Master's degree thesis

LOG950 Logistics

Safety System Design and Maintenance Planning for Oil and Gas Facilities Located in Remote Areas

Kristanna Tunga Anderson

Number of pages including this page: 111

Molde, 22.05.2018

Mandatory statement

Each student is responsible for complying with rules and regulations that relate to examinations and to academic work in general. The purpose of the mandatory statement is to make students aware of their responsibility and the consequences of cheating. Failure to complete the statement does not excuse students from their responsibility.

*Please complete the mandatory statement by placing a mark **in each box** for statements 1-6 below.*		
1.	**I/we hereby declare that my/our paper/assignment is my/our own work, and that I/we have not used other sources or received other help than mentioned in the paper/assignment.**	☒
2.	**I/we hereby declare that this paper** 1. Has not been used in any other exam at another department/university/university college 2. Is not referring to the work of others without acknowledgement 3. Is not referring to my/our previous work without acknowledgement 4. Has acknowledged all sources of literature in the text and in the list of references 5. Is not a copy, duplicate or transcript of other work	Mark each box: 1. ☒ 2. ☒ 3. ☒ 4. ☒ 5. ☒
3.	**I am/we are aware that any breach of the above will be considered as cheating, and may result in annulment of the examination and exclusion from all universities and university colleges in Norway for up to one year, according to the Act relating to Norwegian Universities and University Colleges, section 4-7 and 4-8 and Examination regulations** section 14 and 15.	☒
4.	**I am/we are aware that all papers/assignments may be checked for plagiarism by a software assisted plagiarism check**	☒
5.	**I am/we are aware that Molde University College will handle all cases of suspected cheating according to prevailing guidelines.**	☒
6.	**I/we are aware of the University College's rules and regulation for using sources**	☒

Publication agreement

ECTS credits: 30

Supervisor: Yury Redutskiy

Agreement on electronic publication of master thesis

Author(s) have copyright to the thesis, including the exclusive right to publish the document (The Copyright Act §2).

All theses fulfilling the requirements will be registered and published in Brage HiM, with the approval of the author(s).

Theses with a confidentiality agreement will not be published.

I/we hereby give Molde University College the right to, free of charge, make the thesis available for electronic publication: ☒**yes** □**no**

Is there an agreement of confidentiality? □**yes** ☒**no**

(A supplementary confidentiality agreement must be filled in)

- If yes: **Can the thesis be online published when the period of confidentiality is expired?** □**yes** □**no**

Date: 22.05.2018

Acknowledgements

This master thesis is my final academic work as a student in order to achieve the double degree of the Master of Science in Petroleum Logistics at Molde University College – Specialized University in Logistics and Russian State University of Oil and Gas. The research work has been carried out from December 2017 to May 22, 2018.

PhD Yury Redutskiy has supervised this master thesis. I would like to thank to him for his great guidance, constant support, availability and constructive suggestions throughout my master thesis research study. It was an honor for me to share of his excellent scientific knowledge and of his extraordinary human qualities.

Kristanna Tunga Anderson

Molde, Norway

May 2018

“***Logistics is an application –oriented scientific discipline. It models and analysis economic systems as networks and flows of objects through time and space (specifically goods, information, moneys, and people) which create value for people.”* -** (Delfmann, et al. 2010)

Abstract

Currently, oil and gas companies face dramatic challenges such as volatile prices, booming global demand, and reduced resources within existing fields, which combined with a substantial reduction of ice in the Arctic, is leading the exploration and production of oil into less developed parts of the world. In addition to these challenges the oil companies need to take into consideration that the complex equipment that is used for drilling rigs, oil platforms, especially in the Arctic is under a constant threat operating in harsh conditions offshore which can easily lead to environmental disasters. Therefore, it requires that the exploration and production (E&P) activities must be continued in an economically efficient and safe manner. Safety Instrumented Systems (SIS) are widely used in process facilities for controlling the process and mitigating the possible risks. An optimal design and operation of the SIS is essential for an effective performance that intended to reduce risk of hazards to acceptable levels. The objective of this research has been to address the problem of SIS design and maintenance modelling to optimize the set of safety measures inherent in the SIS and simultaneously to determine the staffing size and their working schedules as well as the maintenance policy for SIS performance. The multi-objective optimization of the SIS design and maintenance planning considered both safety and economic indicators in order to explore the trade-off between the cost of using safety measures and the obtained safety level for SIS performance. The modelling in this research is to ensure the safety of operations by simultaneously evaluating the decisions on the safety system`s components and structures, the facility maintenance frequencies, the staffing size of maintenance personnel and transportation of staff, as well as the schedules of their work shift. A Markov model applied for safety quantification, i.e. addressing the device failures and repairs, technological incidents and restorations, and the periodic maintenance policy, while a black-box optimization algorithm was used in the decision-making process. From the perspective of an engineering project, the results of this SIS design and maintenance planning, optimization should be valued at the stage of defining the requirements specification, helping to formulate rather clear functional safety requirements that can be further used as a starting point for the detailed engineering design of SIS.

Contents

List of Figures

List of Tables

List of Abbreviations

ALARP	As Low As Reasonably Practicable
BP	British Petroleum
CBM	Condition-based Maintenance
CCF	Common Cause Failure
DC	Diagnostic Coverage
DD	Dangerous Detected
DU	Dangerous Undetected
E & P	Exploration and Production
ESD	Emergency Shutdown System
EUC	Equipment Under Control
F & G	Fire and Gas detection system
FC	Final Control element
FT	Fault Tolerance
FTA	Fault Tree Analysis
GA	Genetic Algorithm
HSE	Health and Safety Executive
IEC	International Electro technical Commission
ISA	The Instrumentation, Systems and Automation Society
IT	Information technology
KooN	K-out-of-N
LCC	Lifecycle cost
MA	Markov Analysis
MATLAB/Matlab	MATrix LABoratory (programming language)
MooN	M-out-of-N redundant arrangement
MRT	Mean Repair Time
O&G	Oil and Gas
PFD	Probability of Failure on Demand
PDFavg	Average Probability of Failure on Demand
PLC	Programmable Logic Controller
RAMS	Reliability, Availability Maintainability and Safety
RBD	Reliability Block Diagram
RCM	Reliability Centered Maintenance
RRF	Risk Reduction Factor
SDLC	Systems Development Life Cycle
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SINTEF	The Foundation for Scientific and Industrial Research (in Norwegian)
SD	Safe Detected
SIS	Safety Instrumented System
STR	Spurious Trip Rate
SU	Safe Undetected
TBM	Time-based Maintenance
TI	Test Interval

1.0 Introduction

Over the last decades, demand and consumption of oil have been steadily increasing, while the crude oil has become one of the most present and essential resources in modern society (BP 2017). Today, the oil and gas (O&G) industry has a strong influence worldwide, and it is one of the most powerful branches in the world economy. Since activities in the modern society rely on to a huge extent on the hydrocarbons, oil and gas will still play a vital role in meeting the future energy demand. In fact, global proved oil reserves rose by 15 billion barrels (0, 9 %) to 1707 billion barrels in 2015, which estimated as 50, 6 years of global production based on production level of 2016 (BP 2017). According to the U.S. Geological Survey (USGS), an estimation of 22 % of the world`s undiscovered oil resources are in the Arctic, and roughly 84 % of these resources are expected to be found offshore (Milakovic, Ehlers and Schutz 2014).

Currently, oil and gas companies face dramatic challenges such as volatile prices, booming global demand, and reduced resources within existing fields, which combined with a substantial reduction of ice in the arctic, is leading the exploration and production of oil into less developed parts of the world. In addition to these challenges the oil companies need to take into consideration that the complex equipment that is used for drilling rigs, oil platforms, especially in the Arctic is under a constant threat operating in harsh conditions offshore which can easily lead to environmental disasters. Since drilling has been taking place for hundreds of years, there have been numerous incidents, which had a serious impact on both personnel and the environment. Therefore, it requires that the exploration and production (E&P) activities must be continued in an efficient and safe manner.

For this reason, the major challenges of oil and gas companies might be how to improve the safety and increase the business value in executing the operation in remote and harsh environments in the years ahead. In practice, the technologies used to produce oil and gas and further processing are associated with substantial hazards. The whole chain of oil and gas processes from the field to the end user, is carried out on the hazardous industrial facilities where the occurrence of an incident may lead to significant economic losses, harm to personnel, environmental damage, and other negative consequences. Thus, a proper design of safety systems and maintenance planning can contribute significantly to the safety of operations on such hazardous facilities (Redutskiy 2017a).

The thesis will describe the design of safety instrumented systems (SIS), and their maintenance planning and workforce scheduling for remotely located oil and gas (O&G)

facilities. The maintenance planning is considered within the framework of an O&G industry-engineering project. The structure of the thesis is as follows. The section1.0 provides some background information and motivation for the research problem. The section 2.0 provides a brief overview of main theoretical frameworks for the research. The section 3.0 describes the research methodology used in the research. The section 4.0 presents the mathematical structure and description of the models that are constructed for the research. The section 5.0 presents the computational experiment. The section 6.0 presents the obtained results from the computational experiment. The section 7.0 provides the conclusion of this research and recommendations for future research.

1.1 Research problem

The technology of oil and gas production, processing, transportation and distribution is a complex combination of technical solutions and information technology solutions (Devold 2013). The former category includes technological units and facilities running the processes. The information technology (IT) solution consisting of various automated process control systems and safety systems, as well as servers, operators' and engineers' workstations connected into an industrial network. From the strategic planning perspective, the engineering projects for such technological solutions development include a number of decisions related to these systems design with a long-term view of facilities functioning. These decisions are related to the design of specific processes (facilities and units), choices of instrumentation and architectures for the process control systems and safety-related systems, industrial network hardware, as well as choices of software (interface) for the workstations, database management system and so on.

The focus of this research is development and operation of automated safety systems. These systems are crucial for the petroleum industry processes given the hazardous nature of the technology. The decision related to the safety systems design include the architectures and the instrumentation choices for the system's components. These constitute mostly to the capital investments into the safety systems. In addition to these decisions, the expenditures related to operating (maintaining) the safety systems will be considered in detail. This is especially relevant given that O&G industry is facing a shift towards the operations in nonconventional environments and remote locations, so that the processes in such conditions would run smoothly and would be economically efficient. One of these planning issues is obviously related to the facilities' personnel and their transportation to the remote locations and back. The examples of the remote locations may include the offshore petroleum production (and thereby offshore platforms), or oilfields in the north of Canada or gas fields in the Russian Arctic region. The facilities built in these locations are quite far from large cities or industrial centers, and therefore they are poorly attainable by the conventional road, railway or air transportation. The transportation means to such regions often involves helicopters (for Arctic locations) and supply vessels (for offshore locations). The personnel involved in deploying these facilities and operating them is transported from the cities where the engineering companies are actually located and remain at the production sites during a certain period. Thus, scheduling the trips and work shifts for personnel is a very important aspect of planning the operations.

1.2 Incidents in oil and gas industry

The petroleum industry is potentially one of the most hazardous industry sectors worldwide. Because the operations the petroleum sector is running, is involving combination of serious complex equipment, toxic, flammable, and explosive materials, and processes that are under high pressure can lead to hazardous incidents, besides dealing with numerous environmental hazards. During the past decades, the industry has had several serious incidents with a major accident. A major accident is an acute incident (e.g., a major discharge/emission or a fire/explosion etc.), which immediately or subsequently causes several serious injuries and in some cases loss of human life, serious harm to the environment as well as loss of substantial material assets (PSA 2013). Thus, investigations of major accidents show that technical, human, operational, as well as organizational factors influence the accident sequences. Despite these facts, quantitative risk analyses of oil and gas production facilities have mostly focused on technical safety systems (Vinnem, et al. 2012).

In addition, increasing energy demand is driving the exploration and production in oil and gas industry more and more to the non-conventional environments (remote locations, deep-water, harsh climate conditions). As a result, safety and prevention of hazardous incidents are becoming a big challenge for the operators. One type of unwanted hazardous events that may be named here is vapor cloud explosions. They occur due to the release of flammable gases and ignition (Dadashzadeh, et al. 2013). The unwanted release of a combustible gas or liquid may result in an explosive vapor cloud, which upon ignition forms a threat to the surrounding area (Wiekema 1984). Perhaps, accounting for the causes and the outcomes of such a hazardous event may help to design the safety measures that could prevent such an event and/or mitigate its consequences (Dadashzadeh, et al. 2013). Another kind of unwanted events in the petroleum sector is hydrocarbon leaks which have a major accident potential (Skogdalen and Vinnem 2012).

The research on several major incidents in oil and gas industry shows that the following events are defined essentially as vapor cloud explosions due to dispersion of the flammable gases. *Piper Alpha, 1988*: an explosive inferno on the UK platform claimed the lives of 167 people after a gas leak ignited (PSA 2013). Investigations revealed the release of light hydrocarbons (condensate propane, butane, and pentane) occurred due to the restart of a pump that was out of service for maintenance (CCPS 2005). *BP Texas City, 2005*: a series of explosions and fires occurred due to hydrocarbon liquid leak at BP`s Texas City oil refinery during the startup of an isomerization (ISOM) process unit that had been shut down for maintenance, which claimed 15 lives and caused much serious injuries (Kaszniak and Holmstrom 2008). *Petrobras, 2001*: a major explosion occurred on the Petrobras platform 36 claimed the lives of 11 people (USEPA 2001). Investigation revealed the accident started by the rupture of an Emergency Drain Tank (EDT) because of excessive overpressure that caused a gas leak ignition (Barusco 2002). *BP Deepwater Horizon, 2010*: an explosion and consequent fire resulted in the loss of 11 lives. Investigation showed that the explosion happened due to a well control event allowed hydrocarbons to escape from the Macondo well onto the Transocean`s Deepwater Horizon rig, resulting in a fire on the rig (BP 2010). In addition, the blowout caused oil spill out of damaged well for two months, the worst environmental disaster of all time (USDI 2010).

In O&G industry, lesson learned from such major accidents are important sources of information to prevent the occurrence of similar accidents in the future, and leading *to significant changes in technology, operations, supervision, and regulation* (Skogdalen and Vinnem 2012). As well as recognizing signals and or warnings by using proactive safety indicators will reduce the risk of such major accidents (Øien, Utne and Herrera 2011). Investigations of the hydrocarbon releases, releases often reveal that these events are originate in either failure of a certain asset itself or because of mistakes in the asset's maintenance, e.g., poor practice or insufficient operational controls. As shown in examples above, the consequences of major accidents are quite severe. One of the factors contributing to preventing major accidents is proper maintenance of production facilities (HSE 2014).

1.3 Oil and Gas facilities in remote locations

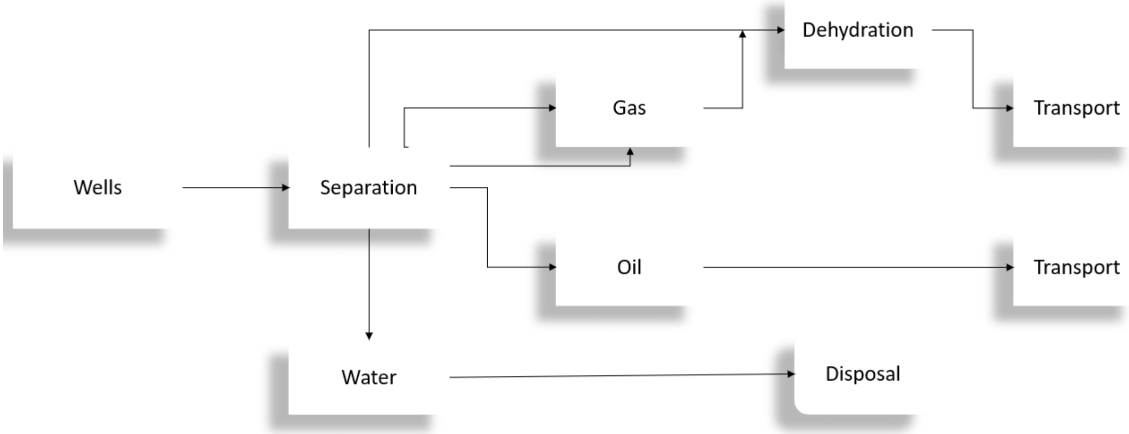


Figure 1: The main function of O&G facility Based on: [(PetroWiki n.d.)]

An oil and gas facility encompasses the equipment between the wells and the pipelines or other transportation systems, and its purpose is to produce oil and gas and to make petroleum ready for sale according to the customers' requirements, e.g. limitations to percentage of allowable water, salt, and other impurities. The main process of an oil and gas facility is to separate the oil, gas, water, and solids and deliver it to the transportation system for further processes. In general, the processing facilities in the petroleum industry are technically complex, involving the integration of knowledge from many different technical and socio-economical disciplines (Berendes 2007). The technology of hydrocarbons is associated with high risks. Today, the risk level is increasing because the industry has faced with even more challenges ahead for operating deeper, colder, more remote locations (e.g., offshore, deep sea, arctic, etc.).

Over the last decade, oil and gas companies are ventured into remote areas (i.e. places to be situated far from the main centers of population; distant) to operate their exploration and production activities due to attainable oil and gas reserves. In many instances, extracting oil in these remote areas might be challenging due to lack of infrastructure development and integration, optimization and systems management, and maintenance for optimal performance of operations. Beside this, the oil and gas companies need to handle the rapidly increasing technological complexity of the industrial production processes and complexity of establishing and maintaining facilities and units for production processes in remote and poorly accessible locations (Zolotukhin, Sungurov and Streletskaya 2015).

1.4 Safety System in oil and gas facilities

The relationship between hazards, threats, consequences as well as potential safety barriers and controls, illustrated in a diagram, in Figure 2. This diagram is called a "bow-tie diagram" and it includes two parts: the left side describes the latent hazard, initiating events, preventive controls, and initial hazard release, while the right-hand side presents the potential major incident as a starting point, barriers in sequence and the consequences that result from the failure of the barriers. Altogether, the bow-tie diagram allows identifying the safety barriers, more discussion in section 2.1.1, implemented to prevent the critical event from taking place and as well to mitigate its effects. Admittedly, the bow-tie diagram is a special case of safety barrier diagrams. Safety barrier diagrams have proven to be a useful tool in documenting the safety measures taken to prevent incidents in oil and gas industry (Duijm 2008).

Usually, several safety systems used in the oil and gas facilities to providing several layers of protection. These safety systems are designed as a series of barriers protecting the personnel, facility assets, environment, etc. Among all these safety measures, there are automated systems, which are usually referred to as Safety Instrumented Systems (SIS), and there are safety measures of another nature (emergency response policy, evacuation plans, etc.). Among SIS, special attention is paid to Emergency Shutdown (ESD) systems as they play a vital role in preventing the hazardous situations occurrence (CCPS 2010). The ESD systems monitor the processes and shut down the technology in circumstances that can quickly lead to emergency situations with drastic consequences, related to, e.g., uncontrolled flooding, escape of hydrocarbons, or outbreak of fire in hydrocarbon carrying areas. Safety of the processes in oil and gas industry is a matter of concern, as the equipment and the processes are rather complex and considered to be hazardous.

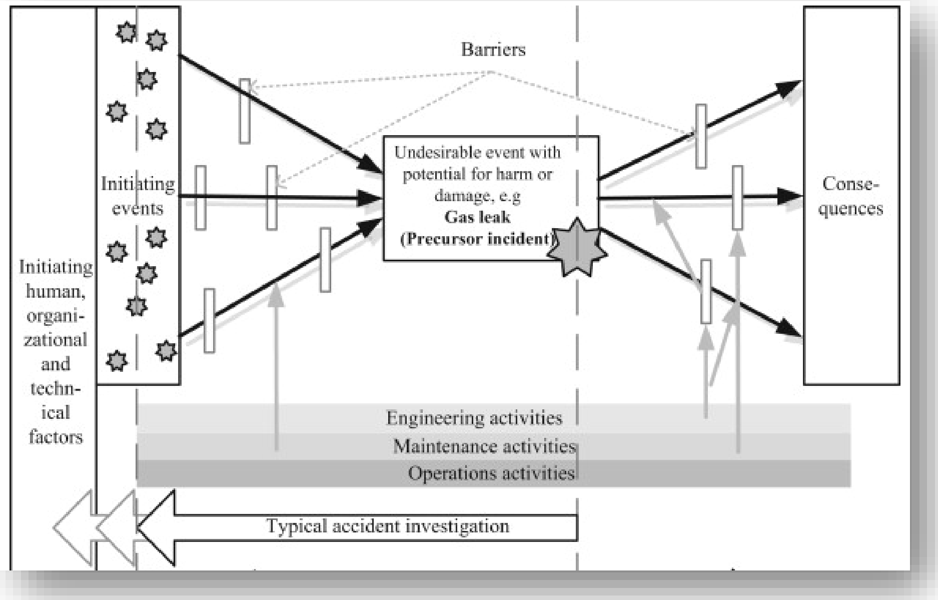

Barriers
Initiating events
Initiating human, organi- zational and techn- ical factors
Undesirable event with potential for harm or damage, e.g
Gas leak
(Precursor incident)
Conse- quences
Engineering activities
Maintenance activities
Operations activities
Typical accident investigation

Figure 2: Barriers for major accidents in O&G industry Source: [(Skogdalen and Vinnem 2012)]

The requirements to the functional safety (i.e. the overall safety of a certain system) of operations at such facilities are an important part of development of the oil and gas industrial solutions. The purpose of the safety requirements is to manage the risk of operating a hazardous system. The safety measures are developed so that the overall functional safety would correspond to a certain acceptable level by introducing a set of safety-related functions (Piesik, Sliwinski and Barnert 2016). For this reason, SISs are installed in oil and gas facilities to detect hazardous events (i.e. to prevent damage to the facility and risk for personnel), and to perform required safety actions to maintain the process return to a safe state (Lundteigen and Rausand 2008). Therefore, a proper design of SIS is imperative for safe operations. During last decades, the importance of safety systems has been increasing in the oil and gas industry (Lundteigen 2008). As can be seen, the safety plays a vital role in this industry because failures can have dramatic consequences.

