 2) dust, insects, etc.

Step 7)

A_j represents constant 'A' for each sub-factor. This is constant 'A' in formula (6.1) which influences the form of the exponential function since the constant 'B' values proved to be almost the same in Table 6-4. In other words, constant 'A' is the deciding element that gives the weight values for each sub-factor. In order to get the weights for each sub-factor, it is required to define a factor 'z'. Multiplication of factor 'z' by the weight W_j for each sub-factor, gives the corresponding value for constant 'A'.

$$A_j = W_j.z \tag{6.8}$$

Step 8)

A_H and B_H which are the constants 'A' and 'B' for each sub-factor in Humphreys Humphreys (1987), are already found in Table 6-4.

Step 9)

Since the values for constant 'B' are similar in Table 6-4, the sub-factor weights 'a' to 'e' are not sensitive to constant 'B'. Therefore, constant 'B' for each sub-factor (j) is considered equal to its counterpart in Table 6-4, hence $B_j=B_H$. However, constant 'A' should be calculated separately for each sub-factor (j) as shown in step 7)

Step 10)

Factor 'z' is now calculated using Solver tool in Microsoft Excel by setting an objective that sum of column 'a' in Table 6-8 is 15100 (same as the target value for column 'a' in Table 6-4). The procedure steps in Microsoft Excel is shown in Appendix B.

It should be noted that factor 'z' is a variable which is used for optimization purpose in Table 6-8.

Step 11)

Constant 'A' is calculated for each sub-factor using the values obtained from steps 6) and 10), as shown in Table 6-9.

Table 6-8: Classification of failure mechanisms per each sub-factor

Factor	Design				Operation		Environment	
Sub-factor	Separation	Similarity	Analysis	Complexity	Procedures	Training	Control	Test
j	1	2	3	4	5	6	7	8
Failure mechanism	Vibration	Instrument failure - general	Instrument failure -general	Out of adjustment	External influence - general (real but not intended demand)	Looseness	External influence - general (real but not intended demand)	Vibration
	Looseness	Misc. general (false demands)	Misc. general (false demands)		Contamination	Contamination	Contamination	Contamination
	Instrument failure -general				Out of adjustment	Out of adjustment	Out of adjustment	
$p_j = \sum_{i=1}^{n} p_{\text{Relevant (i)}}$	**33**	**26**	**26**	**30**	**61**	**50**	**61**	**24**
$W_j = p_j / \sum_{j=1}^{8} p_j$	**0.11**	**0.08**	**0.08**	**0.1**	**0.2**	**0.16**	**0.2**	**0.08**

Table 6-9: Generated Humphreys' table to determine β_{safe}

							Factor z	12.0693
Factor	Sub-factor	Weight					$Y=Ae^{BX}$	
		a (x=5)	b (x=4)	c (x=3)	d (x=2)	e (x=1)	$A_j=W_j.z$ (Constant A)	Constant B
Design	Separation	**1621**	**391**	**94**	**23**	**6**	**1.3276**	**1.4215**
	Similarity	**1161**	**281**	**68**	**16**	**4**	**0.9655**	**1.4184**
	Complexity	**1161**	**281**	**68**	**16**	**4**	**0.9655**	**1.4184**
	Analysis	**1451**	**351**	**85**	**21**	**5**	**1.2069**	**1.4184**
Operation	Procedures	**3072**	**735**	**176**	**42**	**10**	**2.4139**	**1.4298**
	Training	**2458**	**588**	**141**	**34**	**8**	**1.9311**	**1.4298**
Environment	Control	**2902**	**703**	**170**	**41**	**10**	**2.4139**	**1.4184**
	Tests	**1273**	**303**	**72**	**17**	**4**	**0.9655**	**1.4369**
Sum of columns 'a' to 'e'		**15100**	**3634**	**874**	**210**	**51**		

The trends for all sub-factors are shown in Fig. 6-4.

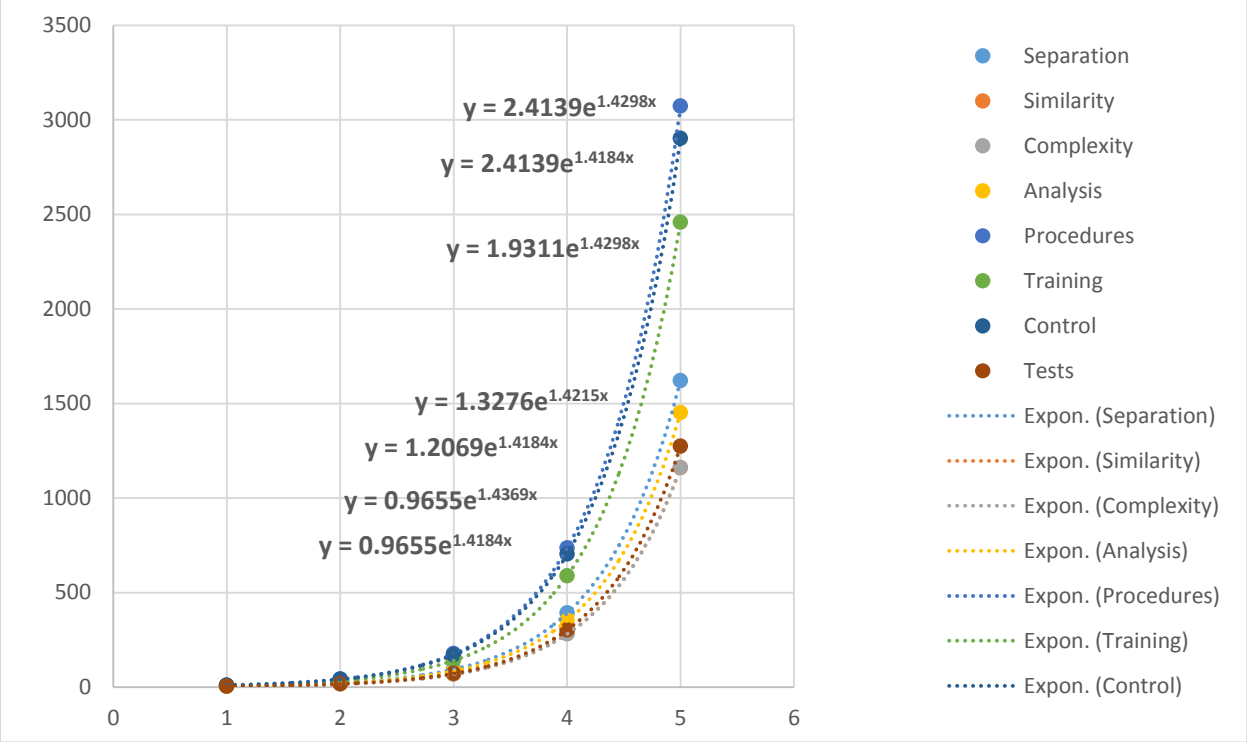

Fig. 6-7: Fitted trends for sub-factors with corresponding functions for generated Humphreys' table

It is also tempting to calibrate Table 6-9 for the beta-factor range for sensors or final elements in IEC 61508 (2010), which is between 0.01 and 0.1. This range is chosen since flame detector is an input element. In this case, column 'a' should correspond to 0.1 while column 'e' should correspond to 0.01. Therefore, the large difference between column 'a' and 'b' in Table 6-9 will not be achieved. In other words, it is not possible to fit an exponential function due to the defined range in IEC 61508 (2010).