1.5 Life Cycle Approach to the Systems Development in Oil and Gas Projects

In the petroleum sector, building any particular technological solution is done in the form of an engineering project comprising the choice of the necessary processes design for implementing the appropriate technology, and also, establishing an IT system to work closely with the technology to control the processes and ensure the proper course of operations. These IT solutions include (Figure 3):

- process automation tools such as sensors, programmable logic controllers (PLCs, or, in other words, industrial computers), valves, drives, switches, etc.
- common IT systems components, such as workstation computers (for operators and IT engineers and technology engineers), servers, and communication networks.

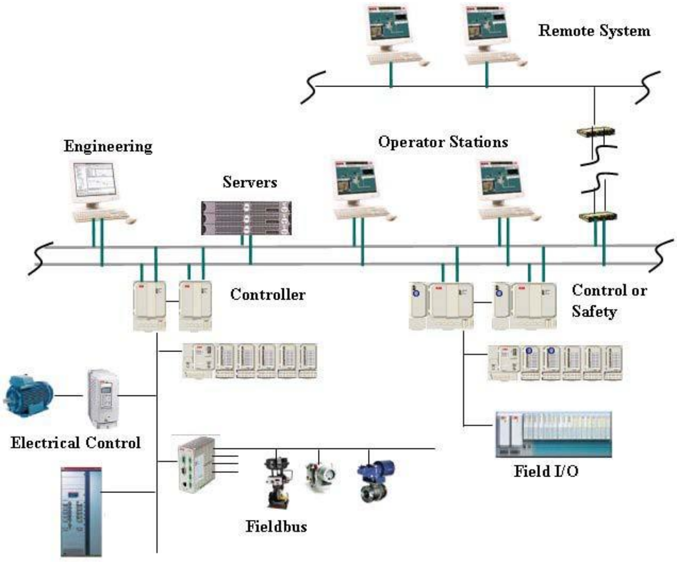


Figure 3: Process automation and IT system at an O&G facility Source: [(Devold 2013)*]*

The process automation of the engineering solution depicted in Figure 3 includes such elements as a general *process control* system (sometime also referred to as *distributed control* systems), system of *interlocks*, *emergency shutdown* system, *fire and gas* detection system, *firefighting* systems and others (Devold 2013). Development of complex and multifunctional IT solutions is usually guided by systems development life cycle approach (SDLC), which has for several decades been the underlying methodology for many approaches to establishing information systems of various nature (Avison and Fitzgerald 2003). SDLC focuses on the phases of development and implementation of computer-based systems. The starting phase is related to project *initiation* (which includes *feasibility study* and *investigation of current systems*).

The next step is development of *requirements specification* to the new system that is further *designed* according to the requirements. Upon the design completion, it is *implemented*, and finally, the longest-running phase of the system's lifecycle, namely, operations and maintenance, takes place. The specifics of the systems developed for oil and gas industry imply that the following is done during each of the mentioned life cycle phases. The project initiation is often considered to be a phase of ***conceptual design*** of a certain solution. At this very first stage, the appropriateness of a particular technology for the required purposes is always evaluated. As for the IT and process control solutions, current technical options (instrumentation alternatives for sensors, valves, controllers, switches, etc., industrial network solutions, servers and workstations hardware) as well as software options are studied and evaluated. Companies who intend to operate the facilities and systems under development initiate the conceptual design phase. These are usually large national or international companies making long-term investments, and thereby assuming a large risk. Examples of such companies are Statoil, BP, Shell, Chevron, ExxonMobil, Gazprom, Rosneft, PetroChina, Petrobras, etc. These companies are often referred to as *Exploration and Production (E&P) operators*, or simply *operating companies*.

When it comes to building new facilities, it is a common practice for the operating companies to assign the engineering workload to a *contractor*. The contractor is often chosen through a bidding process when several engineering contractor companies propose a certain design development. In the bidding process, certain pre-defined design requirements must be provided as an equal basis for all the participants, it is usually given due to budget purposes. When a contractor company is chosen, the following work on the engineering design is delegated to this company. Before the contractor begins the work, however, the operating company together with the contractor have to agree on the ***requirements specification***, an essential document containing a set of requirements to the system under development, and the contractor must fulfill these requirements.

Requirements specification is an important phase of the project's lifecycle and it is especially important for the systems developed for the petroleum sector. This specification has to cover all aspects of the information system as the one depicted in Figure 3, including the functional safety requirements. This is important due to the danger that the oil and gas facilities and processes pose and the severity of the consequences in case of unwanted events occurrence. The importance of requirements specification in reference to the safety systems development is highlighted in (HSE 2003). The British agency Health and Safety Executive conducted an analysis of a sample of incidents and their circumstances. Their study revealed that a significant share of incidents had been caused by the inadequacies in the requirement specification of the control systems responsible for the safety operations, as illustrated in Figure 4.

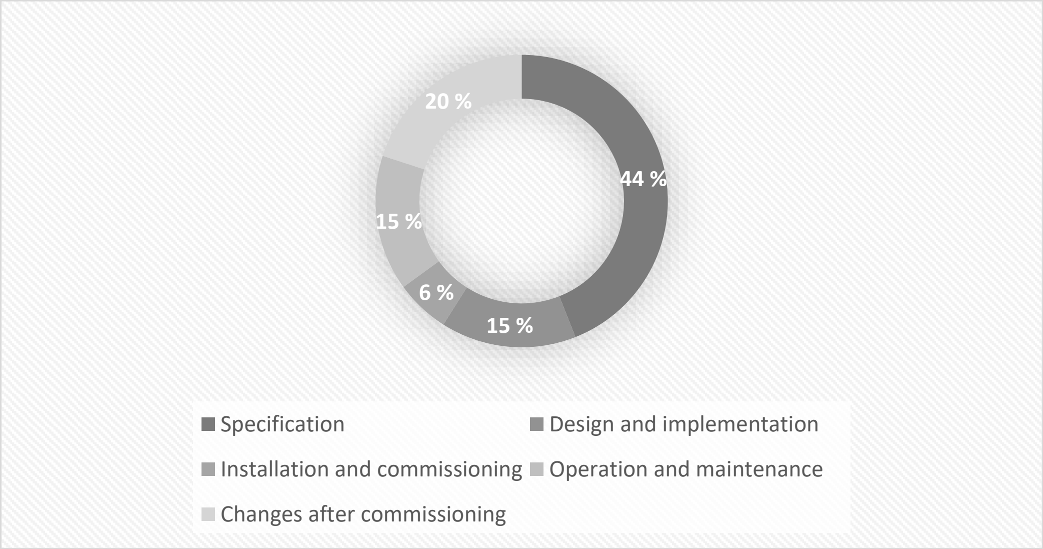


Figure 4: Primary causes of incidents grouped by the life cycle phase   Based on: [(HSE 2003)*]*

The safety requirements consist of two main categories as follows. First, one is functional safety requirements, which are the safety requirements related to the intended purpose of the facility or equipment, e.g., to ensure the facility or equipment maintain a safe state. In other words, explicit descriptive specification of safety functions needed to the incidents on the processes or failures of the instrumentation. Another one is safety integrity requirements that are related to the overall performance of the developed solution. The latter is expressed in a form of a number called the *safety integrity level* (SIL) which varies from 1 to 4, and is assigned to a particular system implementation given the likelihoods of incidents during the system's functioning and the likelihood of the safety systems failure. Any automated system (including safety systems) may fail to implement their indented functions due of to various reasons. This is why the safety measures that are inherent in any automated control system include (a) choice of instrumentation with high reliability indicators, (b) development of an architecture that prove to be fault-tolerant, and (c) avoiding mistakes in the design process (HSE 2003).

The requirement specification with respect to safety requirements are associated with regulations expressed in the international standards IEC (International Electronical Commission). The design and operation of any automated safety system must follow the requirements declared in the standards IEC 61508 (1997) and IEC 61511 (2003), which are widely adopted by the national authorities for the oil and gas industry worldwide.

The IEC 61508 is a generic standard on SIS design and construction. The IEC 61511 is a process industry safety standard that addresses the development of safety requirements for all safety instrumented systems (Hauge, Lundteigen and Rausand 2009). A careful qualitative analysis of safety measures (i.e. risk analysis) has to be conducted for particular solutions under development, so that the safety integrity level may be defined and documented in the requirements (IEC61511 2003).

Risk analysis of the processes and technology in the petroleum industry (most of which is are typical and studied) result in knowledge regarding potential hazards, their likelihoods and their consequences, as well as the necessary protection layers. (Esparza and Hochleitner 2010). This knowledge contributes to creating the requirements specification and helps ensuring the proper performance of the systems. However, the incident analysis conducted by HSE (2003) suggests that accounting for all possible critical situations and their consequences while designing a safety system, is a particularly complicated task. Given that, it is proposed that all safety systems should to be frequently reviewed through the system's operations.

Another important aspect of developing requirements specifications for safety-related systems and their functions is taking into account the viewpoints of all stakeholders involved in the projects in oil and gas industry. These stakeholders are (1) national authorities which are, first of all, in charge of the natural resources, including hydrocarbons that are extracted on the countries' territories, and also the authorities perform their regulatory function by setting the standards for the operations at the hazardous industrial facilities, (2) E&P operator companies who invest into developing the hydrocarbon deposits, building the processing, transportation and distribution facilities, and (3) engineering contractors who are developing the facilities, units and the process control and IT solutions for particular projects. Figure 5 demonstrates the phases of the systems development lifecycle and the key stakeholders (along with their responsibilities) throughout the engineering project of establishing a certain solution or a facility oil and gas industry.

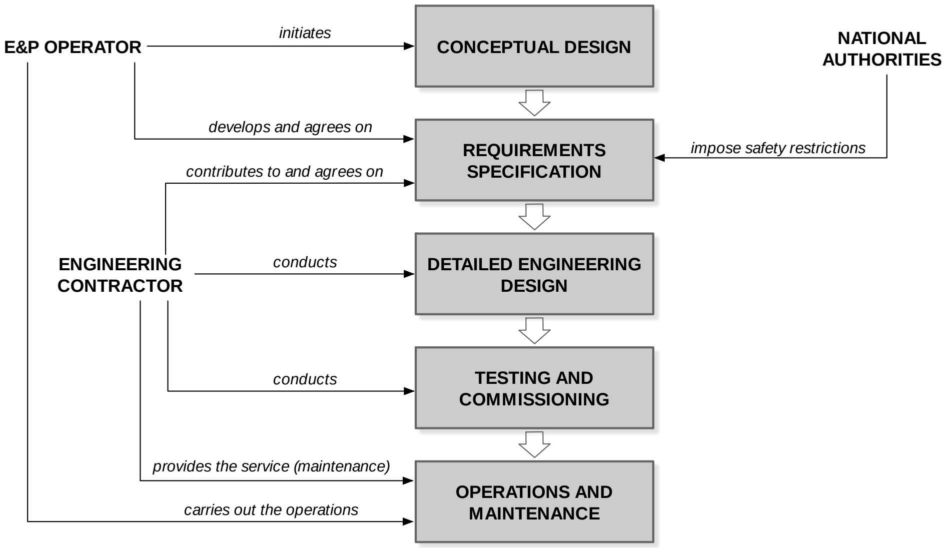

E&P OPERATOR
initiates
CONCEPTUAL DESIGN
NATIONAL AUTHORITIES
develops and agrees on
REQUIREMENTS SPECIFICATION
impose safety restrictions
contributes to and agrees on
ENGINEERING CONTRACTOR
conducts
DETAILED ENGINEERING DESIGN
conducts
TESTING AND COMMISSIONING
provides the service (maintenance)
OPERATIONS AND MAINTENANCE
carries out the operations

Figure 5: Stakeholders in oil and gas engineering projects. Based on: [(Yoset 2017) and (Redutskiy 2017b)]

Fulfilling the requirements, the ***detailed engineering design*** of the solution is conducted by the contractor company. In the next stages, the technological solutions are ***commissioned and tested*** at the facilities and prepared for the ***operations***. Still, the contractors are responsible for the solution’s design and providing further ***service and maintenance*** according to the contract. The system’s testing is conducted to confirm that the installed system is safe and complies with the requirements; otherwise, it is mandatory to run changes in the safety system design (Esparza and Hochleitner 2010).

In addition, important to realize that the contractors who develop the engineering solutions including the necessary safety systems have their own angle in the engineering design context (Redutskiy 2017a). As mentioned before, the contractors participate in bidding competitions to get the hired for their services. Therefore, their proposed solutions should be cheap to be attractive to the hiring operating company. Such solutions can lead to redesigning the safety systems later in the stages. Then the stakeholders of the project will give permission to start up such solutions or reject.

In any case, the requirements specification documents, especially its part concerning the safety requirements, will provide the design basis for developed automated safety systems. Therefore, it is essential that vendors and subcontractors of the engineering contractors verify that assumptions specified in the requirements specification document are in complete agreement with the specifications of their products. Any operational, functional, and environmental limitations related to various subsystems or components which do not satisfies the requirements must be identified and brought to the attention of the engineering contractor and the operator (NOGA 2004). In general, the overall objective of safety system design, implementation, and maintenance is to ensure that the system is able to perform the intended safety functions if or when a specific process demand for it (in other words, a technological incident) should occur (Lundteigen and Rausand 2008).

The safety systems design is associated with the choice of certain devices among the options available, choice of certain instrumentation architectures, decisions on introducing additional safety measures, and planning the maintenance of facilities as well as instrumentation systems (Redutskiy 2017a). It is impossible to design an industrial system that could be maintenance-free due to the technical limitations (Markeset and Kumar 2001). Nevertheless, it is possible to achieve a balance between the investments into the safety system's complexity and the maintenance expenses by using life cycle viewpoint when the design of a safety system is conducted (Moss 1985).

Design, operations, and maintenance of a safety system installed at an oil and gas facility (or any hazardous technology) are associated with expenditures throughout the entire life cycle of the designed system. Major parts of the overall life cycle costs are: the procurement (or purchasing) costs, costs of the systems operations (energy consumption and the system's maintenance), and finally, risk costs. The maintenance of SIS is executed in two ways such as (1) continuously during the operation and (2) periodically in the form of proof tests (i.e. interval tests), which implies shutting down the processes for a certain period to fix all the failures that could not be fixed while the system is running.

Conducting maintenance is associated with costs of staff, maintenance tools, spare parts, and facility downtime (production losses) for the duration of the proof tests (Redutskiy 2017a). The economic perspective of planned maintenance is, first, to minimize the total cost of inspections and repairs, and second, to reduce the systems downtime, e.g., as measured in loss of production or reduced production quality (Eti, Ogaji and Probert 2007). These points are essential for the projects in oil and gas sector, because the stakeholders e.g. government, E&P operators and other companies involved in the development of new industrial facilities and infrastructure expect the overall profit. Thus, the operating companies' concern is about the capital costs of deploying the new facilities and setting up the automated systems, and at the same time, one of the priorities is smooth operation (i.e. less facility downtime) throughout the timespan of the systems operations in order to ensure profitability of their projects. To conclude this section, it should be pointed out that an automated safety system is as safety barrier that is crucial for any hazardous technology. A safety system that is poorly designed may fail to prevent technological incidents that may have serious consequences, such as destruction of the process facilities and assets, as well as harm to the staff involved in the operations. Another problem that an improper design often causes is spurious activation of the safety instrumentation (Wang, et al. 2016). The spurious activations of SIS in oil and gas industry lead to production loss and stress on affected components and systems. Then a partial or full process shutdown and hazards during system restoration and start-up (Lundteigen and Rausand 2008), as well as loss of confidence to the SIS, and more undesired events due to the increased number of shutdowns and start-ups (Lundteigen 2008). Thus, it is important to design the system solutions properly. Therefore, an appropriate design method should aim to avoid of failure actions and spurious activation and to ensure the overall safety of operations.

1.6 Research Purpose and Value

The purpose of this research is to provide firstly a better understanding of the reasonable recommendations for the organizational measures concerning the safety system for remotely located oil and gas (O&G) facilities. Secondly, optimizing the safety system design and the safety instrumented system maintenance problem with a focus on the details of maintenance through workforce scheduling. With this, the relevant issues as the maintenance staff size, duration of maintenance personnel trips and shifts, and transportation of the personnel to and from the facilities remotely located, and the frequencies of maintenance services for the facilities. The research questions are further detailed in the research design methodology section, 3.2.

The objective of the thesis is to address the problem of optimizing the set of safety measures inherent in safety instrumented system (SIS) together with the approach to the SIS maintenance through workforce scheduling. From the perspective of an engineering project, the results of this SIS design and maintenance planning optimization should be valuable at the stage of defining the requirements specification, helping to formulate rather clear functional safety requirements, which can be further used as a starting point for the detailed engineering design of SIS.

2.0 Theoretical frameworks

The literature review provides a brief overview of main theoretical frameworks. These are (1) Risk reduction, (2) Reliability Theory, (3) Asset Management, (4) optimization Theory. The (3) and (4) are discussed under the section research methodology.

2.1 Risk reduction

2.1.1 Safety Barriers

Safety is defined as the absence of unwanted events, which essentially means as the absence of risk, thus, a higher level of safety is either to prevent from the unwanted events or to protect against their consequences (Hollnagel 2004), as illustrated in Figure 6.

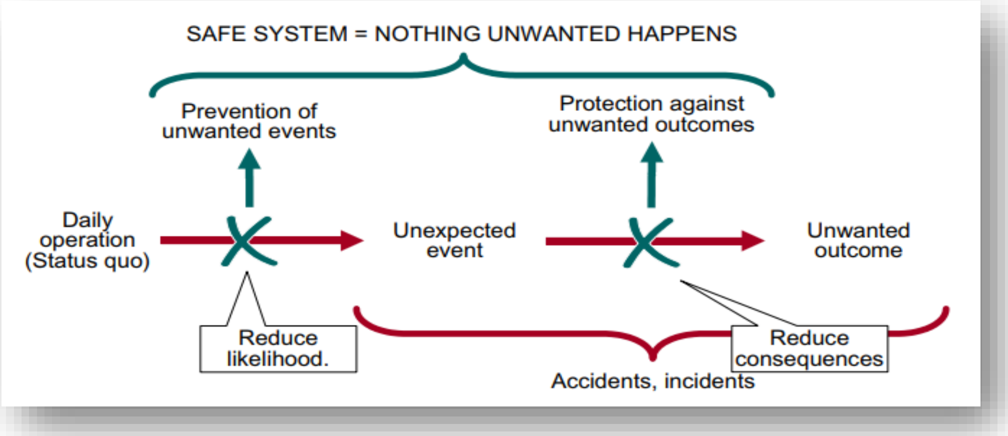

SAFE SYSTEM = NOTHING UNWANTED HAPPENS
Prevention of unwanted events
Protection against unwanted outcomes
Daily operation (Status quo)
Unexpected event
Unwanted outcome
Reduce likelihood.
Reduce consequences
Accidents, incidents

Figure 6: Safety through prevention and protection   Source: [(Hollnagel 2008)]

According to Reason (1990), accidents mostly happen due to a combination of an unexpected event and a dysfunctional or missing barrier, rather than to a single initiating action. There are various measures to reduce accidents. Safety barriers are widely used as measures (Hollnagel 2004). Sklet (2006) defines the terms as safety barrier, barrier function, and barrier system as following:

"Safety barriers are physical and/or non-physical means planned to prevent, control, or mitigate undesired events or accidents. A barrier function is a function planned to prevent,

control, or mitigate undesired events or accidents. A barrier system is a system that has been designed and implemented to perform one or more barrier functions."

Further, a barrier element is a component or a subsystem of a barrier system that by itself cannot perform a barrier function. A barrier subsystem may consist of several redundant barrier elements (Sklet 2006), this is in the case of safety system design, e.g. instrumentation as subsystems represented by their M-out-of-N (MooN) redundancies 2.1.4.2 , (IEC 61508 2010). A barrier system may comprise different types of system elements, e.g., physical, and technical elements such as hardware and software, operational activities executed by humans as well (Sklet 2006). However, all different safety barriers are used to reduce risks, and they are divided into two groups as passive and active barrier, further as physical, technical, and human/operational barrier, shown in Figure 7. Each safety barrier itself contains several elements, and reliability block diagrams can describe the behavior of the elements. Because reliability block diagrams are often used for documenting redundancy in safety systems (Duijm 2008).

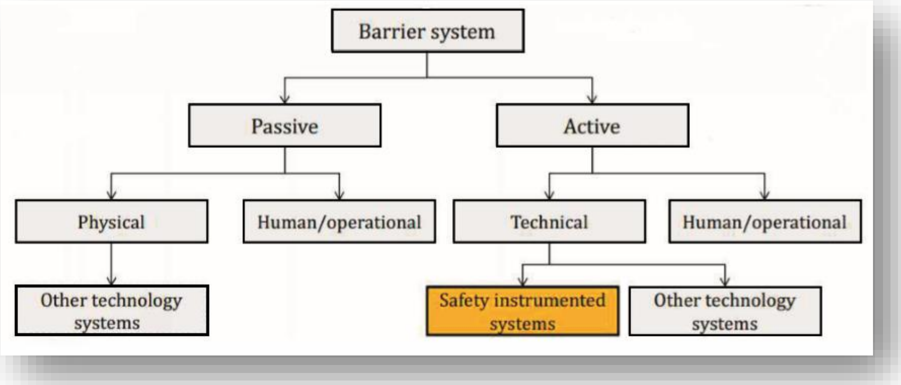


Figure 7: Classification of barriers Source: [(Jin 2013, Sklet 2006)]

The SISs are technical active safety barriers. In oil and gas industry, e.g., safety barriers introduced to prevent hydrocarbon releases, and a new method for qualitative and quantitative risk analysis of the hydrocarbon release frequency on oil and gas platforms introduced in (Sklet 2006). To conclude, all SISs are among the most important and effective safety barriers in reducing the likelihood of hazardous events and mitigating their serious consequences (Jin 2013).

2.1.2 Safety Instrumented Systems

Safety Instrumented Systems are widely used in process facilities for controlling the process and mitigating the possible risks. SISs are frequently used in the petroleum industry to detect hazardous events e.g. gas leakages and high-pressures (Hauge, Lundteigen and Rausand 2009). The standard ISA S84.01 defines SIS, as "SIS *is a distinct, reliable system used to safeguard a process to prevent a catastrophic release of toxic, flammable, or explosive chemicals.*" (ISA 1997). Similarly, the standard IEC 61508 defines SIS, as "SIS *is a system composed of sensors, logic solvers, and final control elements for the purpose of taking a process to a safe state, when predetermined conditions are violated.*" (IEC 61508 1998). The standard IEC 61511 defines SIS as an "*instrumented system used to implement one or more safety instrumented functions. A SIS is composed of any combination of sensors, logic solver, and final elements"* (IEC 61511 2003). Another definition of SIS in (Gruhn and Cheddie 1998) as *"safety instrumented systems are those designed to respond to conditions of a plant that may be hazardous in themselves or if no action were taken could eventually give rise to a hazard. They must generate the correct outputs to prevent the hazard or mitigate the consequences".*

In the process industry, all instruments installed in the process facility are entitled with the generic name of field of instruments, e.g. sensors, final elements, transmitters, valves, etc. (A. C. Torres-Echeverria 2009). In addition, logic solvers are Electrical (E)/Electronic (E)/Programmable Electronic Systems (PES) components or subsystems that execute the application logic, including input/output modules. Electrical refers to logic functions performed by electromechanical techniques, electronic refers to logic functions performed by electronic techniques, and programmable electronic system refers to logic performed by programmable or configurable devices e.g. Programmable Logic Controller (PLC) (ISA 1997). The duty of the input elements (e.g. sensors and transmitters) is to detect hazardous events, the logic solver is for deciding what to do, and the final control elements is to perform according to the algorithm in PLC (IEC 61508 1998). The PLC for SIS is a computer-based system that executing the safety functions to provide control capability, and communications systems for interfacing to other systems. The sensors can be varied according to the required measurements e.g., conventional transmitters; the sensor is connected to an electronic device that amplifies and transmits an analogue signal representing the measured variable. As well as the final control elements are varied, and the most common for safety systems are valves, electric motors, and alarm devices. Their reliability depends on their design and the actuator used to command it (A. C. Torres-Echeverria 2009).

2.1.3 System protection layers

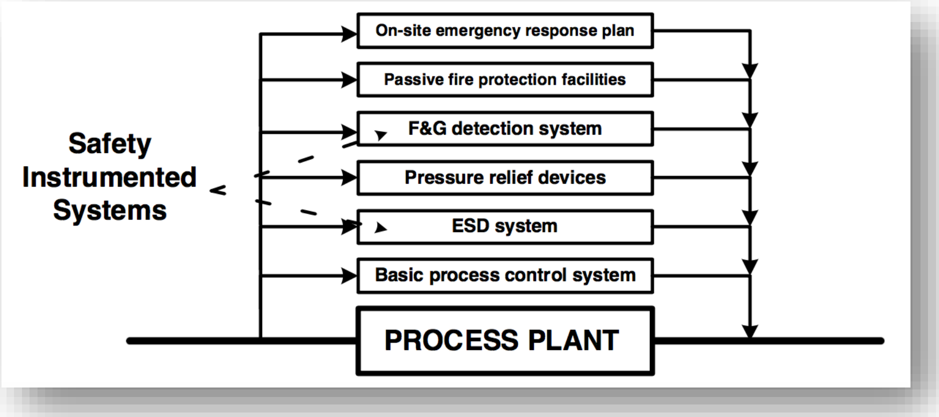

On-site emergency response plan
Passive fire protection facilities
F&G detection system
Pressure relief devices
ESD system
Basic process control system
PROCESS PLANT
Safety Instrumented Systems

Figure 8: Protection layers on a process facility   Source: [(A. C. Torres-Echeverria 2009)]

A layer of protection is a measure put in place as a defense to reduce the risk presented by the facility. Generally, all process facilities have more than one protection layers performing its function in a hierarchical manner for maintaining the safe state of the facility if the previous protection layer has failed to protect, Figure 8 (A. C. Torres-Echeverria 2009). It requires several SISs (e.g. ESD system, Pressure relief devices, and Fire & Gas detection system) must be installed providing multiple protections for ensuring the facility. In O&G industry, SISs are the most important and critical protection layers that are installed on the oil and gas facilities for reducing risks to a minimum level by detecting hazardous events and prevent them from their consequences (Chang, et al. 2015). They are named after their main functions as emergency shutdown (ESD) systems, process shutdown (PSD) systems, high integrity pressure protection (HIPPS) systems, and fire and gas (F&G) detection systems. These systems play an important role in the petroleum industry as well as in the other process industries (Lundteigen 2008). According to CCPS, Centre for Chemical Process Safety (2010), among all SISs, the ESD systems ensure the most significant risk reduction because they respond to highly critical situations where hazards with significant consequences. Thus, it is very important that the safety systems, especially the ESD systems must have a proper design to perform their functions correctly in any operations.

2.1.4 Safety Instrumented System Design

Referring to the standards (IEC 61508 1998, IEC 61511 2003), a general structure of SIS can be represented by a control loop, shown in Figure 9. The design of SIS requires achievement of safety integrity. The safety integrity requirements define the minimum levels of safety integrity and include the restriction of the safety system probability of failure on demand (PFDavg) to a maximum target limit and the minimum levels of fault tolerance (IEC 61508 2010). The fault tolerance is the capacity of a safety system to prevent single faults escalating into system failures that usually achieved by some form of redundancy (e.g. hardware and software redundancy).

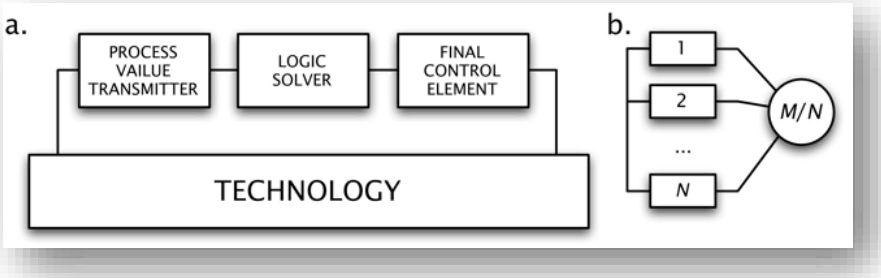


Figure 9: Structure of SIS, introduced by IEC 61508 & IEC 61511 Source: [(Redutskiy 2017a)]

The standards IEC61508 (1998) and IEC61511 (2003) highlighted that redundancy is one of measures that ensure a certain level of safety with regard to the SIS design. Then, several identical redundant components may be sensitive to stress factors that may lead to all components fail at the same time (A. C. Torres-Echeverria 2009).

Another measure is the introduction of additional electrical and physical separation of the devices in each subsystem to mitigate the phenomenon of common-cause failure (CCF), which occurs when all the components of a subsystem fail simultaneously (IEC 61508 1998). Therefore, the technologies of diversity are used for mitigating the problem of CCF, while using identical redundancy to address the problem of random failures in the system (A. C. Torres-Echeverria 2009). In the event of a SIS failure, the purpose of SIS is to force the process in to its fail-safe condition, where the presence of harm is eliminated (W. E. Anderson 2005). For instance, a control valve moves to its fail-open or fail-close condition depending on the SIS design, thereby the ultimate objective of designing SIS is to comply with the requirements of safety integrity level (SIL) (Gabriel 2017).

The process of determining SIL is described in the standard (IEC 61508 2010), and it is based on the risk assessment. The risk is known as a combination of probability or frequency of dangerous event occurrence and its consequences. The safety systems must achieve high levels of dependability (Laprie 1992), thus the reliability and availability of safety related systems need to compliance with the required specifications. A challenge for SIS designers is to balance the SIS reliability with the performing proof tests, which are important means to reveal SIS failures, because performing proof tests is associated with costs of labor and tools as well as production losses due to facility downtime for the duration of the tests. Furthermore, there are many requirements from authorities, oil companies, and international standards, given to the engineering contractors when it comes to the design of safety systems. Thus, the engineering contractors may use the safety life cycle model, which is introduced in the standard IEC61508 (1998), as basis for their product development.

In addition, a non-optimal SIS design can be caused by (1) overdesigned and (2) under designed structures. An overdesigned SIS results in more initial cost, more operation and maintenance cost, and higher spurious trip rate leading to less safety. On the other hand, there will be no safety requirements compliance at all if a SIS under designed. In such cases, the designed SIS can achieve at least the minimum level of safety integrity, SIL 1, but most likely the system will result in a low availability due to depending on the components reliability (Esparza and Hochleitner 2010). Consequently, such insufficient specification of requirements to SIS design often resulting in the development of a solution that marginally ensures the required level of safety (HSE 2003). Therefore, an optimal design and operation of SIS is essential for an effective performance, which intended to reduce risk of hazards to acceptable levels. A SIS must follow a safety life cycle to ensure that the required dependability level is achieved and maintained properly during its entire operating lifetime. This is mainly devised and executed during its design (A. C. Torres-Echeverria 2009).

2.1.4.1 Fault Tolerance for SIS

There are two approaches such as fault prevention and fault tolerance, discussed by some authors. Laprie (1992) stated, *"Fault prevention intends to avoid faults occurring or being introduced into the system, while fault tolerance is a measure to prevent that faults that take place during service provoking a system failure"*. Similarly, in (Jalote 1994) mentioned as *"fault prevention methods focus on methodologies for design, testing, and validation; whereas fault tolerant methods focus on how to use components in a manner that such failures can be masked"*. In safety related systems, the fault tolerance (FT) is achieved by using redundancy. A system is fault tolerant if it can prevent the system from the occurrence of faults by means of redundancy e.g., connecting two transmitters in parallel provides some degree of fault tolerance (A. C. Torres-Echeverria 2009), which is fundamental against dangerous failures in safety systems. The most used form of redundancy is the parallel structure (Torres-Echeverria, Martorell and Thompson 2012).

There are three ways to implement redundancies in the safety systems: (1) passive (i.e. static) that means it requires no extra actions to take for preventing the faults from resulting in further failures, (2) active (i.e. dynamic) that relies on taking some action to detect faults for removing the faults from the system, and (3) hybrid, which is a combination of (1) and (2), according to (Storey 1996). The fault tolerance is used mostly for computer systems. And SISs can be defined as safety computer system, because the logic solvers of SIS are computers (i.e. industrial computers). For the oil and gas facilities, fault tolerance is implemented when redundancy is added to the field instruments e.g. valves, measurement devices, etc.

2.1.4.2 Voting architectures for SIS

In process industry, SIS architecture is practically limited to parallel and majority voting architectures with small number of component e.g. up to four (A. C. Torres-Echeverria 2009). Basis redundancy architecture of SIS, regarding field instruments, is presented in (Gruhn and Cheddie 1998) as for sensors the architectures 1oo1D, 1oo2D and 2oo3, and for final control elements 1oo1, 1oo2 and 2oo2. The architectures with D are the voting architectures with diagnostics (MooND), which indicate that the diagnostic circuit added for logic solvers for modifying the voting output of the system to convert dangerous failures into safe failures. Several dependability models for PES for some architectures with diagnostics as 1oo1, 1oo2, 2oo2, 1oo1D, 2oo3, 2oo2D, and 1oo2D, developed by (W. Goble 1998), which later used as practical process examples. Another most common voting architectures is identified in (CCPS 2007) as for sensors 1oo1, 1oo2, 2oo2, and 2oo3, for logic solver 1oo1, 1oo2, 2oo2, and 2oo3, and for final control elements 1oo1, 1oo2, and

2oo2. In some cases, there will be such architecture 2ooN, where N is a large number. This is not a common architecture, but it can be for *"where the unacceptable process condition can occur in multiple distinct locations,"* (A. C. Torres-Echeverria 2009).

In addition, the standard IEC 61508 (2010) and IEC 61511 (IEC 61511 2003) present these architectures, 1oo1, 1oo2, 2oo2, 1oo2D, and 2oo3 under the name of MooN (M-out-of-N) systems. The standard IEC 61508 (2010) provides an analysis how to obtain simplified equations by means of Reliability Block Diagrams (RBD) for the above-mentioned architectures. A definition of the MooN system is given in IEC61511 (2003): "*Safety Instrumented System, or part of thereof, made of "N" independent channels, which are so connected that "M" channels are sufficient to perform the safety instrumented function*". In (CCPS 2007) as *" "N" designated the total number of devices (or channels) implemented; "M" designates the minimum number of devices (or channels) out of N required to initiate, take, or maintain the safe state."* Thus, it requires a minimum of M units to vote for the execution of the safety function, see Figure 9 (Torres-Echeverria, Martorell and Thompson 2012).

The SISs are usually implemented using simple parallel and MooN majority voting architectures (A. C. Torres-Echeverria 2009). The systems with MooN voting redundancies are a special case of K-out-of-N systems. The failure criterion of a MooN system is the failure of N-M+1 components, where $M \leq N$ and M out of N components are necessary to begin an action (Torres-Echeverria, Martorell and Thompson 2011).

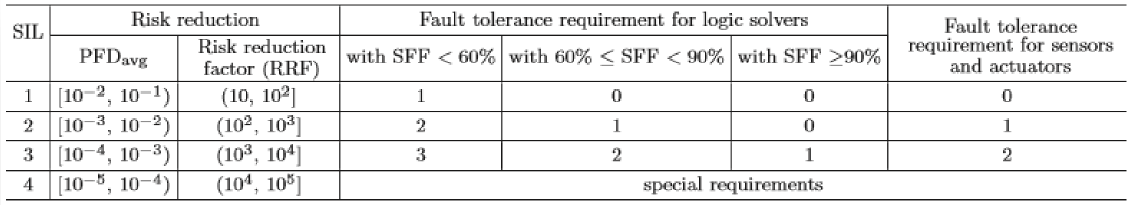
2.2 Safety requirement Specification

In petroleum industry, there are used numerous safety systems that aim to detect the onset of hazardous events and to mitigate the serious consequences of accidents/incidents. SISs are often implemented to reduce the risk to an acceptable level (i.e. an acceptable risk level is a criterion), which is often represented as safety requirement specification set by authorities, company requirements or by the stakeholders during risk analysis (Eliassen 2013). Safety requirement specifications (SRS) are specifications that describe the required safety function that must be performed by a SIS.

The safety requirements can be divided into two main categories. First, the functional safety requirements, which are the safety requirements related to the intended purpose of the facility or equipment (e.g. to ensure the facility or equipment maintain a safe state).

In other words, the specification of safety functions makes explicit the requirements needed to prevent risk of incident throughout all operational modes of the facility or equipment. Second one is the safety integrity requirements that are related to the failure-free performance of a safety system, thus the safety integrity level (SIL) can be expressed quantitatively as an average probability of failure on demand (PFDavg) representing the mechanisms of failures and incidents occurrence for safety systems, in Table 1.

Table 1: Requirements for SIL, defined by IEC61508 & IEC61511 Source: [(Redutskiy 2017a)]



SIL	Risk reduction		Fault tolerance requirement for logic solvers			Fault tolerance requirement for sensors and actuators
	PFD$_{avg}$	Risk reduction factor (RRF)	with SFF $< 60\%$	with $60\% \leq$ SFF $< 90\%$	with SFF $\geq 90\%$	
1	$[10^{-2}, 10^{-1})$	$(10, 10^{2}]$	1	0	0	0
2	$[10^{-3}, 10^{-2})$	$(10^{2}, 10^{3}]$	2	1	0	1
3	$[10^{-4}, 10^{-3})$	$(10^{3}, 10^{4}]$	3	2	1	2
4	$[10^{-5}, 10^{-4})$	$(10^{4}, 10^{5}]$	special requirements			

Likely, failure mechanisms are present in all control systems to varying degrees, thus the safety measures needed to overcome control system failures include (a) the selection of high reliability components, (b) the development of a fault tolerance architecture for the entire system, from sensors through to actuators, and (c) a fault avoidance approach to the design process (HSE 2003).

2.3 Standards IEC61508 and IEC61511

The International Electrotechnical Commission (IEC) introduced the standards, IEC 61508, and IEC 61511. In oil and gas industry, the IEC 61508 (1998) and IEC 61511 (2003) standards are widely used during all phases of the SIS lifecycle. Both standards use SIL as measure of SIS reliability and provide the framework for quantification of SIL, as well as define the four safety integrity levels, from SIL1 to SIL4. They also describe the desired safety and reliability performance that covers (1) the functional safety requirements, stating the tasks SIS required to do and (2) the safety integrity requirements, stating the performance of the SIS (Lundteigen 2008). Therefore, the role of international standards is key of importance for hazardous facilities requiring certain safety measures. In general, the international standards, (IEC 61508 1998) & (IEC 61511 2003) provide a unified approach to safe and reliable SIS design, implementation, and operation and maintenance, considering the challenges and opportunities of using technology and work processes, and procedures (Lundteigen 2008).

2.3.1 Standard IEC 61508

The IEC 61508 (1998) standard, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems" is a basic functional safety standard that is applicable for suppliers of microprocessor-based instrumentation to all kinds of industry. It defines functional safety as *"a part of overall safety relating to the equipment under control (EUC) and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities."* The (IEC 61508 1998) standard presents the ALARP principle. This principle requires that any risk should be reduced to a level that is as low as reasonably practicable (ALARP) considering the technical and economic aspects. Therefore, a safety measure should only be introduced if the benefits of employing the safety measure prove to be greater than the cost of the risk reduction measure. It requires every safety function must achieve a specific SIL, which will be determined in advance based on a previous risk assessment (A. C. Torres-Echeverria 2009). Later, a new IEC 61508 (2010) standard is developed as a performance-oriented standard, thus it specifies the design and operation of SIS to achieve the necessary risk reduction. Thereby, it does also introduce the safety integrity levels (SIL) as the overall performance measure, which can translate the necessary risk reduction into technical requirements and process requirements concerning design, operation, and maintenance (Innal, Lundteigen, et al. 2016). The standard IEC 61508 (2010) organizes its requirements according to a safety life cycle that comprises 16 phases.