Other functions were tried out in order to calibrate the table. Formula (6.9) seemed to be a good fit. The results are shown in Table 6-10.

Table 6-10: Calibrated Table 6-9 for sensor/final element beta-factor in IEC 61508

							Factor z	50.0157
Factor	Sub-factor	Weight					$Y=Ax^B$	
		5	4	3	2	1	$A_j=W_j.z$ (Constant A)	Constant B
Design	Separation	**54**	**39**	**26**	**15**	**6**	**6**	**1.4215**
	Similarity	**39**	**29**	**19**	**11**	**4**	**4**	**1.4184**
	Complexity	**39**	**29**	**19**	**11**	**4**	**4**	**1.4184**
	Analysis	**49**	**36**	**24**	**13**	**5**	**5**	**1.4184**
Operation	Procedures	**100**	**73**	**48**	**27**	**10**	**10**	**1.4298**
	Training	**80**	**58**	**38**	**22**	**8**	**8**	**1.4298**
Environment	Control	**98**	**71**	**48**	**27**	**10**	**10**	**1.4184**
	Tests	**40**	**29**	**19**	**11**	**4**	**4**	**1.4369**
Sum of weights in each column		**500**	**364**	**242**	**136**	**51**		

As previously discussed, constant 'A' has the major influence on the form of the exponential function and constant 'B' values proved to be almost the same in Table 6-4. However, the function fitted here is the power function. Therefore, it is not possible to judge how the weights can contribute to the values of constants 'A' and 'B' in formula (6.9), since these constants have different types of influence on the curve compared to the exponential function.

$$Y=Ax^B \tag{6.9}$$

Here, it is assumed that this is constant 'A' influences the weight of each sub-factor for the most part, and the values for constant 'B' are kept the same. Table 6-10, how the weights shows how the weights look like after applying the new formula with constants A and B.

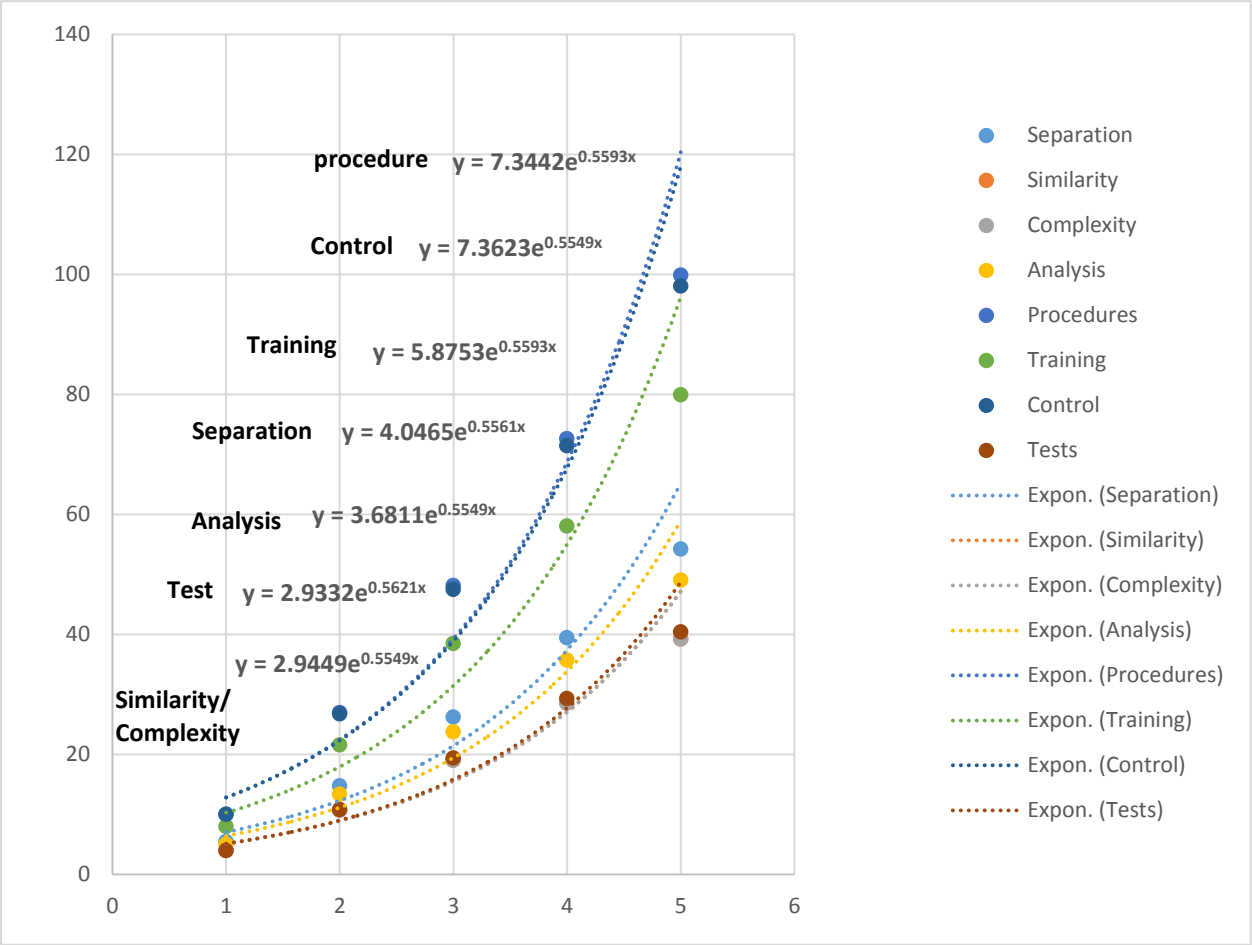

Fig. 6-8: Fitted trends for sub-factors using values in columns 'a' and 'e' in Table 6-10

Values in Table 6-10 need to be re-calibrated in order to have the values based on exponential function. The 'Trend line' tool in Microsoft Excel is used to find out the corresponding functions for each sub-factor, as shown in Fig. 6-8.