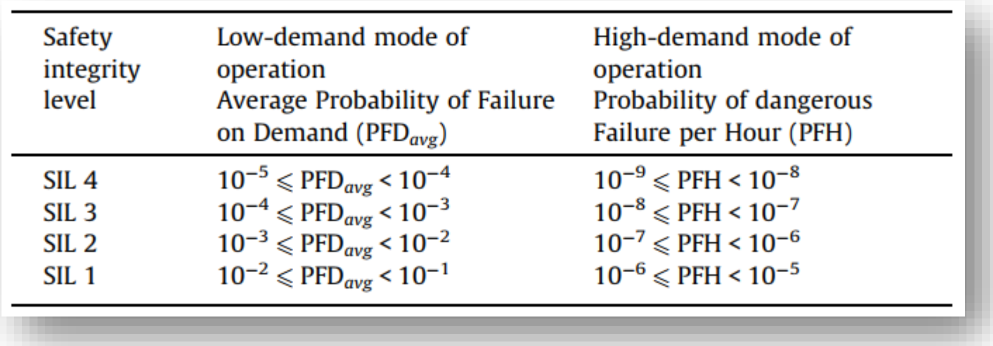
2.3.2 Standard IEC 61511

The IEC 61511 (2003) standard "Functional Safety- Safety Instrumented Systems for the Process Industry Sector" is a sector standard for the end user (e.g., oil and gas facilities), integrators, and the designers of the SISs, as well engineering companies detailing the requirements for design and implementation of SIS for the process industries. In general, the standard defines requirements that must be fulfilled in given devices or subsystems implemented in SIS. In other words, it is a technical standard, which sets out practices in the engineering design of systems in order to ensure the safety of an industrial process using SIS. The IEC 61511 (2003) standard is explicitly from the IEC 61508 (1998) standard; thus, it cannot be completely implemented without referring to the IEC 61508 standard. The IEC 61511 standard also provides the design and management requirements for SISs throughout the entire safety life cycle.

2.3.3 Safety Integrity

Safety is "*the expectation that a system does not, under defined conditions, lead to harm people, either directly or indirectly*" (CCPS 2007). Safety integrity is defined in the standard IEC 61508 (1998) as "*probability of a safety related system satisfactorily performing the required safety function under all the stated conditions within a stated period".* A safe state is generally achieved when a SIS performs its intended safety integrated functions (SIF). If the SIS fails to perform those SIFs, the hazardous event may result in an accident, thus each SIF implemented into a SIS is required to have a high reliability, which is expressed as a safety integrity level (Eliassen 2013). The SISs are normally operate in the low demand mode, which means that regular testing and inspection are required to reveal SIS failures (Lundteigen and Rausand 2007). Depending on how often the demand occurs SISs are classified as low-demand systems and high-demand systems in . The IEC 61508 (1998) standard defines the low-demand mode of operation as *"where the frequency of demands for operation made on a safety- related system is not greater than one per year and no greater than twice the proof-test frequency".* Further, the operational demand modes of safety systems are different in function of two different dependability parameters such as probability of failure on demand (PFD_{avg}) and probability of dangerous failure per hour (PFH).

Table 2: SIL requirements for dependability parameters, IEC61508 Source: [(Catelani, Ciani and Luongo 2011)]



Safety integrity level	Low-demand mode of operation Average Probability of Failure on Demand (PFD_{avg})	High-demand mode of operation Probability of dangerous Failure per Hour (PFH)
SIL 4	$10^{-5} \leqslant PFD_{avg} < 10^{-4}$	$10^{-9} \leqslant PFH < 10^{-8}$
SIL 3	$10^{-4} \leqslant PFD_{avg} < 10^{-3}$	$10^{-8} \leqslant PFH < 10^{-7}$
SIL 2	$10^{-3} \leqslant PFD_{avg} < 10^{-2}$	$10^{-7} \leqslant PFH < 10^{-6}$
SIL 1	$10^{-2} \leqslant PFD_{avg} < 10^{-1}$	$10^{-6} \leqslant PFH < 10^{-5}$

In addition, the safety validation should be performed in terms of the overall safety function requirements and the overall safety integrity requirements, taking in to account the safety requirements allocation for safety system in designing. Moreover, the IEC 61508 and IEC 61511 introduce a set of additional requirements to SIS design for achieving a sufficiently robust system architecture. These requirements are referred to as architectural constraints in (Lundteigen and Rausand 2009) and their intention is to have additional channels to ensure the activation of the SIF in case of failure occur in the SIS. The failure of safety instrumented systems (i.e. not performing its intended safety functions) results in loss of the assets, damages to the environment, harm to personnel on the facilities, and even in worst scenario loss of life (A. C. Torres-Echeverria 2009).

2.4 Reliability Theory

2.4.1 Reliability

In general, reliability presents the ability of an item or system to perform its intended function. The study of reliability includes many different aspects. The reliability theory is derived mainly from probability theory. A definition of reliability is given in (A. C. Torres-Echeverria 2009) as "*the probability of a component or system to perform its intended function during a specific period of time and under a given set of conditions.*" Thus, reliability is measure of dependability. The term dependability is used as reference to attributes such as availability, reliability, and safety in (Laprie 1992). Thereby, a definition of dependability is given in (Rausand and Høyland 2004) as "a collective term to describe the availability performance and its influencing factors", and one more definition found in (Avizienis, Laprie and Randell 2000) as *"dependability is the ability to deliver a service that can justifiably be trusted"*. In (Rausand and Høyland 2004) mentioned that system reliability approach focuses on the reliability of systems composed of several components, based on the probability distribution function of the failure-times of those components.

Study shows that there are many methods have been developed for analyzing the reliability of a system, such as Fault Tree Analysis (FTA), Reliability Block Diagram (RBD), reliability graph (RG), Markov Analysis (MA), and Monte Carlo Simulation (MCS), and of course each method has its own advantages and disadvantages (Kim 2011). In case of safety systems, the standards IEC 61508 (1997) and IEC 61511 (2003) propose methods of safety quantification with the help of simplified equations based on RBD and FTA, and these two approaches work with static methods and mean values, thus they are simple and visual (Redutskiy 2017a). According to Dutuit et al. (2008), the FTA is too simple to handle for the practitioners and it provides approximations which sometimes bring non-conservative results, on the other hand, the use of switching MA is suitable to taking into account dependencies due to proof testing and common cause failure (CCF). The MA is a more complex approach that works with dynamic models and it provides more flexibility for incorporating many failure modes and analyzing their interactions (Redutskiy 2017a).

2.4.2 Reliability importance

In technical systems, the reliability importance of components is measured, because such importance measures provide information how the reliability of individual components influences the reliability or unreliability of the system. Thus, the component`s importance depends on the component`s reliability and location in the system structure (Liu and Lundteigen 2015). Regarding system components, RBD are suitable for systems of non-repairable components, where the order in which failures occur does not matter. On the contrary, MA will be more applicable for the systems that are repairable and/or the order in which failures occur is important (Rausand and Høyland 2004). However, the reliability or unreliability of the safety systems is quantified by the average probability of failure on demand (PFD_{avg}) (Liu and Lundteigen 2015). Referring to SIS, the reliability prediction plays a fundamental role because SISs include complex interactions of pneumatic, hydraulic, electrical, and programmable electronic components. Thus, it is necessary to select a method that can capture the complexity and at the same time contribute with more insight to how the SIS works among SIS designers, operators, and maintenance personnel (Catelani, Ciani and Luongo 2010).

2.4.3 Reliability and Failure Rate

With reference to (A. C. Torres-Echeverria 2009), reliability is the probability of an item that performs its intended function for a specific period of time under specific conditions (i.e. is a probability of non-failure of system) as mathematically expressed as following:

(1) $R(t) = 1 - \int_0^t f(t)dt$

In contrast, the probability of failure for a specific period of time under specific conditions is then as following:

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

Failure rate is the number of failures per unit time of identical items, and it is illustrated as a bathtub curve in Figure 10. This curve explains that the failure rate is high and decreasing in the infant mortality phase that is because many of items can be weak with production fail or other faults. After that, the failure rate is constant practically in the useful time phase, as called constant failure rate, but during this time the components fail randomly caused by external loads. In the last phase, the components ages, thus, the failure rate increases.

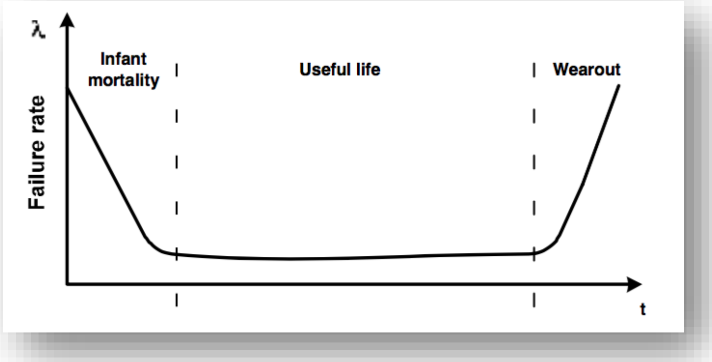


Figure 10: A model "Bathtub curve" of failure rate Source: [(A. C. Torres-Echeverria 2009)]

According to Goble (1998), the constant failure rate would be a conservative worst-case assumption that can be used, referring to (A. C. Torres-Echeverria 2009); the constant rate is a valid assumption for many devices, especially electronic devices. The failure rate can compute as follows (W. Goble 1998).

(3) $\Lambda\ (\mathrm{t})=\frac{f(t)}{R(t)}$

Moreover, the constant failure rate leads to an exponential distribution with a cumulative distribution function, and the cumulative distribution function computes as follows (Lewis 1996).

(4) $F(t) = 1 - e^{-\lambda t}$

(5) $R(t) = e^{-\lambda t}$

Assumption: $\lambda t \ll 0.1$ this denotes that λt is very small. Thus, the probability of failure (i.e. unreliability) can be approximated by the rare event approximation as follows (A. C. Torres-Echeverria 2009).

(6) $F(t) \approx \lambda t$

2.4.4 System Reliability

The total reliability of a system, which contains several of components, can be quantified considering the structure of each component. As mentioned before, there are several different structures for a system. Study shows that for SIS the basic system structures are series, parallel, M-out-of-N, and K-out-of-N, see Figure 12. Thus, a parallel structure characterizes a system that functions if at least one of its components functions. The reliability of such system is as following (A. C. Torres-Echeverria 2009):

(7) $R_{sys} = 1 - (1 - R_1) \cdot (1 - R_2) \cdot \ldots \cdot (1 - R_n) = 1 - \prod_{i=1}^{n} (1 - R_i)$

> Assumption: the term $(1 - R_i)$ is equal to the unreliability of components, thus, if the value is given, it can be directly placed in the equation.

If the system composed of only two components, it can be calculated as follows:

(8) $R_{sys} = R_1 + R_2 - (R_1 + R_2)$

Furthermore, the K-out-of-N structure represents a system that functions if at least K out of the total N components function. This structure is often referred to SIS. And the M-out-of-N structure is equivalent to a K-out-of-N. It assumed that all N components are identical, thus the reliability of such system can be quantified as following (A. C. Torres-Echeverria 2009):

(9) $R_{sys} = \sum_{i=k}^{n} \left(\frac{n!}{i!(n-i)!}\right) R^i (1 - R)^{n-i} = \sum_{i=k}^{n} \binom{n}{i} R^i (1 - R)^{n-i}$

To conclude, the equations of system reliability are applicable to system availability quantification, because both terms are defined as probabilistic measures of system dependability (i.e. system trustworthiness). In order to enhance the reliability of SIS, there are several choices either to improve the inherent reliability by introducing more reliable components, add more redundancy, or carry out more often regular proof testing, which may be costly due to higher operational costs follow from the higher frequency of maintenance and production stops, according to (Innal, Lundteigen, et al. 2016).

2.4.5 Proof test and failure detection

To verify that a SIS performs its safety functions and to reveal any failures, there are several tests have been defined such as diagnostic testing, function testing, and visual inspections (Lundteigen and Rausand 2007). These tests are classified generally by their solicitation mode as on-line or off-line, e.g. diagnostic tests are on-line tests that detect random failures of a component or a system, while proof tests are off-line, which are periodic inspection tests (Mechri, Simon and Ben Othman 2015). More specific, the proof tests are performed to detect the hidden undetected failures of a system in operation. After detecting the hidden failures, the system can be restored in a condition "as good as new" or as close as practical to this condition (IEC 61508 2010). The proof tests are performed at regular intervals (Rahimi and Rausand 2013), and the test interval (T_i) is considered equal to the time between two consecutive proof tests (J. Bukowski 2001). According to Torres-Echeverria et.al (2009), several strategies that can be applied to the proof tests, and the author pointed out four main strategies as follows. The first one is *simultaneous test*, which requires all components must be tested together, and then it needs a sufficient number of technicians to test all system components. During proof test, the SIS is unavailable. The second strategy is *sequential test* that tests all components consecutively one after the other. The third one is *staggered test* where all components are tested with their own period of time. The fourth one is *random test*, which means the time interval between two tests of components is randomly chosen. Moreover, Innal et al. (2016) pointed out that the purpose of performing proof tests is to detect the hidden dangerous undetected failures, which are more critical than other failures. Regarding to system reliability, having more often proof tests can be a strategy to enhance the system reliability, but it may have some possible negative effects such as higher operational costs (i.e. more frequent planned maintenance and production stops cost more) and increased risk level due to more abruption of normal operation.

2.4.6 Failure modes

The standard IEC 61508 proposed a failure mode classification, and it splits all failures into four categories according to failure causes.:

a. *Dangerous Undetected (DU)*- failures that only revealed by a functional test (i.e. proof test) or upon a demand
b. *Dangerous detected (DD)*- failures that detected by automatic self -test or incidentally by personnel
c. *Safe Undetected (SU)*- failures that not detected by automatic self-test or incidentally by personnel and resulting in a spurious trip of component
d. *Safe detected (SD)*- failures that have a potential to spurious trip and revealed by automatic self-test or incidentally by personnel

A definition of safe failure is given as a *"failure that does not have the potential to put the safety-related system in a hazardous or fail-to-function state"* (IEC 61508 2010). Additionally, a different definition of safe failures is given in the PDS method (a method presented and used in Norwegian O&G industry), as "*failures with a potential to cause a spurious trip*", i.e. failures where the safety system is activated without a demand (Hauge, Lundteigen and Hokstad, et al. 2010). According to the standards (IEC 61508 1998) and (IEC 61511 2003), the dangerous failures are failures that prevent the SIS from functioning on demand. Thereby, dangerous detected failures are failures that detected by diagnostic testing, which is performed by dedicated software and hardware that is usually implemented in the components or added to the SIS configuration (Lundteigen and Rausand 2007). During inspection and function testing, which are performed at regular intervals, discover dangerous undetected failures (IEC 61511 2003). The interval between function tests effect directly on the safety instrumented function`s probability of failure on demand (Lundteigen and Rausand 2007). Furthermore, based on the classification of failure modes, the failure rate λ can be defined as follows (IEC 61508 2010).

- λ_{DD}, Rate of dangerous detected failures
- λ_{DU}, Rate of dangerous undetected failures
- λ_{SD}, Rate of safe detected failures (spurious trip)
- λ_{SU}, Rate of safe undetected failures (spurious trip)

In addition, the PDS method presents a rate of critical failures noted as λ_{crit}. This indicates the failures which unless detected can cause a failure on demand or a spurious trip of the safety function (Hauge, Lundteigen and Hokstad, et al. 2010), in Figure 11.

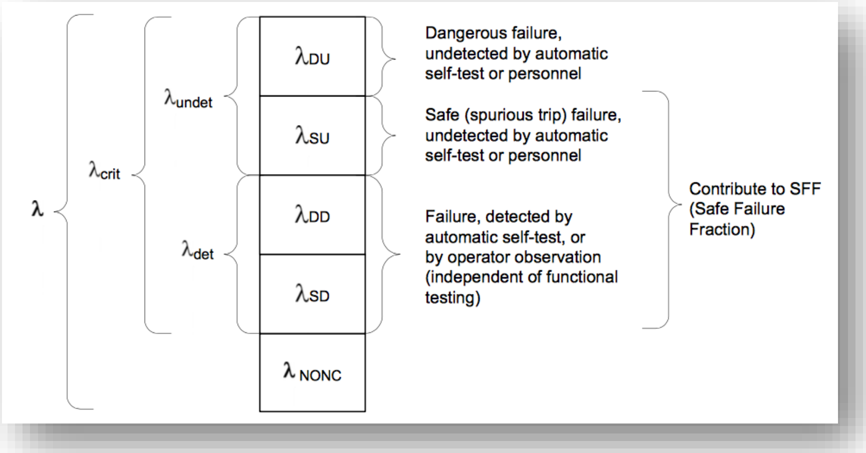

λ
λcrit
λundet
λdet
λDU
λSU
λDD
λSD
λ NONC
Dangerous failure, undetected by automatic self-test or personnel
Safe (spurious trip) failure, undetected by automatic self-test or personnel
Failure, detected by automatic self-test, or by operator observation (independent of functional testing)
Contribute to SFF (Safe Failure Fraction)

Figure 11: Different elements of the failure rate of safety system Source: [Hauge et al. (2010)]

All failures considered, it is important realizing that all detected failures and undetected safe failures contribute to safe failure fraction (SFF) in 2.4.8.

2.4.7 Diagnostic Coverage

With reference to (IEC 61508 2010), the diagnostic coverage (DC) is *"fractional decrease in the probability of dangerous hardware failures resulting from the operation of automatic diagnostic tests"*. The standard introduces the term "safe diagnostic coverage", to present the fractional decrease of safe random hardware failures. The term random hardware failures refer to failures resulting from the natural degradation mechanisms of the component (Hauge, Lundteigen and Hokstad, et al. 2010). According to (Mechri, Simon and Ben Othman 2015), the failures of safety systems are divided into two main groups such as (1) safe failures-λ_S, and (2) dangerous failures- λ_D. These two groups are divided further into four failure modes as detected failures $\{\lambda_{SD}, \lambda_{DD}\}$ and undetected failures $\{\lambda_{SU}, \lambda_{DU}\}$ by using of the rate diagnostic coverage (DC). The diagnostic testing reveals the detected failures, while proof testing only reveals undetected failures. The standard IEC 61508 defines the rate DC as the ratio between the failure rate of detected dangerous failures (λ_{DD}) and the total failure rate of the dangerous failure rate (λ_D), referred in (Goble and

Brombacher 1999). In (IEC 61508 2010) a formula is given to compute the DC rate as following:

(10) $DC = \frac{\lambda_{DD}}{\lambda_D} = \frac{\lambda_{DD}}{\lambda_{DD}+\lambda_{DU}}$

(11) $\lambda_{DD} = DC\lambda_D \,, \lambda_{DU} = (1 - DC)\lambda_D$

Thereby, the rate DC measures the effectiveness of the diagnostic test, and considering the estimated DC; the total failure rate λ^T is as follows (Mechri, Simon and Ben Othman 2015):

(12) $\lambda^T = DC\lambda_D + (1 - DC)\lambda_D + DC\lambda_S + (1 - DC)\lambda_S = \lambda_{DD} + \lambda_{DU} + \lambda_{SD} + \lambda_{SU}$

Here, to highlight that the dangerous failures split into two failure groups as dangerous detected (DD) failures- λ_{DD} and dangerous undetected (DU) failures- λ_{DU}. Only the fraction of DD failures among all dangerous failures is referred to as the diagnostic coverage. Thus, the dangerous failures rate is as follows (Innal, Lundteigen, et al. 2016):

(13) $\lambda_D = \lambda_{DD} + \lambda_{DU} = DC\lambda_D + (1 - DC)\lambda_D$

In (CCPS 2007), another definition of DC introduced as: diagnostic coverage (ε) is the fraction of total failure rate that can be detected by the diagnostic mechanism, which refers to an in-built hardware or software mechanism in safety systems for automatic detection of internal failures. The DC expresses in percentage, and the following formulas can be used for calculating detected and undetected failure rates (A. C. Torres-Echeverria 2009):

(14) $\lambda^D = \varepsilon \cdot \lambda^T$

(15) $\lambda^U = (1 - \varepsilon) \cdot \lambda^T$

2.4.8 Safe Failure Fraction

The standard IEC 61508 introduces the safe failure fraction (SFF) in relation to the requirements for hardware fault tolerance. SFF is the ratio of safe failures and dangerous detected failures to the total failure rate, as expressed following (IEC 61508 1998):

$$\textbf{\textit{(16)}}\quad SFF = 1 - \left(\frac{\lambda_{DU}}{\lambda}\right)$$

In the PDS method, SFF is the fraction of failures that are not critical with respect to safety unavailability of the safety function, and it can be expressed as follows (Hauge, Lundteigen and Hokstad, et al. 2010).

$$\textbf{\textit{(17)}}\quad SFF = 1 - \left(\frac{\lambda_{DU}}{\lambda_{crit}}\right)$$

$$\textbf{\textit{(18)}}\quad SFF = \left[1 - \left(\frac{\lambda_{DU}}{\lambda_{crit}}\right)\right] \cdot 100\%$$

Another definition of SFF is presented in (Gabriel 2017), as *"Safe Failure Fraction (SFF) is the fraction of the overall random hardware failure rate of a device resulting to a detected dangerous failure or a safe failure"*. The author also proposed a method to calculate SFF. According to the standard IEC 61508 (2010), all components, especially those, which require allowing the subsystem to process safety function (e.g. electrical, electronic, electromechanical, etc.) should be considered carefully when assessing the SFF and diagnostic coverage of a safety system.

3.0 Research Methodology

This section describes the research methodology used in the research of this thesis. Research methodology refers to a discussion of the underlying reasoning why particular methods are used, and methods are the technical steps taken to do the research. Thus, this part describes the formulation of the research question and a plan how to collect data and defining the methods that can be used for analyzing the data as well as the approaches used to solve the problem to answer the research questions.

3.1 Research objective

In theory, there are two main objectives of research such as (1) fact finding and (2) theory building. The theory building research makes predictions before evidence is gathered through data gathering, while fact-finding research uses data evidence to make theoretical predictions (Wacker 1998). This thesis is based on certain theoretical predictions used to select the methods of the research, its aim is to make theoretical predictions based on the analyzed data, and the result of computational models, thus the objective of this research fits the characteristics of both theory building and fact-finding.

3.1.1 Research strategy

In theory, the research strategies split into two parts such as (1) quantitative research, which concerns the quantification in the collection and analysis of data, and (2) qualitative research, which concerns more the descriptive detail and explanation of data. In addition, the relationship between theory and research is defined by two main approaches such as (1) deductive, where the researchers assumes one or more theoretical hypotheses and subjects them to empirical study, and (2) inductive, where the researchers build new theory based on their empirical findings and observations, into the certain theoretical domain, according to Bryman and Bell (2015). This thesis uses both quantitative and qualitative research strategies as well as belonging to the deductive approach of the research. With a qualitative research, the purpose of research is to gain a better understanding of the requirement specifications for SIS and the nature of the problems related to the SIS design and maintenance planning for remotely located O&G facility. On the other hand, with a quantitative research selecting optimization methods to solve the problem, addressing the issues of various maintenance policies for establishing the staffing size and determining the crew schedules for the O&G facilities located in remote areas.

3.1.2 Research design

A research design can be defined as a plan that helps the researcher in the process of collecting, analyzing, and interpreting observations (Nachmias and Nachmias 1993). It is the logical sequence that connects the empirical data to a study's initial research questions and, ultimately, to its conclusions (Yin 2003). Thus, the purpose of a research design is to maximize valid answers to the research questions and describing how, when and where data will be collected and analyzed. A better way to understand the model is by making a case study research in order to achieve the real time results, according to Yin (2014). In theory, there are two main designs of case studies such as (1) single-case design and (2) multiple-case design. The single-case study entails the detailed and intensive analysis of a single case, which can be a single organization, a single location, a single person, or a single event (Bryman and Bell 2015). On the contrary, a multiple-case study contains more than a single case, and the conduct of such a case requires extensive resources and time beyond the means of a single student (Yin 2003). To conclude, the research design of this thesis is a quantitative single-case study.

3.1.3 Research method

A research method is a technique for gathering the necessary data through available sources e.g., documentation, archival records, interviews, observations, or physical artifacts, according to Yin (2003). This thesis uses a combination of research techniques due to the choice of research strategies in 3.1.1. For better understanding of the problem set, it is essential to gather the necessary qualitative information about Safety system design in the petroleum industry and maintenance planning for the remotely located O&G facilities, thereby the focus is on the maintenance personnel (i.e., staffing size, personnel transportation, work scheduling), used search engines for scientific and academic research. There are many academic search engines available, but some engines, are the most relevant for this research and as well as the most trusted academic resources, that used widely by researchers and scholars. For the quantitative research, the data used in the research is taken from a project implemented by Rosneft in East Siberia in Russia. The chosen methodology for this study includes as following:

- Markov analysis of the safety system functioning, based on the standard Markov model for the safety system`s performance used in various works, like in Bukowski (2006).

- Lifecycle modeling of the whole solution`s reliability and costs associated with the decisions throughout the entire timespan of facility operations, based on the widely accepted cost modelling used in various works, like in Torres-Echeverria (2009), with the necessary modifications to reflect the approach to maintenance of the remotely located facilities.

- Black-box optimization of the safety system design and maintenance planning, following the ideas of the various works on engineering design, e.g., Martorell et.al. (2004).

3.2 Research problem and research questions

One of the most important parts of research is to define the research questions. The development of the research questions requires patience and time, and they need to have both substance (i.e. what the study is about) and form (i.e. who, where, how, or why), according to Yin (2003). During the different stages of the research study and as moving through the literature review, it is possible to go back to the initial research questions and revise them or suggest new ones, pointed out in (Bryman and Bell 2015). The purpose of the research questions is to gain better understanding of the research problem statement and finding an optimal solution to it. The research questions below are the final research questions for this study, and they differ a bit from the research questions that initially outlined during the proposal paper.

The overall problem statement for this master`s thesis is:

Optimizing the problem of the safety system design, considering the set of safety measures inherent in SIS and the approach to the SIS maintenance through workforce scheduling for formulating straightforward requirements that could be a starting point for the detailed engineering design of SIS.

For this, the following research questions are made in understanding the stated problem and its solutions:

- Research Question (RQ) [Part1]: Safety Systems

RQ1.1: What are the recommendations to the requirement specifications for the design of safety systems?

- Research Question (RQ) [Part2]. Maintenance

RQ2.1: How important is maintenance of SIS to operations on the remotely located O&G facilities?

RQ2.2: What are the required maintenance frequencies of SIS in the remotely located O&G facilities?

RQ2.3: How to establish the staffing size and determine the crew schedules, considering the transportation to and from the remotely located O&G facilities?

- Research Question (RQ) [Part3]. Solutions

RQ3.1: What can be done to improve the safety of operations on the O&G facilities that located in poorly accessible regions?

RQ3.2: What can be the future research for this topic that can provide better solutions?

3.3 Problem analysis and data collection

The research mainly includes quantitative methods and algorithms with a goal to address the problem of SIS design and maintenance modelling to optimize the set of safety measures in the SIS and simultaneously determines the number of maintenance personnel and their working schedules. Thus, the modelling in this research is to ensure the safety of operations by simultaneously evaluating the decisions on the safety system`s components and structures, the facility maintenance frequencies, the staffing size of maintenance personnel and transportation of staff, as well as the schedules of their work shift. Thereby, the details of the SIS functioning and maintenance are merged into a Markov model used for safety quantification. Besides, a black-box optimization algorithm used for the decision-making process. In addition, the objective function defined in this research is to address the economic perspective on the lifecycle of the technological solution. In other words, the purpose of the cost-minimization objective is to explore a trade-off between the capital investments into the complexity of the safety system as well as the operational expenditures associated with the system maintenance and the expected losses in case of the incidence of hazardous events. Altogether, this research will contribute to the area of engineering design by addressing the issues of SIS design and their maintenance for the remotely located process facilities. Overall, the purpose of the research is to answer the research questions and find a solution to the main problem statement. For this purpose, it requires to collect the necessary data for the computational experiment. The data adopts from a real project implemented by a Russian company (Rosneft). Another point worth noting is this study is based on the research by Redutskiy (2017a). The objectives and models for this research on the one hand is case specific. On the other hand, the solution methods and models that are used in this research can be transferable to other process industries, considering the safety system problems.

3.4 Research area

3.4.1 Spurious trip

Referring to 2.4.6, dangerous failures lead to hazardous consequences, while safe failures result in spurious activation without causing any hazards. For the complex SIS, it is difficult to reveal all hardware failures perfectly either by diagnostic test or proof tests. Theoretically, the dangerous undetected failures must be revealed by means of proof tests rather than safe ones. Then the safe failures remain undetected and cannot be eliminated, but they exist in the system through the entire system lifecycle. This results in spurious trip of SIS at any time. Once the spurious trip of SIS revealed, it must be repaired. The time used for the repair is called the mean repair time (MRT), according to the standard IEC 61508 (2010). The PDS method defines the spurious trip as "a spurious activation of a single SIS element or of a SIF (Sintef 2006).

3.4.2 Common Cause Failure

Common Cause Failure (CCF) is a great treat to SIS reliability, which may lead to simultaneous failures of redundant components and safety barriers (Lundteigen and Rausand 2007). In addition, redundancy is often introduced to improve the reliability of SISs, but CCF may violate the intended reliability gain (Rahimi and Rausand 2013). Despite of substantial amount of research, there is no an accepted common definition of CCF. The authors regarding their application area usually interpret the term. Referring to SIS, there is a definition of CCF given in the standard IEC61511 (2003), as a "*CFF is a failure which is the result of one or more events, causing failures of two or more separate channels in a channel system, leading to a system failure."* A channel is a single redundant path within a SIF, and it also can be a single SIF in case more than one SIF is required to obtain the necessary risk reduction (Lundteigen and Rausand 2007). In other words, a CCF is a result of an event that affects simultaneously several or all components of a redundant system, resulting in loss of the required function, i.e. SIS fails to function when a demand occurs (Innal, Lundteigen, et al. 2016). Therefore, the standards IEC 61508 and IEC 61511 require that the effect of CCF must be considered in reliability calculations, and the standard IEC61508 recommends for SIS using the beta-factor model, where β is the conditional probability of a CCF when a failure has occurred (Rausand and Høyland 2004). According to the beta-factor model, the total failure rate of a component $\lambda^T$is the sum of independent failures (λ^I) and CCFs (λ^C), which can be expressed as following (Mechri, Simon and Ben Othman 2015):

$$\textbf{\textit{(1)}} \quad \lambda^T = \lambda^I + \lambda^C = (1-\beta)\lambda^T + \beta\lambda^T$$

Where β is the failure probability due to a common cause given the occurrence of a failure (Lundteigen and Rausand 2007). As described in (Innal, Lundteigen, et al. 2016) β represents the ratio of CCFs (λ^C), thus, the expression of β is given as following (Mechri, Simon and Ben Othman 2015):

$$\textbf{\textit{(2)}} \quad \beta = \frac{\lambda^C}{\lambda^C+\lambda^I} = \frac{\lambda^C}{\lambda^T}$$

Further, applying this β equation into the total failure rate equation, thus the detected and undetected failure modes are divided into the independent failures and common cause failures. Thereby, the final CCF quantification expresses as following (Mechri, Simon and Ben Othman 2015):

$$\textbf{\textit{(3)}} \quad \lambda^T = \lambda_{DD}^I + \lambda_{DD}^C + \lambda_{DU}^I + \lambda_{DU}^C + \lambda_{SD}^I + \lambda_{SD}^C + \lambda_{SU}^I + \lambda_{SU}^C$$

Considering only the dangerous failure of the components, the various rates of the detected and undetected dangerous failures express as follows (Mechri, Simon and Ben Othman 2015):

$$\textbf{\textit{(4)}} \quad \begin{cases} \lambda_{DD}^I = (1-\beta_D)\lambda_{DD} = (1-\beta_D)DC\lambda_D \\ \lambda_{DD}^C = \beta_D\lambda_{DD} = \beta_D DC\lambda_D \\ \lambda_{DU}^I = (1-\beta_U)\lambda_{DU} = (1-\beta_U)(1-DC)\lambda_D \\ \lambda_{DU}^C = \beta_U\lambda_{DU} = \beta_U(1-DC)\lambda_D \end{cases}$$

Here, the factors β_D and β_U respectively represent the proportion of detected and undetected CCFs related to the DC rate (Langeron, et al. 2008). This is because safe failures do not have any effect on the ability of the SIS to perform its functions, while dangerous failures may prevent the SIS from performing on demand (Mechri, Simon and Ben Othman 2015). The frequency and quality of maintenance may lead to CCF and therefore affect the beta-factor, e.g., a SIS element with low inherent reliability will fail rather often and will require frequent maintenance, which may cause CCFs (Rahimi and Rausand 2013). With reference to (A. C. Torres-Echeverria 2009), the Common Cause Failure (CCF) is an important factor. The author proposes the following formulas to calculate the CCF and the independent failures, noted as “normal”.

$$\textbf{\textit{(5)}} \quad \lambda^{CCF} = \beta \cdot \lambda^T$$

(6) $\lambda^{Normal} = (1 - \beta) \cdot \lambda^{T}$

Moreover, an extended version of this beta -factor model is developed and called as the PDS method that is often used in the Norwegian oil and gas industry (Sintef 2006). The PDS method is used to quantify unavailability and loss of production for SISs, and it accounts all types of failure categories, e.g. technical, software, human, etc. (Hauge, Lundteigen and Hokstad, et al. 2010). In general, the oil and gas industry are directing on CCF in the design phase of the SIS (Lundteigen and Rausand 2007).

3.4.3 Probability of Failure on Demand (PFD)

The probability of failure on demand (PFD) is "*a value that indicates the probability of a system failing to respond to a demand*". The average probability of a system failing to respond to a demand in a specified time interval is noted as PFDavg. Then, the PFD equals to 1 minus Safety Availability (i.e. safety unavailability). The Safety Availability is "*fraction of time that a safety system is able to perform its designated safety service when the process is operating"* (ISA 1997).

The Average Probability of Dangerous Failure on Demand (PFDavg) is a probabilistic measure to SIL based on how often the SIS is required to respond to hazardous events (IEC 61508 2010). In other words, the PFDavg is the safety unavailability of the system that affects its ability to react to hazards (Mechri, Simon and Ben Othman 2015) & (Torres-Echeverria, Martorell and Thompson 2012). This measure applies when the SIS needs to respond on the average every year or less and usually used for low-demand mode.

The standard IEC61508 (1998) recommends analytical formulas for the PFDavg that are tailor-made for selected configurations. And the quantification of the PDF value considers several parameters such as system configuration and architecture, failure rates, proof test intervals, repair and restoration times, and common cause failures. The PFDavg calculation is based on random hardware failures (Mechri, Simon and Ben Othman 2015), as expressed by a constant failure rate λ, and not all failures are equally important and relevant for the quantification (Innal, Lundteigen, et al. 2016).

As mentioned in (Mechri, Simon and Ben Othman 2015), (Torres-Echeverria, Martorell and Thompson 2012), (Dutuit, et al. 2008), and (Goble and Brombacher 1999), the PFDavg calculation must be obtained by quantitative methods, and this calculation must be connected with the computation of the safety function unavailability on demand. The SIS performance qualification, i.e. PFDavg is usually obtained by reference to the standard IEC61508 (1998), a target range of PFDavg is allocated to each of the four SILs. It is necessary to evaluate how the reliability of system can be improved if the calculated PFDavg is above the target range of specified SIL requirements (Innal, Lundteigen, et al. 2016).

3.4.4 Reliability Block Diagram (RBD)

Reliability Block Diagram (RBD) is a method that illustrates simple structures and is used for system reliability quantification, and moreover, it represents the logical relationship between the components for successful functioning of the system, e.g. each square block represents one component (A. C. Torres-Echeverria 2009). According to Rausand and Høyland (2004), a reliability block diagram is a success-oriented network describing the function of the system, i.e., it shows the logical connections of components needed to fulfill a specified system function. If the system has more than one function, each function must be considered individually, and a separate reliability block diagram must be established for each system function. For instance, Figure 12 illustrates the three basic system structures with three components as RBDs.

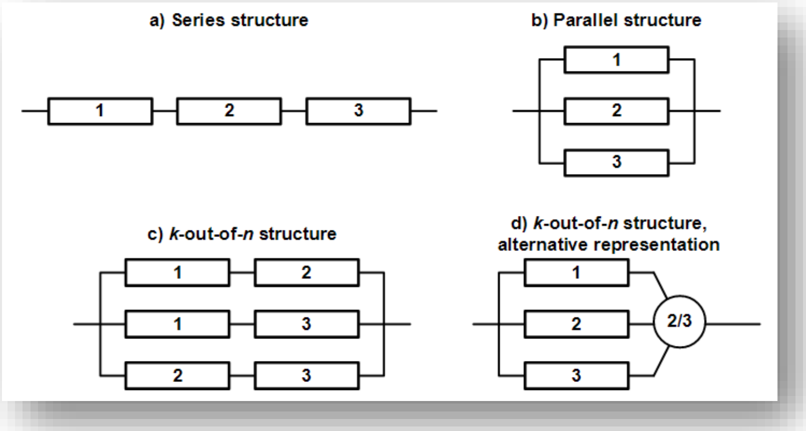

a) Series structure
1
2
3
b) Parallel structure
1
2
3
c) *k*-out-of-*n* structure
1
2
1
3
2
3
d) *k*-out-of-*n* structure, alternative representation
1
2
3
2/3

Figure 12: Basic system structures, RBDs Source: [(A. C. Torres-Echeverria 2009)]

In the work (Catelani, Ciani and Luongo 2010), the RBD methodology is proposed and applied to SIS designed for Steam turbine, oil and gas application, computing the PFD_{avg} in order to clarify the safety aspects for both operators and technicians. And, the authors concluded that RBD models are intuitive and easy to create i.e. RBD shows system decomposition in blocks easy to study, and thus it can help the technicians especially in case of complex systems.

3.4.5 Markov Method

Markov Analyses (MA) is one of modeling approaches that mentioned in IEC 61511 (2003), as a holistic approach often used in dependability studies when one wants to model a repairable system with components at constant failure and restoration rates (Liu and Rausand 2011). According to Mechri, et.al. (2013), Markov models are probably the most relevant model to consider the different events such as failure, proof test, failure rate, common cause failure. Markov model is well suitable if the SIS is periodically tested and in low-demand mode. Markov model is used to compute SIS performance whatever is the demand mode (Jin, Lundteigen and Rausand 2011). However, the main advantage of Markov model is to be more accurate and flexible according to the specific feature of each mode (Chen 2011).

For instance, the Markov model applied in (Mechri, Simon and Ben Othman 2015) to calculate the performance of safety systems (PFDavg) that operating in low-demand mode to integrate the proof tests. The proof tests are carried out for at regular intervals to reveal hidden failures (Rahimi and Rausand 2013). Further, the Markov chains are interesting formal models that requires identifying the different states (Liu and Rausand 2011) where a SIS and its characteristic parameters can take, e.g., it is possible to model different failure modes of the components, test strategies, repair operation, diagnostic coverage and CCF. However, the explosion of the state numbers strictly limits this method due to that the modeling process involves the enumeration of all accessible states and all transitions between these states (Mechri, Simon and Ben Othman 2015).

Moreover, Markov chains models are usually used for some dynamic effects associated with tests and maintenances. This approach is applied in (Redutskiy 2017a) for modeling the performance of SIS to account for device failures occurrence and repairs, the occurrence of technological incidents, and execution of facility maintenance work over the lifecycle of a hazardous facility.

3.4.6 Asset Management

3.4.6.1 Maintenance for safety systems

Maintenance is an action that combines all technical and administrative considerations in order to retain a system or to restore it to a state in which the system can perform its required functions (Dekker 1996). With this, the maintenance process takes in preventive and corrective actions carried out to maintain a system to its operating condition (Nguyen, Do and Grall 2015). Thereby, the objectives of maintenance are multiple as for ensuring the system function (i.e. availability, efficiency, and product quality), and ensuring the system life (i.e. asset management) and ensuring the safety of the system as well as safeguarding human life (Dekker 1996). The availability of a complex system often is strongly associated with the components reliability and maintenance policy, and the maintenance policy has influences both on the components repair time and reliability affecting the system degradation and availability (Frangopoulos and Dimopoulos 2004). Thus, optimal maintenance policies proposed to provide optimal system reliability, availability, and safety performance at the lowest possible maintenance cost (Nguyen, Do and Grall 2015).

According to Eti, et.al. (2007), maintenance can gain much from improving the work processes involved in maintenance functions by integrating the maintenance requirements into the planning and decision-making stages. More precisely, if there is a wise consideration of reliability, availability, maintainability, and supportability (RAMS) and risk in maintenance planning, policy decision making to the maintenance requirements of safety system, then the frequency of failures and their consequences can be reduced significantly, and considerable savings can be made in the operation processes.