Table 6-11: Re-calibrated Table 6-10 based on $Y=Ae^{BX}$

Factor	Sub-factor	Weight					$Y=Ae^{BX}$	
		a (x=5)	b (x=4)	c (x=3)	d (x=2)	e (x=1)	Constant A	Constant B
Design	Separation	65	37	21	12	7	4.0465	0.5561
	Similarity	47	27	16	9	5	2.9449	0.5549
	Complexity	47	27	16	9	5	2.9449	0.5549
	Analysis	59	34	19	11	6	3.6811	0.5549
Operation	Procedures	120	69	39	22	13	7.3442	0.5593
	Training	96	55	31	18	10	5.8753	0.5593
Environment	Control	118	68	39	22	13	7.3623	0.5549
	Tests	49	28	16	9	5	2.9332	0.5621
Sum of columns 'a' to 'e'		602	345	198	113	65		

Finding constant 'A' and 'B' leads to finding weights for each sub-factor in columns 'a' to 'e', as shown in Table 6-11. The devisor changes from 50000 to 6000 in order to achieve the beta-factor range for sensors/final elements in IEC 61508.

6.4 Case study

The objective of this case study is to evaluate defensive measures to obtain 'equipment specific' β_{safe}. STR is calculated using the formulas introduced in Section **Error! Reference source not found.** and therefore the formulas themselves are the focus of that section.

The references for FMEDA reports are confidential. Therefore, it was not possible to access such a database. As a result, the FMEDA report for flame detectors from exida (2012b) was decided to be used through discussion with the supervisor of the thesis. Unfortunately, data is not available for all flame detector parts in Table 6-12. So it is further examined to see how the available information can be used. Hence, a β would be suggested based on the proposed approach in Section 6.3.2.

Table 6-12: Failure rates according to IEC 61508 (per 10^{-9})(exida, 2012b)

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
X2200 UV Relay	208	78	501	72	91.6%
X2200 UV Current	0	75	704	61	92.7%
X2200 UV mA w/HART	0	67	877	73	92.8%
X5200 UV/IR Relay	248	102	591	85	91.7%
X5200 UV/IR Current	0	98	834	74	92.6%
X5200 UV/IR mA w/HART	0	90	1007	86	92.7%
X9800 IR Relay	220	95	412	79	90.2%
X9800 IR Current	0	93	628	68	91.4%
X9800 IR mA w/HART	0	84	800	80	91.7%

In FMEDA report for flame detectors (exida, 2012b), three types are introduced including:

- X2200 flame detector
- X5200 flame detector
- X9800 flame detector

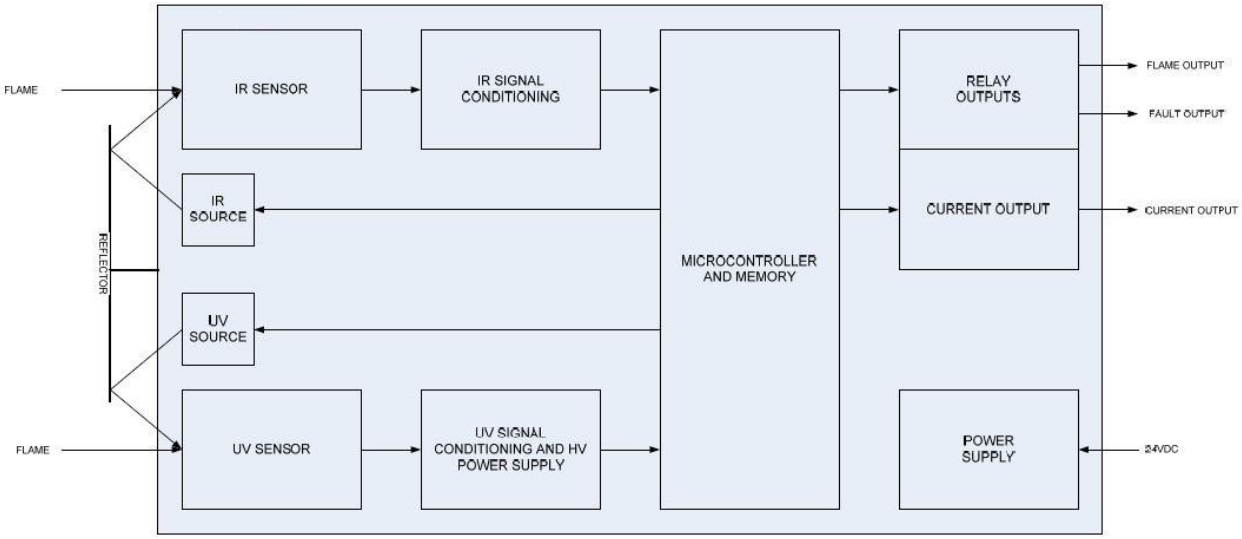

Fig. 6-9: X5200 flame detector parts (exida, 2012b)

The failure rate data for the above-mentioned flame detectors are given in Table 6-12. X5200 flame detector is taken as the case study here. X5200 flame detector is less susceptible to spurious failures since it includes both infrared (IR) sensor and ultraviolet (UV) sensor. X5200 flame detector parts are shown in Fig. 6-9.

Table 6-13: Failure rates according to IEC 61509 (per 10-9)

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
X5200 UV/IR relay	248	102	591	85
X5200 UV/IR Current		98	834	74
X5200 UV/IR mA w/HART		90	1007	86
X5200 flame detector	248	290	2432	245

However, the failure rate data in exida (2012b) is just available for the following parts:

- Relay output
- Current output (0-20 mA analog output)
- HART communication (Highway Addressable Remote Transducer) which is not shown in Fig. 6-9.

HART allows the operator to monitor the status of the detector, determine factory settings, adjust field settings and initiate field tests (det-tronics 2011).

According to IEC 61508 (2010), in some configurations early detection of failures may prevent an actual spurious trip of the system. Therefore, $\lambda_{SO} = \lambda_{SU}$ and λ_{SO} (SO-failure rate) does not include λ_{SD} (safe detected failure rate) for 2oo4 configuration.

Due to lack of data, it is difficult to investigate which defensive measures should be more deeply highlighted in the sensitivity analysis. For example no failure rate is available for infrared and ultraviolet sensors of the flame detector. Flame detectors are susceptible to SO-failure due to 'false demand' or 'real but not intended demand' failure mechanisms. Therefore, these failure mechanisms give weights to the corresponding defensive measures, as shown in Table 6-8. This cannot be evaluated in case of considering each component of the flame detector separately. As a result, the whole detector unit is considered here instead of different components of the detector. It is assumed here that the values in the last row of Table 6-13 show the failure rates of the flame detector (whole unit).