However, to improve the reliability of the system, the reliability improvement measure is used to identify the importance ranking of components relating to the improvement ability on the system reliability. This importance measure does not consider the maintenance cost (Rausand and Høyland 2004). Therefore, an extension of this importance measure as “cost-based group improvement factor" for group-based maintenance decision-making proposed by (Nguyen, Do and Grall 2015) .

In addition, reliability centered maintenance (RCM) is a method that can be applied to define maintenance policy in order to assurance the system operational performance, mentioned by Modarres (1993) and Kahn and Haddara (2004). The RCM provides a standard, common methodology for assessing, ranking, and evaluating the effectiveness of any maintenance procedure, and it also brings structure and order into the strategy, which provides a resource map that identifies the roles played by the various working groups (Eti, Ogaji and Probert 2007). According to (Dekker 1996), RCM is a more qualitative approach to maintenance, and it directs maintenance efforts at those parts and units where reliability is critical. The maintenance optimization models are the quantitative approach.

3.4.6.2 Maintenance optimization models

Maintenance optimization is a method to determine the most effective and efficient maintenance plan, considering inspection time and frequency, work preparation, required maintenance resources. The best possible balance can be achieved between direct maintenance costs, e.g., labor cost, transportation costs, and the consequences of not performing maintenance as loss of production and assets (Shafiee and Sørensen 2017). In (Dekker 1996), the author defined maintenance optimization models as mathematical models that is used to find the optimum balance between the costs and benefits of maintenance, while taking all kinds of constraint into consideration. Mostly, maintenance benefits consist of savings on costs i.e. less failure costs.

In (Nguyen, Do and Grall 2015) mentioned that there are mainly two types of maintenance technique such as (1) time-based maintenance (TBM) and (2) condition-based maintenance (CBM). The TBM is about preventive maintenance decision based on the system age and all information on the system lifetime (Dekker, Wildeman and van der Duyn Schouten 1997), while CBM is a maintenance decision making process, which relies on diagnostic of the system condition over time (Bouvard, et al. 2011). For instance, Tian et al., (2012) developed a multi-objective CBM approach to deal with the multi-objective CBM optimization problem considering system cost and reliability. This optimization approach thoroughly explores the tradeoff between the optimization objectives, and it provides an optimal solution that responds to the decision maker`s preference (Alaswad and Xiang 2017). In CBM optimization, there are multiple and conflicting design objectives that can be as minimizing the maintenance costs, maximizing the reliability, minimizing equipment downtime, etc. (Tian, Lin and Wu 2012).

Furthermore, there is a bi-objective optimal inspection and maintenance planning approach proposed by (Barone and Frangopol 2013) for structural systems with a purpose to minimize both system failure rate and expected total cost, and further the authors considered several multi-objective optimization problems for determining maintenance schedules for deteriorating structures. And for each optimization problem the minimizing total cost is considered as first objective, and as second objective might be as following, e.g. system reliability, availability, risk, and hazard function. Moreover, an overview on time-based and condition-based maintenance in industrial applications with the most recent condition monitoring techniques, are presented in (Ahmad and Kamaruddin 2012). In fact, safety systems have many redundancies and components with great number of combination and alignment alternatives among them. Therefore, it needs other approaches that can deal with such complexities.

3.4.6.3 Workforce Scheduling and Routing Problem (WSRP)

Regarding the oil and gas facilities remotely located, one of the arisen problems is workforce scheduling, crews need to be carried out the maintenance at locations far from the coast or the central location, hence requiring some form of transportation. With reference to (Castillo-Salazar, Landa-Silva and Qu 2016), the workforce scheduling and routing problem (WSRP) considers any environment where it does need a skilled workforce should be scheduled to performing a set of activities distributed over geographically different locations and the activities must be performed within a given time window, assuming the time window for each activity is usually determined by the recipient of the job.

It can be studied as a part of the vehicle routing problem with time windows (VRPTW), which has the main objective to minimizing the total travel distance (Desrochers, Desrosiers and Solomon 1992). This can be associated with the performing maintenance to several installations spread across many locations and each installation specifies a time window (i.e. time for performing a task at a operators premises) when the maintenance takes place.

Another point regarding to VRPTW is “a depot”. This can be the location where the staff are sent out and come back (i.e. same starting and ending location).

Besides this, an extended version of VRPTW is introduced in the work of (Brandao and Mercer 1998) and called as vehicle routing problems with multi-trips, and they address the fact that a worker could perform more than one trip on a day to visit the location. A trip is referred to a series of tasks before going back to the depot (Castillo-Salazar, Landa-Silva and Qu 2016). In addition, regarding time window, an interesting problem “manpower allocation” presented in (Lim, Rodrigues and Song 2004). They address to assigning workers to a set of customer locations to perform the service activities with the objectives to minimizing the number of servicemen used, the total travel distance, the service time, including the waiting time at service points, and simultaneously maximizing the number of tasks assigned. This is relevant to WSRP, especially in this study. Thus, in addition, the transportation must be considered, and assumed that all workforces use the same type of transport considering the cost efficiency.

3.4.7 Optimization Theory

3.4.7.1 Genetic Algorithm (GA) approach

The genetic algorithms (GA) are considered as an evolutionary computation techniques that are very useful for solving complex problems with high dimensional, discrete, non-linear and discontinuous. It has a capacity to handle integer variables (Torres-Echeverria, Martorell and Thompson 2012). In this paper (Gen and Yun 2006) the genetic algorithms applied to find the set of Pareto-optimal solutions for multi-objective supply chain network (SCN) design problem, which means the problem has multiple and conflicting objectives such as cost, service level, resource utilization, etc.

Moreover, GA are able to deal with problems which objective function is not explicit, and it works with an initial population of potential solutions called individuals. Each individual is a potential solution to the optimization problem: a coded representation of one set of decision variables in the decision space. These individuals are evaluated, selected and mated to create new and better ones, which are fed into a new generation, making an iterative process that mimics the natural evolution, thereby each step of the GA is executed by the application of genetic operators (Torres-Echeverria, Martorell and Thompson 2012) in Figure 13.

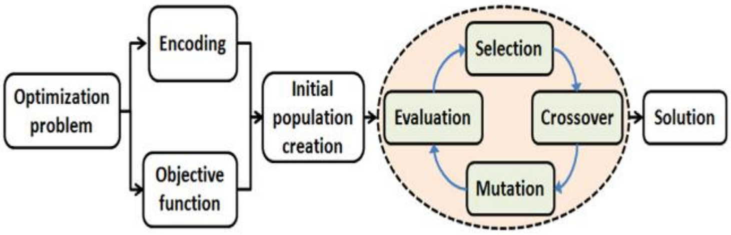


Figure 13: A general structure of GA   Source: [(Innal, Dutuit and Chebila 2015)

Regarding to optimization of SIS design, a comprehensive overview of work related to MooN optimization using GA is presented in (Torres-Echeverria, Martorell and Thompson 2012), and the authors developed a very interesting SIS optimization procedure that considers many aspects such as PFDavg, STR, SIS reconfiguration during proof-tests, different tests strategies and life cycle costs. According to the studies in the field of SIS in many articles, GA have been developed and coded in MATLAB software to solving different optimization problems. Genetic Algorithms are an evolutionary computation technique, which provide the decision maker a pool of good optimal solutions (A. C. Torres-Echeverria 2009).

3.4.7.2 Multi-objective optimization

In this research, the focus is multi-objective optimization, which is an essential part of optimization theory. Multi-objective formulations are realistic models for complex engineering optimization problems. Considering the real-life situations, it might be necessary to formulate the optimization problem with more than one objective function simultaneously (Jahromi and Feizabadi 2017). More often, a single objective with several constraints may not adequately represent the problem and can result in unacceptable results regarding the other objectives (Konak, Coit and Smith 2006).

Thus, a multi-objective optimization is a simultaneous minimization of the different objectives (Innal, Dutuit and Chebila 2015). Nevertheless, it is impossible to obtain a perfect multi-objective solution that simultaneously optimizes each of objective function. Thereby, a reasonable solution to a multi-objective problem is to investigate a set of solutions, each of which satisfies the objectives at an acceptable level without being dominated by any other solution (Konak, Coit and Smith 2006).

By using a multi-objective genetic algorithm allows to identify a set of Pareto optimal solutions in one single run (Deb, et al. 2000), providing the decision maker with the complete spectrum of optimal solutions with respect to the various objectives, thus the decision maker can select the best compromise among these objectives (Giuggioli Busacca, Marsequerra and Zio 2001). More specific, if a solution is not dominated by any other solution in the solution space, it is a Pareto optimal (i.e. non-dominated) solution. Thereby, the set of all feasible non-dominated solutions in the decision space is the Pareto optimal set, thus the corresponding objective function values in the objective space are the Pareto front (Innal, Dutuit and Chebila 2015).

In the modeling of multi-objective problem, the user is need to use optimization toolbox of MATLAB to choose the right solver (e.g. gamultiobj-Multiobjective optimization using genetic algorithm) and call the function to handle related the objective function, which can contain several objectives (e.g. $PFD_{avg}^{SIS}, STR_{SIS}, C_p^{SIS}\ and\ C_T^{SIS}$), referring to the work of (Innal, Dutuit and Chebila 2015).

3.4.7.3 Black box optimization

Research shows that the black box optimization is a useful tool for solving the complex maintenance-optimization problems. In the recent years, the black-box complexity theory produced several very fast black-box optimization algorithms, according to Doerr et al. (2015), and these black-box algorithms often profit from solutions inferior to the previous best. Black-box complexity is counting the number of queries needed to find the optimum of a problem without having access to an explicit problem description (Doerr, Kotzing, et al. 2013), and it was presented to measure the difficulty of solving an optimization problem through generic search heuristics (Droste, Jansen and Wegener 2006).

In fact, the choice of how to model the optimization problem has a significant influence on its black-box complexity, revealed by Doerr et al. (2013). However, Limbourg and Kochs (2006) mentioned that black box optimizations are problem solving heuristics, which are “intelligently guess” new solutions based on older experiences and some general assumptions. It is often used for optimization of maintenance decisions at componential level because black box optimization model does not consider the relationships between components (Shafiee and Sørensen 2017).

Considering important design problems, there is a need to make some decisions by finding the global optimum of a multi-extremal objective function subject to a set of constraints. Especially in engineering applications, the functions involved in optimization process are black-box with unknown analytical representations and hard to evaluate. This type of problems often cannot be solved by traditional optimization techniques, according to Kvasov and Sergeyev (2015), and the authors developed some powerful deterministic approaches to construct numerical methods for solving practical black-box optimization problems.

4.0 Models for Safety system design and maintenance

An important part of this research is to develop mathematical model for solving the SIS design and maintenance optimization problems. This section presents the mathematical structure and description of the models that are constructed for this study.

4.1 General Model: SIS design and maintenance planning

This section is based on (Redutskiy 2017a). The generalized model in this paper is used as a base model contained in this study.

4.2 Modelling assumptions

In the case of oil and gas facilities, one of the most important aspects may be maintenance of the safety systems to ensure a smooth operation, in relation to the economic perspective of the plant. The functions of the safety systems are aimed at reducing the risk of dangerous events. In some cases, the automatic instrumentation systems may fail due to technical errors that may result in the shutdown of the entire process. To prevent such situations from occurring, maintenance is required either continuously or periodically. At the processing facility, crews of technicians must stay in shift to monitor the operation and perform the necessary maintenance due to the given maintenance policy. In the case of remote locations, the crews will travel to and from the facility, for that reason they must have a work schedule that includes both daily work and rest time in addition to the travel frequency.

In addition, the following assumptions are considered for this modelling:

- Only random hardware failures are considered
- Regarding the failure classification presented in 2.4.6, a spurious trip causes shutdown in the technology and all safe failures are detected
- Technology is shut down for a repair in case a detected failure (DD or ST) occurs
- The occurrence of failures, incidents, repairs of devices, and technology restorations will be modelled as exponentially distributed with constant failure rate
- Proof tests are considered, i.e. periodic maintenance: As a result, all unseen failed devices are restored

The common terms used for the different failures are given in Table 3.

Table 3: Notations for failure classification Source: [(Redutskiy 2017a)]

Notation	**Description**
Failure modes (used in superscript)	
DF	Dangerous Failure
DD	Dangerous Detected Failure
DU	Dangerous Undetected Failure
RF	Random Hardware Failure
ST	Spurious Trip
Notations for the general reliability categories	
$\boldsymbol{\lambda}$	failure rate
$\boldsymbol{p}$	probability of failure

4.3 Problem setting

The ***decision variables*** of the problem of SIS design and maintenance planning optimization includes the following:

- Device models of transmitters, logic solvers, and final control elements from the databases of alternatives

- Redundancy architectures for each subsystem, considering MooN architectures where N is the total number of identical devices in the subsystem, and M is the number of devices needed to be in the operating condition so that the subsystem's intended function could be performed
- Additional electric separation of devices within each subsystem to ensure that all the subsystems do not fail at the same time with a common cause
- Proof tests, i.e. the periodic maintenance frequency, with test interval (TI) between two consecutive overhauls
- Maintenance policy, a decision for performing the maintenance either sequential or parallel
- Staff size, i.e. the number of workers required to work at any point in time to conduct either the continuous maintenance or a periodic overhaul (i.e. proof tests)
- Workforce schedule, a predefined working schedule including start date, work duration, etc. for the crews

The following ***objectives*** are measured in this modelling:

- Average probability of failure on demand (PFD_{avg}) represents the mechanisms of failures and incidents occurrence
- Mean downtime of the technological facility (DT) presents the expected value of the technological facility being in the shutdown state, more specific instrumentation failures and spurious trips contribute to the downtime, and so do the technological incidents
- Lifecycle cost of the ESD system installed at a processing facility

4.4 Mathematical formulation

The generalized mathematical formulation of the SIS design and maintenance planning problem is presented in this section.

4.4.1 Lifecycle modelling

This modelling is continuing the general model presented in 4.1, with a focus on workforce scheduling for shift work to conduct the maintenance at the remotely located oil and gas processing facility. The lifecycle cost is evaluated, and personnel levels are estimated by Markov model. In addition, the workforce scheduling is modelled as a set-covering problem considering the company's reward system for the shift durations and working hours.

First, the notations used for the modelling of the SIS design and maintenance planning optimization problem, followed by the formulations of objective functions, variables, and constraints below.

Table 4: Notations for the SIS design and LC modelling

Notation	Description
$\boldsymbol{q}$	index of subsystems of the SIS
	$q = 1$ corresponds to sensors
	$q = 2$ corresponds to logic solver
	$q = 3$ corresponds to final control elements
$\boldsymbol{l}$	index of device models
$\boldsymbol{r}$	index of redundancy
$\boldsymbol{w}$	index of weeks in the technological solution's operations timespan
$\boldsymbol{s}$	index of possible trips for works travelling to the facility
$\boldsymbol{c}$	index of daily shift work alternatives
$\boldsymbol{S_q^{inst}}$	set of device model alternatives for instrumentation subsystem q
$\boldsymbol{S_q^{red}}$	set of redundancy alternatives for instrumentation
$\boldsymbol{S^{TRIP}}$	set of all possible trips, considering all trip durations, and starting times
$\boldsymbol{S^{DS}}$	set of all daily shifts: daily work and rest schedule for each worker for trips
	Decision variables
$\boldsymbol{x_{lq}^{inst}}$	binary decision variable: equals 1, if device model l is chosen for subsystem q; 0, otherwise
$\boldsymbol{x_{rq}^{red}}$	binary decision variable: equals 1, if redundancy option r is chosen for subsystem q; 0, otherwise
$\boldsymbol{x_q^{sep}}$	binary decision variable: equals 1, if additional electrical/physical separation is introduced for subsystem q; 0, otherwise
$\boldsymbol{x_s^{WFT}}$	integer variable: # of crews taking the s^{th} trip to a facility (for each s^{th} trip, the duration of the trip and the starting time is specified
$\boldsymbol{x_{sc}^{WFS}}$	binary variable: equals 1, if workers taking the s^{th} trip are to work under the c^{th} daily schedule
$\boldsymbol{x_w^{required}}$	integer variable: the required # of workers at the facility during week w
$\boldsymbol{TI}$	integer variable: time between two consecutive proof tests, [weeks]

$\boldsymbol{x_q^{MP}}$	binary variable: maintenance policy for the q^{th} subsystem
	Parameters and Functions
$\boldsymbol{PFD_{avg}}$	average probability of failure on demand
$\boldsymbol{DT}$	facility downtime
$\boldsymbol{C_{lifecycle}}$	lifecycle cost of the solution
$\boldsymbol{SIL}$	safety integrity level determined for a particular SIS configuration, as demonstrated in Table 1 (SIL defined in IEC 61508 and IEC 61511)
$\boldsymbol{SIL^{REQ}}$	the necessary target SIL prescribed by governmental regulations on safety
$\boldsymbol{\sigma_{ws}}$	binary parameter indicating whether week w is covered by the trip option s or not

The objective functions:

$$minPFD_{avg}\left(X^{inst},X^{red},X^{sep},X^{WF},X^{MP},TI\right) \tag{4.1}$$

$$minDT(X^{inst},X^{red},X^{sep},X^{WF},X^{MP},TI),$$

$$minC_{lifecycle}\left(X^{inst},X^{red},X^{sep},X^{WF},X^{MP},TI\right).$$

Decision variables:

$$X^{inst}=\left\{x_{lq}^{inst}\right\},\ X^{red}=\left\{x_{rq}^{red}\right\},\ \ X^{sep}=\left\{x_q^{sep}\right\}, \tag{4.2}$$

$$X^{WF}=\{x_s^{WFT},x_{sc}^{WFS}\}$$

Constraints for the requirements:

$$SIL\left(X^{inst},X^{red},X^{sep},X^{WF},X^{MP},TI\right)=SIL^{REQ}, \tag{4.3}$$

Constraints for subsystem:

$$\sum_{l \in S_q^{inst}} x_{lq}^{inst} = 1, \qquad \forall q, \tag{4.4}$$

$$\sum_{r \in S_q^{red}} x_{rq}^{red} = 1, \qquad \forall q, \tag{4.5}$$

Constraints for workforce scheduling:

$$\sum_{s \in S^{TRIP}} \sigma_{ws} \cdot x_s^{WFT} \geq x_w^{required}, \qquad \forall w, \tag{4.6}$$

$$\sum_{c \in S^{DS}} x_{sc}^{WFS} = 1, \qquad \forall s. \tag{4.7}$$

In oil and gas industry, regarding the standards IEC 61508 and IEC 61511, the designed technological solutions are expected to maintain the safety integrity level, especially for a hazardous process the run on the facility. Thus, this is expressed in the constraint (4.3). The constraints (4.4) and (4.5) restrict that only one option for the selection of device model and a redundancy architecture for a subsystem.

The constraint (4.6) expresses that the number of workers required to be available at the facility at any time (w) to perform the maintenance, should be covered by a sufficient number of crews taking certain (s^{th})trips. The last constraint (4.7) ensures that only one daily shift schedule should be chosen for every trip taken by a crew (either 8 hours shift or 12 hours shift, given in Table 12).

4.4.2 Markov Model: Modelling a subsystem

In addition, the dangerous and safe failures of components of any subsystem are modeled for the time interval TI (i.e. test interval) that referred to a period between two consecutive proof tests: [0, TI]. And the failures in a subsystem with MooN architectures include (N-M+2) states described by Markov model, as illustrated in the following Figure 14.

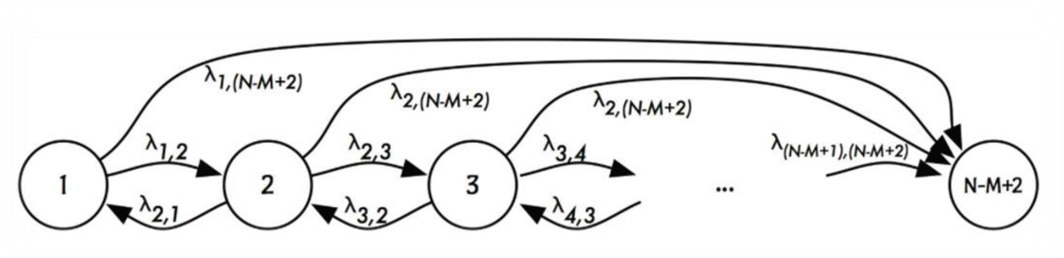


Figure 14: Markov process of failures and repairs Source: [(Redutskiy 2017a)]

Furthermore, state is the operating state for all N components, while state 2 and all further states represent failure of one component each. Thus, the entire subsystem fails to perform when (N-M+1) components fail which corresponds to the end state on the graph. Occurrence of independent failures and repairs is depicted by consecutive transitions between the states, e.g. $\lambda_{1,2}$ presents the failure, while $\lambda_{2,1}$ is corresponding repair. Additionally, the common cause failure (CCF) occurrence is depicted by direct transitions from any state to the end state.

Assumption: the occurrence of device failures, incidents and repairs is stochastic and modelled in the framework of reliability theory. Thus, the exponential distribution for the probability of failure occurrence, which corresponds to constant failure rate, is demonstrated by the following formula (Redutskiy 2017a):

$$p(t) = 1 - e^{-\lambda \cdot t} \tag{4.8}$$

The mathematical formulation of the modelling a subsystem is divided into three sections regarding the different modes of failure (i.e. outputs).

Table 5: Notations used in the modelling a subsystem

Notations	Description
	Indices, parameters, and functions
$\boldsymbol{i, j}$	indices of Markov model states
$\boldsymbol{TI}$	test interval, the time period between proof tests, [h]
$\boldsymbol{N}$	total number of components in MooN architecture
$\boldsymbol{p_j^{DU}(t)}$	the probability of $(j-1)$ dangerous undetected failures in a subsystem
$\boldsymbol{p_j^{DD}(t)}$	the probability of $(j-1)$ dangerous detected failures in a subsystem
$\boldsymbol{p_j^{ST}(t)}$	the probability of $(j-1)$ spurious trips in a subsystem
$\boldsymbol{t}$	time, [h]
$\boldsymbol{M}$	the necessary number of operating devices in MooN redundancy scheme
$\boldsymbol{\lambda_{i,j}^{DU}}$	transition rate (from state i to state j)
$\boldsymbol{\lambda_{i,j}^{DD}}$	transition rates for the model of dangerous detected failure occurrence
$\boldsymbol{\lambda_{i,j}^{ST}}$	transition rates for the model of spurious trips
$\boldsymbol{\beta}$	common cause failure factor, a fraction
$\boldsymbol{\lambda}$	the dangerous failure rate for one component, $[h^{-1}]$
$\boldsymbol{\varepsilon}$	diagnostic coverage, a fraction
$\boldsymbol{\mu}$	repair rate for one component, $[h^{-1}]$
	Output of the model
$\boldsymbol{\lambda^{DU}}$	the dangerous undetected failure rate for the subsystem
$\boldsymbol{\lambda^{DD}}$	the dangerous detected failure rate for the subsystem
$\boldsymbol{\lambda^{ST}}$	spurious tripping rate for the subsystems

4.4.2.1 Markov model of dangerous undetected failures in a subsystem:

$$\left(\frac{dp_j^{DU}}{dt}\right) = \sum_{i=1}^{N-M+2} p_i^{DU}(t) \cdot \lambda_{i,j}^{DU}, \quad j \in \{1, \dots, (N-M+2)\}, \tag{4.9}$$

$$\lambda_{i,i}^{DU} = -\lambda \cdot (1-\varepsilon) \cdot [(N-j+1) \cdot (1-\beta) + \beta], \tag{4.10}$$

$$\lambda_{i,i+1}^{DU} = (N-j+1) \cdot (1-\varepsilon) \cdot (1-\beta) \cdot \lambda,$$

$$\lambda_{i,(N-M+2)}^{DU} = (1-\varepsilon) \cdot \beta \cdot \lambda,$$

$$i \in \{1, \dots, (N-M+2)\},$$

$$p_1^{DU}(0) = 1, \qquad p_i^{DU}(0) = 0, \tag{4.11}$$
$$i \in \{2, \dots, (N - M + 2)\},$$

$$\boldsymbol{\lambda^{DU}} = -\frac{\mathbf{lo\ g}\left(\mathbf{1} - \boldsymbol{p_{N-M+2}^{DU}(TI)}\right)}{\boldsymbol{TI}}. \tag{4.12}$$

4.4.2.2 Markov model of dangerous detected failures in a subsystem:

$$\left(\frac{dp_j^{DD}}{dt}\right) = \sum_{i=1}^{N-M+2} p_i^{DD}(t) \cdot \lambda_{i,j}^{DD}, \quad j \in \{1, \dots, (N - M + 2)\}, \tag{4.13}$$
$$\lambda_{1,1}^{DD} = -\varepsilon \cdot \lambda \cdot [N \cdot (1 - \beta) - \beta],$$
$$\lambda_{1,2}^{DD} = N \cdot \varepsilon \cdot \lambda \cdot (1 - \beta),$$
$$\lambda_{1,N-M+2}^{DD} = \varepsilon \cdot \beta \cdot \lambda,$$
$$\lambda_{i,(i-1)}^{DD} = (i - 1) \cdot \mu,$$

$$\lambda_{i,i}^{DD} = -\varepsilon \cdot \lambda \cdot [(N - j + 1) \cdot (1 - \beta) + \beta] - (i - 1) \cdot \mu, \tag{4.14}$$
$$\lambda_{i,i+1}^{DD} = (N - j + 1) \cdot \varepsilon \cdot (1 - \beta) \cdot \lambda,$$
$$\lambda_{i,(N-M+2)}^{DD} = \varepsilon \cdot \beta \cdot \lambda,$$
$$i \in \{2, \dots, (N - M + 2)\},$$

$$p_1^{DD}(0) = 1, \qquad p_i^{DD}(0) = 0, \tag{4.15}$$
$$i \in \{2, \dots, (N - M + 2)\},$$

$$\boldsymbol{\lambda^{DD}} = -\frac{\mathbf{lo\,g}\left(\mathbf{1}-\boldsymbol{p^{DD}_{N-M+2}}(\boldsymbol{TI})\right)}{\boldsymbol{TI}}. \tag{4.16}$$

4.4.2.3 Markov model of spurious trips in a subsystem:

$$\left(\frac{dp^{ST}_j}{dt}\right) = \sum_{i=1}^{N-M+2} p^{ST}_i(t) \cdot \lambda^{ST}_{i,j}, \qquad j \in \{1, \dots, (N-M+2)\}, \tag{4.17}$$

$$\lambda^{ST}_{1,1} = -\lambda^S \cdot [N \cdot (1-\beta) - \beta],$$

$$\lambda^{ST}_{1,2} = N \cdot (1-\beta) \cdot \lambda^S,$$

$$\lambda^{ST}_{1,N-M+2} = \beta \cdot \lambda^S,$$

$$\lambda^{ST}_{i,(i-1)} = (i-1) \cdot \mu,$$

$$\lambda^{ST}_{i,i} = -\lambda^S \cdot [(N-j+1) \cdot (1-\beta) + \beta] - (i-1) \cdot \mu, \tag{4.18}$$

$$\lambda^{ST}_{i,i+1} = (N-j+1) \cdot (1-\beta) \cdot \lambda^S,$$

$$\lambda^{ST}_{i,(N-M+2)} = \beta \cdot \lambda^S,$$

$$i \in \{2, \dots, (N-M+2)\},$$

$$p^{ST}_1(0) = 1, \qquad p^{ST}_i(0) = 0, \tag{4.19}$$

$$i \in \{2, \dots, (N-M+2)\},$$

$$\boldsymbol{\lambda^{ST}} = -\frac{\mathbf{lo\,g}\left(\mathbf{1}-\boldsymbol{p^{ST}_{N-M+2}}(\boldsymbol{TI})\right)}{\boldsymbol{TI}}. \tag{4.20}$$

With reference to (Redutskiy 2017a), the mathematical formulations presented in (4.9), (4.13), and (4.17) are for describing for any failure mode, the probability of the subsystem being in a particular Markov state, known as Kolmogorow forward equations. Further, the equations (4.10), (4.14), and (4.18) express the non-zero (failure) transition rates for the three failure modes, and all the rest transition rates equal to zeroes. The starting point of the stochastic process is state 1, which corresponds to the initial distribution of probabilities in the formulations (4.11), (4.15), and (4.19). The probabilities of the stochastic process being in state the last state, (N-M+2) in Figure 14 , is the probability of the dangerous undetected, dangerous detected, and spurious trips failures for the modelled subsystem, thus, given the exponential distribution of failures, the corresponding failure rates can be obtained in the equations (4.12), (4.16), and (4.20).

4.4.3 Markov model for the lifecycle of ESD system

Modelling the lifecycle of ESD system from the safety perspective and as well as the economic perspective is described in this section. The following assumptions are made for the life cycle modeling:

- the subsystem is performing its intended function,
- the subsystem is under overhaul due to a DD failure,
- the subsystem is under overhaul due to a ST,
- the technology is running on the facility,
- the technology is in the DU failure mode,
- the technological incident has occurred.

The incidents, failures, and repairs are modelled during the entire lifecycle of the ESD system. The time horizon for lifecycle modelling is illustrated in the following Figure 15.

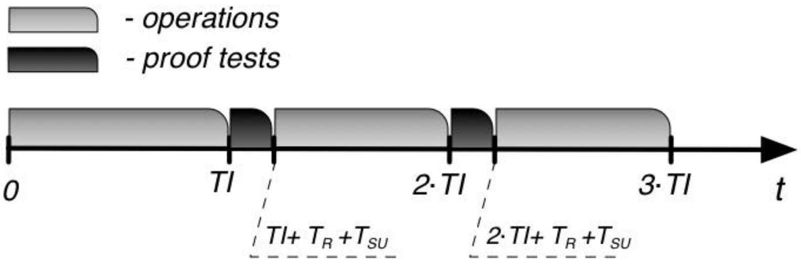


Figure 15: Time horizon for lifecycle modelling   Source: [(Redutskiy 2017a)]

Reference to (Redutskiy 2017a), the occurrence of failures in the three subsystems (PVT, LS, and FCE) and technological incidents (TECH) is displayed in Table 6, and the transition between the 12 states are illustrated in Figure 16.

Table 6: Markov model for the lifecycle of ESD system Source: [(Redutskiy 2017a)]

STATE	*PVT*	*LS*	*FCE*	*TECH*	EXPLANATIONS
1	*up*	*up*	*up*	*up*	Normal course of the process
2	*up*	*up*	*up*	*down*	Safety function performed
3	*O/S*	*up*	*up*	*down*	
4	*up*	*O/S*	*up*	*down*	Overhaul after a ST
5	*up*	*up*	*O/S*	*down*	
6	*O/D*	*up*	*up*	*down*	
7	*up*	*O/D*	*up*	*down*	Overhaul after a DD failure
8	*up*	*up*	*O/D*	*down*	
9	*failure*	*up*	*up*	*up*	
10	*up*	*failure*	*up*	*up*	Undetected failure has occurred
11	*up*	*up*	*failure*	*up*	
12	ESD is shut down, The incident has occurred: failure on demand				

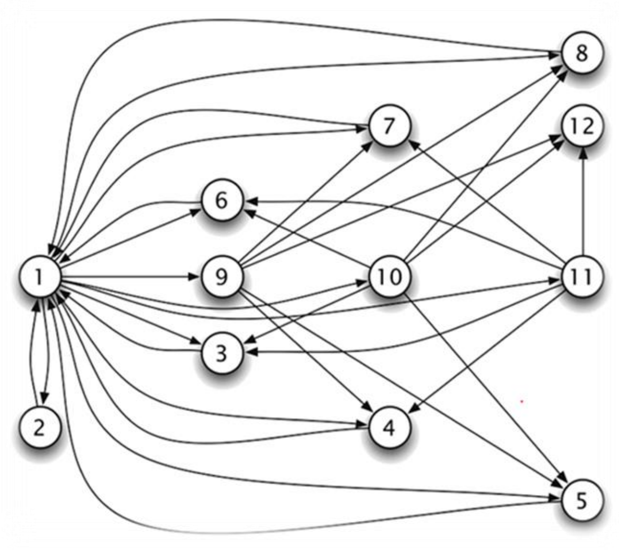


Figure 16: Markov process for the LC of ESD system Source: [(Redutskiy 2017a)]

Mathematical formulations of Markov model for the life cycle of ESD system, considering the safety perspective:

Table 7: Notations for LC modelling from the safety perspective

Notations	Description
	Indices, parameters, and functions
$\boldsymbol{i, j}$	indices of states for Markov model
$\boldsymbol{q}$	index of ESD subsystems
$\boldsymbol{N}$	total number of components in MooN architecture
$\boldsymbol{k}$	index of time periods between the proof tests
$\boldsymbol{p_j(t)}$	the probability of the process being in the j^{th} state
$\boldsymbol{\lambda_{i,j}}$	transition rate from state i to state j, $[h^{-1}]$
$\boldsymbol{t}$	time, [h]
$\boldsymbol{LC_h}$	duration of the lifecycle, [h]
$\boldsymbol{r}$	incidents occurrence rate, $[h^{-1}]$
$\boldsymbol{\mu^t}$	restoration rate for the technology, $[h^{-1}]$
$\boldsymbol{\mu}$	repair rate for one component, $[h^{-1}]$
$\boldsymbol{\lambda_q^{DU}}$	DU failure rate for the q^{th} subsystem, $[h^{-1}]$
$\boldsymbol{\lambda_q^{DD}}$	DD failure rate for the q^{th}subsystem, $[h^{-1}]$
$\boldsymbol{\lambda_q^{ST}}$	ST rate for the q^{th} subsystem, $[h^{-1}]$
$\boldsymbol{\pi_j^k}$	initial condition for the k^{th}time period
$\boldsymbol{T_R}$	repair time necessary for conducting proof tests, $[h]$
$\boldsymbol{T_{SU}}$	start-up time after the shutdown necessary for maintenance
$\boldsymbol{K}$	the lifecycle periods
	Output of the model
$\boldsymbol{PFD_{avg}}$	average probability of failure on demand
$D\boldsymbol{T}$	mean down time of the process, hours

The lifecycle of ESD system is divided in to K periods, which is expressed in the following formulation:

$$K = \left\lceil \frac{LC_h}{TI} \right\rceil, \tag{4.21}$$

The modelling time horizon during each k-th time period:

$$\begin{aligned} t \in [0; TI] &\cup [TI + T_R + T_{SU}; 2 \cdot TI] \\ &\cup [2 \cdot TI + T_R + T_{SU}; 3 \cdot TI] \cup \ldots \\ &\cup [(K-1) \cdot TI + T_R + T_{SU}; K \cdot TI], \end{aligned} \tag{4.22}$$

The probabilities of the Markov process being in each state:

$$\frac{dp_j(t)}{dt} = \sum_{i=1}^{12} p_j(t) \cdot \lambda_{i,j}, \qquad j \in \{1, \ldots, 12\} \tag{4.23}$$

The non-zero transition rates and the remaining rates in the current state, Figure 16:

$$\lambda_{1,1} = -\left(\sum_q \lambda_q^{DU} + \sum_q \lambda_q^{DD} + \sum_q \lambda_q^{ST} \right) \tag{4.24}$$

$$\lambda_{1,2} = r,$$

$$\lambda_{1,3} = \lambda_1^{ST},\ \lambda_{1,4} = \lambda_2^{ST},\ \lambda_{1,5} = \lambda_3^{ST},$$

$$\lambda_{1,6} = \lambda_1^{DD},\ \lambda_{1,7} = \lambda_2^{DD},\ \lambda_{1,8} = \lambda_3^{DD},$$

$$\lambda_{1,9} = \lambda_1^{DU},\ \lambda_{1,10} = \lambda_2^{DU}, \lambda_{1,11} = \lambda_3^{DU},$$

$$\lambda_{2,1} = \mu^t, \lambda_{2,2} = -\mu^t,$$

$$\lambda_{3,1} = \mu,\ \lambda_{3,3} = -\mu, \lambda_{4,1} = \mu, \lambda_{4,4} = -\mu, \lambda_{5,1} = \mu,\ \lambda_{5,5} = -\mu,$$
$$\lambda_{6,1} = \mu,\ \lambda_{6,6} = -\mu,\ \lambda_{7,1} = \mu, \lambda_{7,7} = -\mu, \lambda_{8,1} = \mu,\ \lambda_{8,8} = -\mu,$$

$$\lambda_{9,4} = \lambda_2^{ST}, \qquad \lambda_{9,5} = \lambda_3^{ST}, \qquad \lambda_{9,7} = \lambda_2^{DD}, \qquad \lambda_{9,8} = \lambda_3^{DD},$$
$$\lambda_{9,9} = -(\lambda_2^{ST} + \lambda_3^{ST} + \lambda_2^{DD} + \lambda_3^{DD} + r),$$

$$\lambda_{9,12} = r,\ \lambda_{10,3} = \lambda_1^{ST}, \lambda_{10,5} = \lambda_3^{ST}, \lambda_{10,6} = \lambda_1^{DD}, \lambda_{10,8} = \lambda_3^{DD},$$

$$\lambda_{10,10} = -(\lambda_1^{ST} + \lambda_3^{ST} + \lambda_1^{DD} + \lambda_3^{DD} + r),$$

$$\lambda_{10,12} = r,\ \lambda_{11,3} = \lambda_1^{ST}, \lambda_{11,4} = \lambda_2^{ST}, \lambda_{11,6} = \lambda_1^{DD}, \lambda_{11,7} = \lambda_2^{DD},$$

$$\lambda_{11,11} = -(\lambda_1^{ST} + \lambda_2^{ST} + \lambda_1^{DD} + \lambda_2^{DD} + r),\ \lambda_{11,12} = r,$$

The lifecycle of the system begins, and the process is in the state 1, $k = 1$:

$$\pi_1^1 = 1, \quad \pi_2^1 = 0, \dots \pi_{12}^1 = 0, \tag{4.25}$$

The process continues in the periods $k = 2,3, \dots, K,$:

Assumption: periodically conducted proof tests are considered perfect, i.e. all previously undetected failures become resolved. The probabilities of being in states 2-8 are monotonic over the entire lifecycle of the system, and the remaining probabilities fail to be well behaved at the points of time when proof tests are conducted.

$$\begin{gathered}\pi_1^k = p_1\big((k-1)\cdot TI\big) + p_9\big((k-1)\cdot TI\big) + p_{10}\big((k-1)\cdot TI\big) \\ + p_{11}\big((k-1)\cdot TI\big) + p_{12}\big((k-1)\cdot TI\big), \\ \pi_j^k = p_j\big((k-1)\cdot TI\big), \qquad j \in \{2, \dots, 8\}, \\ \pi_j^k = 0, \quad j \in \ \{2, \dots, K\},\end{gathered} \tag{4.26}$$

The repair time is calculated given the choices of sequential of parallel proof testing policy for each subsystem. The checks and repairs for every subsystem start simultaneously (when the proof tests begin). Knowing the repair time for one device in each subsystem and the maintenance policy for the subsystem, the total repair time that the subsystem requires may be calculated. Finally, we need to choose the subsystem that is being under repair the longest, to obtain the overall proof test duration:

$$T_R = \max\{x_q^{MP} \cdot T_q^{repair} \cdot N_q + (1 - x_q^{MP}) \cdot T_q^{repair},\ \forall q\} \tag{4.27}$$

The purpose of this modelling (4.23)-(4.26) is to obtain the values of $p_1(t) \ldots . p_{12}(t)$, the probability of failures of 12 states, over the entire lifecycle of the system. These values are used to evaluate further the safety indicators such as the average probability of failure on demand (PFDavg), which is the main value of $p_{12}(t)$, and the facility downtime (DT) of the process, obtaining from the probability of the Markov process being in states 2-8. For these indicators the following formulations are used for obtaining the values:

$$PFD_{avg} = \frac{1}{LC_h} \cdot \int_0^{LC_h} PFD_{avg}(t)\, dt = \frac{1}{TI} \cdot \int_0^{TI} p_{12}(t)dt + \\ + \sum_{k=2}^{K} \frac{1}{(TI - T_{SU})} \cdot \int_{(k-1)\cdot TI + T_{SU}}^{k \cdot TI} p_{12}(t)dt, \tag{4.28}$$

$$DT = \sum_{j=2}^{8} \left[\int_0^{TI} p_j(t)\, dt + \sum_{k=2}^{K} \int_{(k-1)\cdot TI + T_{SU}}^{k \cdot TI} p_j(t)dt \right]. \tag{4.29}$$

4.4.4 Modelling for the staffing size requirements

In this modelling, the purpose is to define the number of workers that required during each week of operations regarding the maintenances such as (1) continuous and (2) periodic.

The following assumptions are made for this modelling.

- For the continuous maintenance, the total repair time for all subsystems of N_q elements should be as maximum 8 work- hours.

In addition, the repair times for the devices in subsystems are given in Table 14. The subsystems are illustrated in Figure 17.