Flame detectors are categorized under fire detectors in NORSOK S-001 (2008). The proposed method is based on the fire and gas detectors data in OREDA (2009), and therefore a flame detector is aptly considered in this case study.

A 2oo4 configuration of flame detectors is studied here. A redundant configuration is chosen since CCFs influence several flame detectors. Besides, Table 5-1, shows that in a MooN voting, when M≥2, β is the most influential parameter in spurious trip rate calculation.

6.4.1 Evaluation of defensive measures to obtain βsafe for the Case study

The definition of each defensive measure (sub-factor) including the weights a, b,…, e is given in Appendix B. Each defensive measure is further evaluated to obtain the corresponding weight for X5200 flame detector. Therefore the value of β_{safe} will be achieved in the end using Table 6-9. In addition, β_{safe} is also calculated based on recalibrated Table 6-11 for IEC 61508. It is assumed that the detectors with 2oo4 configuration are installed in offshore oil and gas installation. Therefore, in this context the design and operation are framed.

The defensive measures are evaluated for flame detector X5200 based on the above mentioned assumptions and Appendix B.

Separation (d):

The flame detector as a whole unit has dual sensors and these sensors are assumed to be on different circuit boards though in the same enclosure. It is assumed that circuits of the sensors are in the same enclosure with barriers. Therefore, 'd' is selected.

Similarity (e):

This defensive measure may be argued in two different ways:

First, X5200 flame detector takes advantage of dual built-in sensors (det-tronics 2011; exida, 2012b). That is to say there is low similarity inside the detector. Separation is a defensive measure which applies to design related causes as previously discussed in Section 6.3.1. Therefore, the detector should be looked into, not the configuration. For example, the manufacturer does not have any idea about the configuration of the flame detectors which are going to be installed in a platform, and focuses on the element itself.

The manufacturer may just provide the failure rate. However, if it is intended to suggest the beta-factor, they should consider the inherent properties of the component. Through the analysis of the internal parts, the beta-factor can be judged. Therefore, it is decided to select weight '**e**' here.

The second argument is that two detectors of the same design (same manufacturer) have some diversity inside which may compensate for some of the negative effect of having the identical flame detectors in the configuration. Therefore, despite the fact that we have four identical detectors, we have some degree of diversity embedded. However, it does not seem like a correct argument here since the designer considers only the unit itself as a whole and does not bother about the configuration.

Complexity (d):

Although R signal conditioning, UV signal conditioning, microcontroller and memory for sensors and HART communication give a degree of complexity to flame detector X5200, it consists of electrical devices with simple safety function according to exida (2012b). HART communication lets the operator monitor the condition of the detector and it is not safety related (exida, 2012b). Since PIU (Proven-In-Use) assessment has been carried out for this flame detector, it may be considered as a well-understood design. The assessment shows that the detector has a proven history of successful operation according to exida (2012b). However, it is decided here not to give the best case scenario, since this flame detector has dual sensor and hence two signal conditioning component beside microcontroller and memory for sensor. In other words, some degree of complexity is accounted for, i.e. weight '**d**' is allocated.

Analysis (e):

FMEDA (Failure Mode Effect and Diagnostic Analysis) is an extension of FMEA (Failure Mode & Effect Analysis) and is meant to identify online diagnostic techniques and failure modes relevant to safety-instrumented design (exida, 2012b). The FMEDA of X5200 flame detector has been carried out and verified using Fault injection testing according to (exida, 2012b).

For these flame detectors proven-in use assessment has been carried out. This assessment has the following benefits:

- Systematic failures will be prevented (due to pre-existing devices with a proven history of successful operation)
- It is not required to carry out a number of functional safety lifecycle assessment

Therefore, it is not required to carry out a number of functional safety lifecycle assessment according to exida (2012b). However the manufacturer, det-tronics (2011), has created FSM (Functional Safety Management) plan, SRS (Safety Requirements Specification) and validation test plan according to exida (2012b). Since extra safety analysis has been carried out beside the minimum requirements, weight **'e'** is chosen for this sub-factor.

Procedures (c):

Based on Appendix A, the accuracy of the procedures and how well they are written and reviewed is not the sole important factor here. In addition, the number and complexity of operator actions should also be taken into account. In other words, it is likely to reduce human errors and thereby CCFs. However, it is not able to fully remove the possibility of errors. For example, the probability of having an out of adjustment status is partly reduced by good procedures. Nevertheless, the operator involvement should be taken into consideration.

It is assumed here that due to X5200 design, the operator interaction is minimal and the procedure is well written but not detailed. Therefore 'c' is selected

Det-Tronics, the manufacturer of X5200 flame detectors, has created a safety manual det-tronics (2011)

Training (c):

As previously mentioned, it is assumed that the flame detector (SIS) is going to be installed in an offshore facility. Based on IEC 61508 (2010), there is a requirement stating that maintenance of the equipment needs sufficient competence. It is also mentioned in Clause 5.2.1 of (NOG-070, 2004) that the competence is required for all activities that influence the safety life cycle of the SIS.

It is assumed here that the involved operators need some general introductory course for X5200 flame detectors to be trained in application of IEC 61508 Standard on the Norwegian continental shelf. In an international company, the corresponding course would be CFSP (Certified Functional Safety Professional) i.e. functional safety on an execution level.

Environmental control (c):

This defensive measure cannot be applied to flame detectors to a great extent. For example, transmitters can be put inside a housing to both limit the personnel access and reduce the influence of environmental stressors. However, this is not applicable to flame detectors and they cannot be isolated, since their intended function is to detect flame. In other words, they are normally exposed to the surrounding environment. Therefore '**b**' is reasonable here.

Environmental test (d):

EMC test report has been reviewed as part of the IEC 61508 functional safety assessment in exida (2012b). EMC test (electromagnetic compatibility (EMC)) which includes testing of electronic equipment is an environmental test. It is to ensure that flame detectors perform their intended function in electromagnetic environment. Therefore comprehensive environmental tests are carried out according to the definition of weight '**d**' in Appendix A.

6.4.2 Calculation of βsafe for the Case study

As previously mentioned, in order to calculate $\beta_{safe,}$ all allocated weights for eight sub-factors are added together and divided by the 'divisor'. The devisor for calibrated table according to Humphreys' beta-factor range is 50000. The divisor is changed to 6000 for calibrated table according to IEC 61508 to achieve the beta-factor range for sensors/final elements. The values of allocated weights in Table 6-14 are taken from Table 6-9 and Table 6-11.

Table 6-14: Calculation of β_{safe} for case study (example 1)

Sub-factor		Weigh value Humphreys $0.001 \leq \beta \leq 0.3$	Weigh value IEC 61508 $0.01 \leq \beta \leq 0.1$
Divisor		50 000	6000
Separation	d	12	12
Similarity	e	5	5
Complexity	d	9	9
Analysis	e	6	6
Procedures	c	39	69
Training	c	31	55
Environmental control	c	39	68
Environmental test	d	9	9
Sum		552	150
βsafe		0.01	0.03

The obtained value for β_{safe} is 1% based on Humphreys beta-factor range and 3% based on IEC 61508 beta-factor range. It should not be interpreted that β_{safe} obtained by the proposed approach in this thesis, is always higher for IEC 61508 beta-factor range compared to Humphreys'. For example, changing weights of some sub-factors leads to β_{safe}=4% for both Humphreys and IEC 61508 beta-factor ranges, as shown in Table 6-15.

Table 6-15: Calculation of βsafe for case study (example 2)

Sub-factor		Weigh value Humphreys 0.001≤β ≤0.3	Weigh value IEC 61508 0.01≤β ≤0.1
Divisor		50 000	6000
Separation	d	23	12
Similarity	e	4	5
Complexity	d	16	9
Analysis	e	5	6
Procedures	c	735	69
Training	c	588	55
Environmental control	c	703	68
Environmental test	d	17	9
Sum		2091	233
βsafe		0.04	0.04

In other words, the difference in obtained values for IEC 61508 and Humphreys is due to the different beta-factor ranges introduced by IEC 61508 (2010) part 6 – Annex D and Humphreys (1987).

6.4.3 Calculation of STR for the Case study based on existing formulas

Using data in Table 6-11 and β_{safe} in Table 6-14, STR is calculated for a 2oo4 configuration of X5200 flame detectors. Formulas by different approaches in Table 6-16 are used for calculation of STR. Also, $\beta_{Danegrous}$ value is adapted from SINTEF (2013a).

Table 6-16: Spurious trip formulas used by different approaches for 2oo4 configuration Lundteigen and Rausand (2008)

Configuration	Approach		
	New	PDS	ISA
2004	$\beta^{SO}\lambda_{SO} + \beta^{DD}\lambda_{DD}$	$4\beta^{D}\lambda_{SO}$	$\beta^{D}(\lambda_{SO} + \lambda_{DD})$

The only formula that gives different values for STR in Table 6-17 is the one in the 'New' column. It is due to β_{safe} which is only defined in this approach.

Table 6-17: Spurious trip rates for case study

β_{safe}	Configuration	Approach		
		New	PDS	ISA
Humphreys	2004	1.73E-7	8.12E-8	1.91E-7
IEC 61508	2004	1.79E-7	8.12E-8	1.91E-7

The slight difference in STR's obtained by the new approach shows that both Table 6-9 and Table 6-11 are suitable for obtaining β_{safe} value, based on what β-factor range is chosen.

Chapter 7

7 Conclusions and recommendations for further work

7.1 Conclusion

A literature survey on STR showed that the most contributing factor to high frequency of spurious activations of SIS, is the beta-factor parameter. However, the approaches in ISA and PDS for STR calculation do not even consider β_{safe}. They give more conservative values compared to the new approach proposed by Lundteigen and Rausand (2008).

When STR is calculated, an average frequency of spurious activation is considered over a long period of time. In other words, for a SIS with a certain configuration, STR is equal to a constant value (e.g., for a 2oo3 voting). However, after an SO-failure occurs at a point on the time axis the STR will experience a stepwise reduction due to a decrease in number of remaining components.

The spurious activation of an element on other engaged equipment should be taken into account, and decision making about the operation strategy should be made accordingly. For example, water boiler is meant to produce steam for auxiliary machinery on a vessel. In other words, spurious activation of a 'too low level transmitter' adversely affects other equipment, since it leads to boiler shutdown. In this case, a new SIF may be introduced to stop other engaged equipment in order to prevent hazardous events. Therefore, spurious activation of the too low level transmitter will lead to activation of the newly-introduced SIF. Therefore, activation of the new SIF shall be taken into account while the spurious trip rate for the too low level transmitter is being calculated. However, this issue is not considered in available formulas for STR calculation.

STL is per safety function, just like SIL is per safety function. It is nevertheless not possible to look at a safety function in isolation. One should always look at it in the full context of the plant. In other words, PFD does not consider what happens afterwards to other functions, neither does PFS. This has of course consequences. A single system might trip and multiple systems might trip afterwards; the complete Xmas tree might trip or the complete upstream or downstream might trip. So it depends on the function that tripped originally and its consequences on the EUC. For example, one may say that a safety instrumented function needs SIL 1 from a safety point of view. But when the same function trips, it inflicts a huge damage that may need STL 5 at the same time.

The observed β-values are different from installation to installation SINTEF (2015). It means that a high rate of CCF events can be observed for this certain equipment group while this value is lower on another installation since they evaluate CCFs differently.

Therefore, it is necessary to adjust the average estimates of β. The equipment specific CCF checklists have been developed by SINTEF (2015) to obtain this objective. Based on this suggested approach, the data for fire and gas detectors (equipment group) are used to create factor-weight table and determine β_{safe} accordingly in this thesis.

The proposed method in this thesis, is based on the common failure mechanism concept in Cooper et al. (1993).

In Humphreys' method, defensive measures are weighed based on root causes including design, operation and environment related causes. Through the literature study, the link between the root causes and failure mechanisms was identified. Therefore, the defensive measures were weighed against failure mechanisms since it is difficult to determine root causes due to insufficient information about failure description according to Cooper et al. (1993). Besides, OREDA (2009) provides data for failure mechanisms but not root causes.

Through an in-depth investigation of Humphreys' method, the root causes which lead to spurious failures were examined and their relationship to different failure mechanisms were identified. Therefore, more insight was achieved into the causes of spurious failures, and it was found out that it is possible to weigh defensive measures not only based on the root causes, which are design, operational and environmental related causes, but also based on failure mechanisms.

Having identified the root causes and the relevant failure mechanisms for flame detectors, defensive measures against these failure mechanisms were introduced. The weights of each defensive measure against the relevant failure mechanisms were calculated to determine β_{safe}. However, it should be noted that the generated table is 'equipment specific'. For example, it is not possible to obtain β_{safe} values using the same proposed factor-weight table (Table 6-9), for other field devices such as temperature transmitters or pressure transmitters. This is due the fact that the defensive measures introduced for the flame detectors are based on the failure mechanisms which cause flame detector to have spurious failure.

The proposed method in this thesis can be used in two ways:

- A desired beta-factor value is intended. Therefore the defensive measure are selected in a way obtain the certain β_{safe}.
- The designer knows the value of each defensive measure and the value of β_{safe} is calculated accordingly.

7.2 Recommendations for further work

The balance between the concepts of safe and dangerous has been a matter of controversy. Therefore, decision making after detection of a failure is not an easy task since it should be

decided what is best with respect to spurious trip and what is best with respect to safety at the same time. In other words, the trade-off between STR and PFD can be an area of further research.

As discussed in conclusion part, one may do further research to find the best trade-off between STL and SIL. For example, one may say that a safety instrumented function needs SIL 1 from a safety point of view. But when the same SIF trips, it may inflict a huge damage that may need STL 5 at the same time.

ISO/TR 12489 (2013) technical report considers a safe state as a state when safety is achieved as described in IEC 61508 (2010); IEC 61511 (2003). However, it mentions that the probability of a hazardous event with respect to a certain safety function may increase with respect to safe state of another safety function. Therefore, the maximum allowable STR for the former function should consider the potential increased risk associated with the latter function. This issue was also discussed in Section 4.1. It was mentioned that spurious activation of an element may lead to stress on other equipment. This can be an area of further research since the current formulas do not consider the effect of STR on associated equipment.

In the proposed approach, two different tables were generated for Humphreys' beta-factor range and IEC 61508 beta-factor range. An important area for further research may be to determine a beta-factor range for safe failures since it is not discussed in the literature or any Standard.

Appendix

A. Translation of Humphreys' sub-factor weights to determine β_{safe}

In this appendix different defensive measures introduced by Humphrey, are translated to defensive measures for SIS in order to clarify the meaning of each weight in columns 'a' to 'e'.

1) Separation: the degree to which redundant units can be affected by a single environmental event depends on physical separation.

a) Circuits on the same circuit board
b) Circuits on different boards
c) Circuits in the same enclosure without barriers
d) Circuits in the same enclosure with barriers
e) Circuits in different enclosures

2) Similarity: The vulnerability of redundant items to a common mode failure depends on the degree of similarity.

a) Identical units
b) Similar units with only small difference in circuit
c) Similar units with different circuits
d) Units with different function but identical components
e) Diverse units with different components and different functions

3) Complexity: complex or not well-understood designs are associated with more risk and therefore more susceptible to CCFs. Inclusion of software adds to complexity as well.

a) Limited knowledge and experience of the design. Not designed specifically for the application or redundant units include software.
b) Not designed specifically for the application. More than 10 equipment years' experience in similar environments by users
c) Equipment specifically designed for application but limited experience
d) Equipment specifically designed for application. Design is well understood and documented.
e) Equipment specifically designed for application. 10 equipment years' experience in similar environments by users

4) Analysis: FMEA or the fault analysis provides an important and independent check on design with respect to detection of failures and the adequacy of testing.

a) No safety analysis
b) Limited analysis - high level FMEA

c) Detailed fault analysis of the most important circuits linked with FMEA.
d) Detailed fault analysis of all circuits in an equipment of novel or difficult design.
e) Detailed fault analysis of a well understood equipment which employs straightforward traditional design techniques.

5) Procedures: the degree to which the procedures cause human errors can lead to CCFs. Although proper, well-written procedures greatly reduce human error, the number and complexity of operator actions are important factors which should not be overlooked.

Therefore, two judgments are considered evaluating 'procedures' sub-factor, i.e. both written procedure and operator involvement should be evaluated together.

a) No written procedures- Normal operator interaction.
b) No written procedures - Minimal operator interaction or, written procedures - Normal operator interaction
c) Written procedures - Minimal operator interaction, or detailed procedures and Normal operator interaction
d) Detailed procedures - Minimal operator interaction
e) Detailed procedures - Minimal operator interaction and more than 10 operating equipment years' experience.

6) Training: Training directly influences the probability of human error and therefore CCFs. The training must also include the training of experienced operators in emergency procedures.

a) On the job training
b) Systematic regular training
c) SIL GL course part 1 (CFSP course)
d) SIL GL course part 2 (CFSE course)
e) Both courses in c) and d) should be attended. Besides, the personnel are involved more than 50% of their time with the particular system and the system is in use for more than 10 years.

Considering Norwegian continental shelf, SIL GL part 1 is a general introductory course with while SIL GL Part 2 is a specialization course for application of IEC 61508 standard (Norsk forening for automatisering, 2013, 2014).

If functional safety is a major role of professionals in the organization, CFSE course is required. Professionals are responsible for leading, coordinating, and reviewing the activities of the safety lifecycle, including the more complex activities such as SIL Selection and SIL verification. If functional safety is professionals' secondary role or they are expected to support safety lifecycle projects on an execution level, the CFSP is required

(exidacfse, 2015).

7) Control: The degree, to which the environment, in which the system is installed, is controlled, for example, limited access of the personnel to the equipment. This sub-factor does not relate to the severity of the environment.

a) Units accessible to the personnel and exposed to environmental stressors
b) limited access to the personnel but exposed to environmental stressors such as heat in the compartment by adjacent machinery
c) Accessed by authorized personnel only and small risk of mechanical damage by other operating devices in the vicinity (exp. Flame detectors vulnerability to being damaged while working with overhead crane in a compartment) but exposed to environmental stressors
d) Accessed by authorized personnel only and no risk of mechanical damage by other operating devices in the vicinity. Fairly controlled environmental stressors
e) Trained personnel only or access under supervision is provided. Environmental stressors controlled to great extent

8) Environmental Test: The severity of the environment is taken into account by the designer which is necessary but not sufficient. Environmental testing reveals certain common cause susceptibilities. These tests may include conventional tests like shock, vibration, humidity, etc. tests or more comprehensive ones such as radiation test.

a) No environmental tests other than those conducted by component manufacturers
b) Limited environmental tests on prototype units
c) Environmental tests including shock, vibration, temperature and humidity
d) Comprehensive environmental tests on the operating units, considering as many as environmental effects such as steam, gas, radiation and electromagnetic waves
e) Same as d) for the equipment subject to burn-in of at least one year

B. Steps involved in using the solver inbox within MS Excel

Solver is a Microsoft Excel add-in program which can be used for what-if analysis. Solver can be used for optimization purpose. It is meant to find a Max., Min. or a set value for a formula in one cell which is subject to constraints, or limits, on the values of other formula cells on a worksheet. Solver works with a group of cells, called variable cells that are used in computing the formulas in the objective and constraint cells. Solver adjusts the values in the variable cells. Therefore two following items are satisfied:

- The limits on constraint cells
- The intended result in the objective cell.

In this section the step by step procedure for using Solver is explained. In our problem of finding weights for each sub-factor, as illustrated in Figure 1-A, Factor z determines how relatively big the values of Constant A are ($A_j = W_j . z$). For every row Figure 1-A, this will affect the values for respective weights. Our objective is to make the sum of all the weights in column 5 to be equal to 15100. Here is how to define and solve this problem in MS Excel 2010. In order to find the Solver toolbox, click **Solver** on the **Data** tab, in the **Analysis** group. If the **Solver** command or the **Analysis** group is not available, you need to load the Solver Add-in program. The following steps are shown on Figure 1 with the same numbers:

1. In the **Set Objective** box, enter a cell reference or name for the objective cell. The objective cell must contain a formula (in this case the sum of all the weights in column 5).
2. Since you want the objective cell to be a certain value (in this case 15100), click **Value of**, and then type 15100 in the box.
3. In the **By Changing Variable Cells** box, enter a reference for each decision variable cell range (in this case Factor z). The variable cells must be related directly or indirectly to the objective cell. In our problem, Factor z affects the values for Constant A on every row which in turn influence the values of the weights on Column 5. The value of our objective cell is the sum of the weights on Column 5.
4. In the **Subject to the Constraints** box, enter any constraints that you want to apply. Our problem does not involve any constraints. Therefore, this box can be left empty.
5. Since our problem is linear, choose **Simplex LP** in the **Select a Solving Method** box. Simplex algorithm is a popular algorithm for linear programming.
6. Click **Solve** and do one of the following:

a. To keep the solution values on the worksheet, in the **Solver Results** dialog box, click **Keep Solver Solution**.

b. To restore the original values before you clicked **Solve**, click **Restore Original Values**.

A)

Factor	Sub-factor	Weight 5	4	3	2	1	$A_j=W_j.z$ (Constant A)	Constant B
							Factor z	12.0693
							3 $Y=Ae^{BX}$	
Design	Separation	1621	391	94	23	6	1.3276	1.4215
	Similarity	1161	281	68	16	4	0.9655	1.4184
	Complexity	1161	281	68	16	4	0.9655	1.4184
	Analysis	1451	351	85	21	5	1.2069	1.4184
Operation	Procedures	3072	735	176	42	10	2.4139	1.4298
	Training	2458	588	141	34	8	1.9311	1.4298
Environment	Control	2902	703	170	41	10	2.4139	1.4184
	Tests	1273	303	72	17	4	0.9655	1.4369
Sum of columns 'a' to 'e'		1 15100	3634	874	210	51		

B)

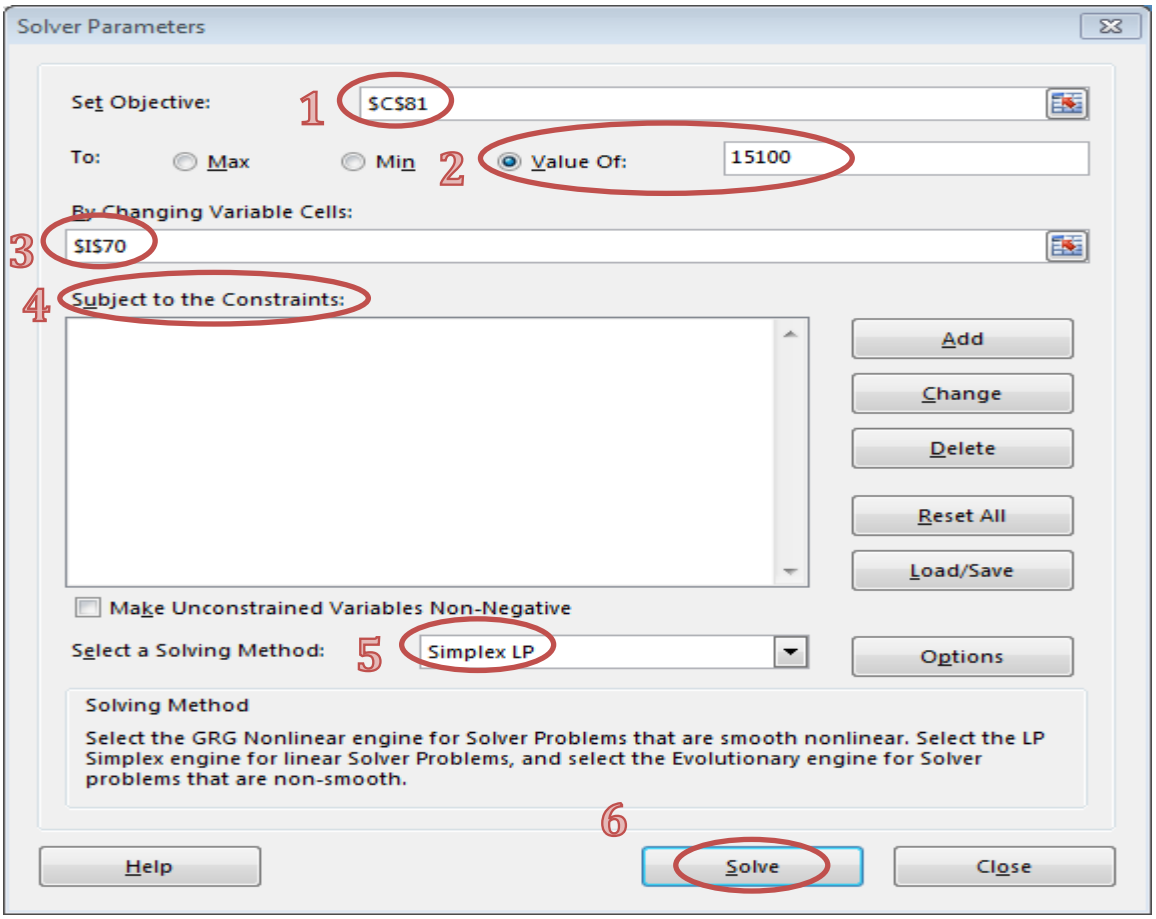

Fig. 0-1: Steps for using the solver toolbox within MS Excel. A) table of values for our problem, B) Solver interface

References

ANSI/ISA-84.00.01, (2004). Functional Safety: Safety Instrumented Systems for the Process Industry Sector: Framework, definitions, system, hardware and software requirements Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

Bourne, A.J., G.T., E., D.M., H., D.R., P., I.A., W., (1981). Defences against common-mode failures in redundancy systems - A guide for management, designers and operators. United Kingdom Atomic Energy authority, Safety and Reliability Directorate, Warrington.

Castanier, B., Rausand, M., (2006). Maintenance optimization for subsea oil pipelines. International Journal of Pressure Vessels and Piping 83, 236-243.

Center for Chemical Process, S., (2010). Understanding Failure, Guidelines for Safe and Reliable Instrumented Protective Systems. John Wiley & Sons, Inc., pp. 311-342.

Cooper, S.E., Lofgren, E.V., Samanta, P.K., Wong, S.-M., (1993). Dependent failure analysis of NPP data bases. Nuclear Engineering and Design 142, 137-153.

Dang, T., Schwarz, M., Börcsök, J., (2015). Effect of demand rate on evaluation of spurious trip rate of a SIS. International Journal of Mathematical Models and Methods in Applied Sciences 9, 487-498.

det-tronics (2011). X2200 UV, X9800 IR, X5200 UVIR SIL 2 Certified Flame Detectors Safety Manual. det-tronics.com, Minneapolis, MN.

exida (2012a). Failure Modes, Effects and Diagnostic Analysis - Project: 644 Temperature Transmitter. exida.com, Sellersville, PA.

exida (2012b). IEC 61508 Functional Safety Assessment, Project: X2200/5200/9800 flame detectors. exida.com, Sellersville, PA.

exidacfse (2015). Functional safety certification program. exidacfse.com, Sellersville, PA.

Gentile, M., Summers, A.E., (2006). Random, systematic, and common cause failure: How do you manage them? Process Saf. Prog. 25, 331-338.

Goble, W.M., Cheddie, H., (2004). Safety Instrumented Systems Verification: Practical Probabilistic Calculations. ISA-The Instrumentation, Systems, and Automation Society.

Grattan, D., Nicholson, S., (2010). Integrating switchgear breakers and contactors into a safety instrumented function. Journal of Loss Prevention in the Process Industries 23, 784-795.

Guo, B., Song, S., Ghalambor, A., Lin, T.R., (2014). Chapter 18 - Pipeline Vibration and Condition Based Maintenance, In: Lin, B.G.S.G.R. (Ed.), Offshore Pipelines (Second Edition). Gulf Professional Publishing, Boston, pp. 299-337.

Hokstad, P., Rausand, M., (2008). Common Cause Failure Modeling: Status and Trends, In: Misra, K. (Ed.), Handbook of Performability Engineering. Springer London, pp. 621-640.

Houtermans, D.M.J.M., (2006). Safety Availability Versus Process Availability, Introducing Spurious Trip Levels. RISKNOWLOGY B.V., Brunssum, Netherlands.

Humphreys, P., Jenkins, A.M., (1991). Dependent failures developments. Reliability Engineering & System Safety 34, 417-427.

Humphreys, R.A., (1987). Assigning a numerical value to the beta factor common cause evaluation. Proceedings: Reliability'87 2C.

IEC 61508 (2010). Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. International Electrotechnical Commission, Geneva.

IEC 61511 (2003). Functional Safety - Safety Instrumented Systems for the Process Industry. International Electrotechnical Commission, Geneva.

ISA-TR84.00.02 (2002). Safety Instrumented Systems (SIS) -Safety Integrity Level (SIL) Evaluation Techniques.

ISO 14224 (2006). Petroleum, petrochemical and natural gas industries. Collection and exchange of reliability and maintenance data for equipment. International Standards Organization, Geneva.

ISO/TR 12489 (2013). Petroleum, petrochemical and natural gas industries - Reliability modelling and calculation of safety systems. International Standards Organization, Geneva.

Jin, H., Lundteigen, M.A., Rausand, M., (2011). Reliability performance of safety instrumented systems: A common approach for both low- and high-demand mode of operation. Reliability Engineering and System Safety 96, 365-373.

Lotfifard, S., Faiz, J., Kezunovic, M., (2012). Over-current relay implementation assuring fast and secure operation in transient conditions. Electric Power Systems Research 91, 1-8.

Lundteigen, M.A., Rausand, M., (2007). Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing. Journal of Loss Prevention in the Process Industries 20, 218-229.

Lundteigen, M.A., Rausand, M., (2008). Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas. Reliability Engineering & System Safety 93, 1208-1217.

Lundteigen, M.A., Rausand, M., (2010). Reliability of safety instrumented systems: Where to direct future research? Process Safety Progress 29, 372-379.

Machleidt, K., Litz, L., (2011). An optimization approach for safety instrumented system design, Reliability and Maintainability Symposium (RAMS), 2011 Proceedings - Annual, pp. 1-6.

Microsoft Excel, (2010). Define and solve a problem by using Solver.

Moubray, J., (1997). Reliability Centred Maintenance. Industrial Press, New York, NY.

NOG-070 (2004). Application of IEC 61508 and IEC61511 in the Norwegian Petroleum Industry. The Norwegian Oil and Gas Association, Stavanger, Norway.

Norsk forening for automatisering, (2013). SIL-GL Del 1, kurs, IEC 61508 - Retningslinjer for bruk av sikkerhetsstandarden (Guidelines for use of safety standard). nfaplassen.no, Stavanger.

Norsk forening for automatisering, (2014). SIL-GL Del 2 kurs, IEC 61508 - Retningslinjer for bruk av sikkerhetsstandarden (Guidelines for use of safety standard). nfaplassen.no, Stavanger.

NORSOK S-001 (2008). Technical safety, 4th ed. Standards Norway, Lysaker, Norway.

NUREG-75/014 (1975). Reactor safety: An assessment of accident risk in U.S. commercial nuclear power plants. Nuclear Regulatory Commission, Washington, D,.

OREDA (2009). OREDA : offshore reliability data handbook, 5th ed. Available from: Det Norske Veritas, NO 1322 Høvik, Norway: OREDA Participants, Trondheim.

Panikkar, S.B., (2014). Preventing Spurious Trips in the Chemical Process Plant: The role of Functional safety Management, The TÜV Rheinland Functional Safety Symposium, Köln, Germany.

Rahimi, M., Rausand, M., Lundteigen, M., (2011). Management of factors that influence common-cause failures of safety-instrumented systems in the operational phase. Advances in Safety, Reliability, and Risk Management, ESREL 2011, 2036-2044.

Rausand, M., (2014). Reliability of Safety-Critical Systems. John Wiley & Sons, Inc.

Rausand, M., Høyland, A., (2004). System reliability theory: models, statistical methods, and applications. John Wiley & Sons.

SINTEF (2013a). Reliability data for safety instrumented systems, PDS data handbook. SINTEF Safety Research, Trondheim, Norway.

SINTEF (2013b). Reliability prediction methods for safety instrumented systems, PDS method handbook. SINTEF Safety Research, Trondheim, Norway.

SINTEF (2015). Common Cause Failure in Safety Instrumented Systems. SINTEF Safety Research, Trondheim, Norway.

web.maths.unsw.edu.au, (2015). Goodness-of-Fit Statistics. http://web.maths.unsw.edu.au/~adelle/Garvan/Assays/GoodnessOfFit.html, Garvan Institute.