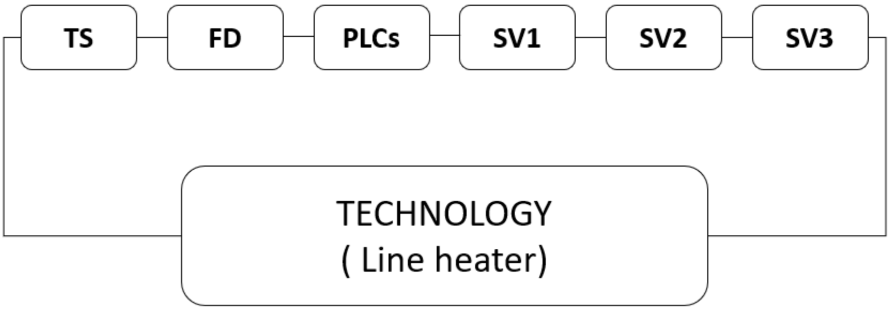


Figure 17: A control loop of "Line heater"

- A certain number of workers, $x_w^{required}$ defined in Table 4, is required during the week of proof tests at the facility. Defining this variable will be depended on the decision made by the maintenance policy for the subsystems, which is defined as a binary variable x_q^{MP} in Table 4. Thereby, the variable for maintenance policy is considered as follows.

- If $x_q^{MP} = 0$, sequential proof testing police,
- If $x_q^{MP} = 1$, parallel proof testing police.

The number of workers for performing the proof tests for the subsystems:

$$\boldsymbol{x_w^{required}} = \sum_q \left[x_q^{MP} \cdot N_q + (1 - x_q^{MP})\right] \qquad (4.30)$$

$$w \in \left\{\frac{TI}{7 \cdot 24}; \frac{2 \cdot TI}{7 \cdot 24}; \dots; \frac{k \cdot TI}{7 \cdot 24}\right\} \qquad (4.31)$$

The number of workers for performing the continuous overhauls for the subsystems:

$$\boldsymbol{x_w^{required}} = \frac{PH^{effort}}{8}, \quad \forall w \setminus \left\{\frac{TI}{7 \cdot 24}; \frac{2 \cdot TI}{7 \cdot 24}; \dots; \frac{k \cdot TI}{7 \cdot 24}\right\} \qquad (4.32)$$

$$PH^{effort} = (N_1 - M_1) \cdot T_{rep}^{TS} + (N_2 - M_2) \cdot T_{rep}^{FD} + (N_3 - M_3) \cdot T_{rep}^{PLS} + (N_4 - M_4) \cdot T_{rep}^{SV1} + (N_5 - M_5) \cdot T_{rep}^{SV2} + (N_6 - M_6) \cdot T_{rep}^{SV3} \quad (4.33)$$

The equation (4.33) is for computing the effort in person-hours (PH) to repair all the subsystems, $q = \{1,2,3,4,5,6\}$ and total number of components $N^{Total} = \{N_1 + N_2 + N_3 + N_4 + N_5 + N_6\}$, see Figure 17, for performing the continuous maintenance.

4.4.5 Markov model for the life cycle cost of ESD system

In this modelling, the total cost contains of three main components regarding the aspects such as procurement, operation, and costs associated with risk.

Table 8: Notations for LC modelling from economic perspective

Notations	Description
$\boldsymbol{q}$	index of ESD subsystems
$\boldsymbol{\tau}$	time, $[y]$
$\boldsymbol{LC_y}$	lifecycle, $[y]$
$\boldsymbol{C_{lifecycle}}$	lifecycle cost [currency units (CU)]
$\boldsymbol{C^{proc}}$	procurement cost [CU]
$\boldsymbol{C_{\tau}^{oper}}$	the yearly operation cost [CU]
$\boldsymbol{C_{\tau}^{risk}}$	the yearly risk cost [CU]
$\boldsymbol{C^{design}}$	the design cost [CU]
$\boldsymbol{C_{lq}^{purch}}$	the cost of purchasing one device chosen for subsystem q [CU]
$\boldsymbol{C_{lq}^{cons}}$	yearly electricity consumption by one device in subsystem q [CU]
$\boldsymbol{C_{lq}^{test}}$	the cost of conducting one proof test for one component of subsystem q [CU]
$\boldsymbol{C^{PL}}$	hourly losses of production [CU/h]
$\boldsymbol{C_{lq}^{rep}}$	the cost of repairing one component of subsystem q [CU]
$\boldsymbol{C_{q}^{SP}}$	the cost of spare parts replenishment for subsystem q [CU]
$\boldsymbol{C^{FM}}$	the yearly cost of facility maintenance [CU]
$\boldsymbol{C^{inc}}$	the cost of an incident and hazardous consequences [CU]
$\boldsymbol{C_{s}^{trip}}$	the costs associated with trip s (related to the transportation and the trip's duration) [CU]
$\boldsymbol{\gamma_{c}^{shift}}$	the cost modifier associated with the daily shift schedule

$\boldsymbol{\gamma^{purch}}$	purchase cost modifier corresponding to the chosen circuitry configuration
$\boldsymbol{\gamma^{design}}$	design cost modifier corresponding to the chosen circuitry configuration
$\boldsymbol{\gamma^{cons}}$	consumption cost modifier corresponding to the chosen circuitry configuration
$\boldsymbol{\sigma}$	spare part cost fraction
$\boldsymbol{T_{SU}}$	start-up time after the shutdown necessary for maintenance before the facility can be restarted, [h]
$\boldsymbol{DDR_y}$	dangerous detected failure rate for the given ESD, $[y^{-1}]$
$\boldsymbol{STR_y}$	spurious tripping rate for the given ESD, $[y^{-1}]$
δ	discount factor for the cost model

The present value of lifecycle cost of the ESD system:

$$\boldsymbol{C_{lifecycle} = C^{proc} + \sum_{\tau=1}^{LC_y} (C_\tau^{oper} + C_\tau^{risk}) \cdot \frac{1}{(1+\delta)^{\tau-1}}} \tag{4.34}$$

The procurement cost:

$$C^{proc} = C^{design} \cdot \gamma^{design} + \sum_q \sum_{l \in S_q^{inst}} \sum_{r \in S_q^{red}} C_{lq}^{purch} \cdot x_{lq}^{inst} \cdot \gamma^{purch} \cdot N_{rq} \cdot x_{rq}^{red} \tag{4.35}$$

The operation cost:

$$\begin{aligned} C_\tau^{oper} = {} & \sum_q \sum_{l \in S_q^{inst}} \sum_{r \in S_q^{red}} C_{lq}^{cons} \cdot x_{lq}^{inst} \cdot \ \gamma^{cons} \cdot N_{rq} \cdot x_{rq}^{red} + \\ & \frac{365*24}{TI} \cdot \sum_q \sum_{l \in S_q^{inst}} \sum_{r \in S_q^{red}} C_{lq}^{test} \cdot x_{lq}^{inst} \cdot N_{rq} \cdot x_{rq}^{red} + \\ & \frac{365*24}{TI} \cdot C^{PL} \cdot T^{SU} + (C^{PL} \cdot T^{SU} + \ \sum_q \sum_{l \in S_q^{inst}} \sum_{r \in S_q^{red}} C_{lq}^{rep} \cdot \\ & x_{lq}^{inst} \cdot N_{rq} \cdot x_{rq}^{red} + \sum_q C_q^{SP}) \cdot DDR_y + C^{WF} + C^{FM} \end{aligned} \tag{4.36}$$

The cost of spare parts replenishment for each subsystem:

$$C_q^{SP} = \sigma \cdot \sum_q \sum_{l \in S_q^{inst}} \sum_{r \in S_q^{red}} C_{lq}^{purch} \cdot x_{lq}^{inst} \cdot \ \gamma^{purch} \cdot N_{rq} \cdot x_{rq}^{red} \tag{4.37}$$

The dangerous detected failure rate for the ESD system:

$$DDR_y = 365 \cdot 24 \cdot \frac{\log(1 - \sum_{j=6}^{8} p_j(LC_h) \big| X^{inst}, X^{red}, X^{sep}, TI)}{LC_h} \tag{4.38}$$

In addition, the following equations introduced in order to show the impact of introducing electrical separation on the solution cost by choosing corresponding values of the cost modifiers for each subsystem:

$$\gamma^{design} = \gamma_1^{design} \cdot x_q^{sep} + \gamma_2^{design} \cdot \left(1 - x_q^{sep}\right) \tag{4.39}$$

$$\gamma^{purch} = \gamma_1^{purch} \cdot x_q^{sep} + \gamma_2^{purch} \cdot \left(1 - x_q^{sep}\right) \quad \forall q$$

$$\gamma^{cons} = \gamma_1^{cons} \cdot x_q^{sep} + \gamma_2^{cons} \cdot \left(1 - x_q^{sep}\right)$$

The cost associated with the workforce transportation to the facility and their daily shift schedule:

$$C^{WF} = \sum_{s \in S^{TRIP}} \sum_{c \in S^{DS}} C_s^{trip} \cdot x_s^{WFT} \cdot \gamma_c^{shift} \cdot x_{sc}^{WFS} \tag{4.40}$$

The risk cost:

$$C_{\tau}^{risk} = (C^{PL} \cdot T^{SU} + \sum_{q} \sum_{l \in S_q^{inst}} \sum_{r \in S_q^{red}} C_{lq}^{rep} \cdot x_{lq}^{inst} \cdot N_{rq} \cdot x_{rq}^{red}) \cdot STR_y + C^{inc} \cdot r \cdot PFD_{avg} \qquad (4.41)$$

The spurious tripping rate of the process:

$$STR_y = 365 \cdot 24 \cdot \frac{\log(1 - \sum_{j=3}^{5} p_j(LC_h) \middle| X^{inst}, X^{red}, X^{sep}, TI)}{LC_h} \qquad (4.42)$$

In addition, the dangerous detected failure rate DDR_y in (4.38), is obtained from states 6-8, and the spurious tripping rate STR_y in (4.42), is obtained from the states 3-5, of the lifecycle Markov model.

4.5 Multi-objective optimization

The model in Redutskiy (2017a) is formulated as a multi-objective problem, a literature review in section 3.4.7.2. The author used a Markov model for modelling the SIS performance, more specific it is to account for device failures occurrence and repairs, the occurrence of technological incidents and execution of facility maintenance work over the lifecycle of a hazardous facility.

In order to make the presented SIS design optimization problem compliant the author used a black box optimization algorithm. Further, to run the model there is a mathematical and programming capabilities of Mathworks Matlab software employed. Thereby, Markov analysis of system safety and the life cycle cost evaluation were implemented in the form of MATLAB script functions.

The inputs of the functions are the design variables representing a SIS design and the time interval for the planned maintenance.

The outputs of programmed functions provide the values of the PFDavg, DT, and Lifecycle cost.

Altogether, the scripts represent the objectives for the multi-criteria optimization problem. Further, MATLAB's optimization toolbox provides *gamultobj* solver that implements the multi-objective controlled elitist genetic algorithm.

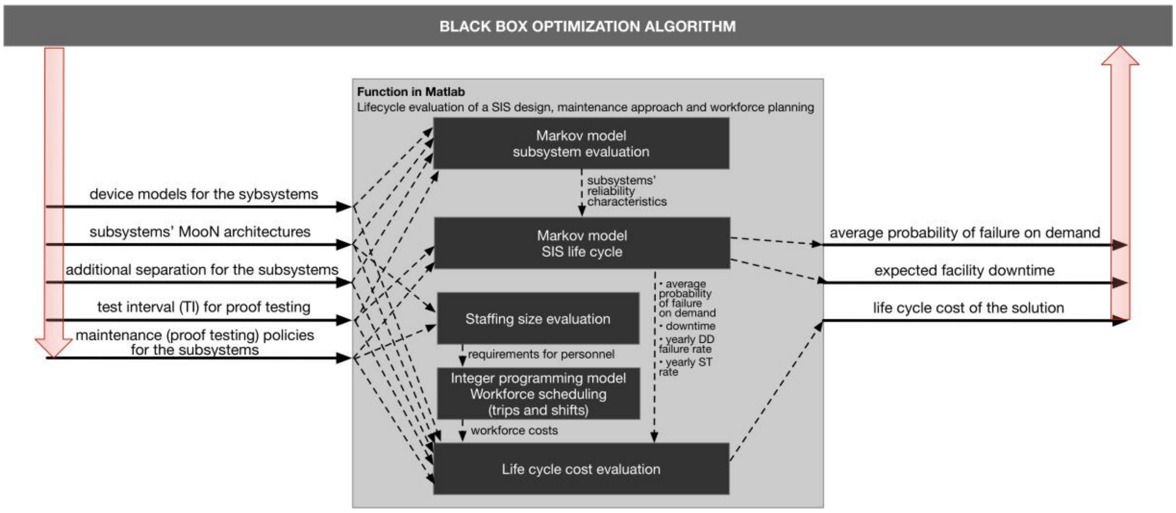

BLACK BOX OPTIMIZATION ALGORITHM
Function in Matlab
Lifecycle evaluation of a SIS design, maintenance approach and workforce planning
Markov model subsystem evaluation
subsystems' reliability characteristics
Markov model SIS life cycle
Staffing size evaluation
requirements for personnel
Integer programming model Workforce scheduling (trips and shifts)
workforce costs
Life cycle cost evaluation
• average probability of failure on demand
• downtime
• yearly DD failure rate
• yearly ST rate
device models for the sybsystems
subsystems' MooN architectures
additional separation for the subsystems
test interval (TI) for proof testing
maintenance (proof testing) policies for the subsystems
average probability of failure on demand
expected facility downtime
life cycle cost of the solution

Figure 18: Modelling and multi-objective optimization framework

Modelling and multi-objective optimization framework: Life cycle evaluation of an SIS solution for a certain technology as a programmed function. Black-box optimization of the instrumentation specification together with the approach to maintenance and workforce planning. Source: own elaborations based on (Redutskiy 2017a) and (A. C. Torres-Echeverria 2009)

5.0 Solution

This section presents the computational experiment and data used to solve the stated multi-objective problem in order to obtain some results for the research problem.

5.1 Computational experiment

The generalized model presented in 4.4.1 cannot be solved with any classical integer optimization method due to its complexity. Thus, Markov model computations are applied for computing such complex model.

The modelling has been programmed in MATLAB in the form of script functions.

The genetic algorithm (i.e. a black-box optimization algorithm run by **gamultobj** solver in Matlab's optimization toolbox, illustrated in Figure 18) is applied to solve the SIS design and maintenance planning problem for the various options of the periodic overhauls frequency.

The Markov model for the lifecycle considers the structure of technology in Figure 17, the Line heater consists of six subsystems linked in series, and as well as the descriptions in Table 6. The lifecycle model has 21 states (due to six subsystems, Figure 17 in 4.4.4), and the occurrence of an incident is illustrated in Table 9. The optimization model has 655 binary variables and 53 integer variables for design decision.

Table 9: Failure on demand: Markov model for the LC of ESD system

#	**TS**	**FD**	**PLC**	**SV1**	**SV2**	**SV3**	TECH	**EXPLANATIONS**
1	up	up	up	up	up	up	**up**	Normal course of the process
2	up	up	up	up	up	up	**down**	Safety function performed
3	***ST***	up	up	up	up	up	**down**	
4	up	***ST***	up	up	up	up	**down**	Overhaul after a ST
5	up	up	***ST***	up	up	up	**down**	
6	up	up	up	***ST***	up	up	**down**	
7	up	up	up	up	***ST***	up	**down**	
8	up	up	up	up	up	***ST***	**down**	
9	***DD***	up	up	up	up	up	**down**	
10	up	***DD***	up	up	up	up	**down**	
11	up	up	***DD***	up	up	up	**down**	Overhaul after a DD failure
12	up	up	up	***DD***	up	up	**down**	
13	up	up	up	up	***DD***	up	**down**	
14	up	up	up	up	up	***DD***	**down**	
15	***DU***	up	up	up	up	up	**up**	
16	up	***DU***	up	up	up	up	**up**	Undetected failures occur
17	up	up	***DU***	up	up	up	**up**	
18	up	up	up	***DU***	up	up	**up**	
19	up	up	up	up	***DU***	up	**up**	
20	up	up	up	up	up	***DU***	**up**	
21	**down**	**down**	**down**	**down**	**down**	**down**	**down**	**The incident has occurred.**

For the multi-objective genetic algorithm, the following settings are applied:

- Population size: 200
- Selection function: tournament
- Generational gap: 80%

- Crossover and mutation functions: custom functions for integer values of decision variables
- Initial population created with the uniform distribution applying a customized population creating function adapted for integer variables.

The optimization problem is solved with the target SIL constraint in (4.3) for the purpose of minimizing the objective functions in (4.1), i.e. the average probability of failure on demand , facility downtime, and lifecycle cost, as well as with the logical constraints in (4.4), (4.5) and set-covering workforce scheduling constraint in (4.7). As a result, there are eight solutions obtained, presented in the following subsection 6.0.

5.2 Case data

For the chosen methodology in this study, the Russian company, Rosneft, gives all data, a case of a technological unit “Line heater” at the oil and gas processing facility. The data are used in the previous master thesis project, as in (Golyzhnikova 2016). This technological unit is aimed to heat gases or liquids prior to separation and pressure reduction in a safe manner. As mentioned earlier, an occurrence of dangerous actions of the oil and gas processing facility may result in interrupting the process, harming the facility and personnel, damaging the environment and as well as economic losses. For this reason, the critical actions that may quickly lead to incidents were identified. The critical process parameters and shutdown actions are given in the following Table 10 and Table 11 respectively.

Table 10: Critical process parameters

#	Parameter	Event	Frequency, $[y^{-1}]$
1	Temperature of the air	Threshold HH $= 850\ °C$	0.03
2	Flame detected on main burner	No flame detected	0.08

Table 11: Shutdown actions

#	Final control element	Action
1	Open SV for discharging the fuel gas to flare	open
2	Close SVs on the input and output lines	close

Further, the data regarding the alternatives of shift work and trips are given in the following Table 12. The alternatives of shift work are given by the choices of a crew can work either 8-hour (the shift consists of three workers) or 12-hour (the shift consists of two workers).

After that, the crew will work at the facility for a duration of one, two, four, or six weeks. In addition, the company has a system of bonuses to reward the workers taking long trips. The pay rate cost modifier in Table 13.

Table 12: Daily shift options with associated costs

Daily shift alternatives:	**# of workers for continuous service**	**pay rate, CU/day**
(1) 8 hours of work, 16 hours of rest	3	125
(2) 12 hours of work, 12 hours of rest	2	250

Table 13: Trip alternatives with cost modifier

Trip alternatives:	**# of weeks**	**pay rate cost modifier**
(1)	1-week trip	1
(2)	2-weeks trip	1.25
(3)	4-weeks trip	1.5
(4)	6-weeks trip	2

Table 14: Repair times for the subsystems of Line heater

***Repair times*:**

# subsystems	**time [h]**
Temperature Sensors, T_{repair}^{TS}	1
Flame Detector, T_{repair}^{FD}	1
Programmable Logic Controllers, T_{repair}^{PLC}	4
Safety Valves (SV1, SV2, SV3), T_{repair}^{SV}	2

The alternatives of devices for subsystems with corresponding characteristics are given in the below.

The following alternatives are given for the subsystems; temperature sensors in Table 15, flame detectors in Table 16, programmable logic controllers in Table 17 and for the safety valves in Table 18.

Additionally, the percentage of spare part cost fraction- σ is fixed for the subsystems given as 20%, 30%, and 20%, respectively.

Table 15: Data for the subsystem, temperature sensors (TS)

Alternatives:	**TT1**	**TT2**	**TT3**	**TT4**	**TT5**
Dangerous failure rate, $[1/h]$	$2 \cdot 10^{-5}$	$2{,}86 \cdot 10^{-5}$	$5 \cdot 10^{-5}$	$9 \cdot 10^{-7}$	$7{,}14 \cdot 10^{-7}$
Spurious trip rate, $[1/h]$	10^{-5}	10^{-5}	$4{,}6 \cdot 10^{-6}$	$4{,}6 \cdot 10^{-7}$	$4{,}8 \cdot 10^{-7}$
Diagnostic coverage, %	60	60	89	80	90
Purchase cost, CU	400	250	750	1000	1500
Design cost, CU	30	15	15	13	14
Installation cost, CU	15	18	15	13	12
Consumption cost, per year CU	20	8	18	15	10
Maintenance cost, per year CU	200	150	125	125	135
Repair cost, per hour CU	5	5	5	5	6
Test cost, CU	5	5	5	4	5

Table 16: Data for the subsystem, flame detectors (FD)

Alternatives:	FD1	FD2	FD3	FD4
Dangerous failure rate, $[1/h]$	10^{-5}	$1{,}67 \cdot 10^{-5}$	$6{,}67 \cdot 10^{-6}$	$5{,}43 \cdot 10^{-6}$
Spurious trip rate, $[1/h]$	10^{-5}	10^{-5}	$3 \cdot 10^{-6}$	10^{-6}
Diagnostic coverage, %	75	80	80	85
Purchase cost, CU	600	400	1000	1050
Design cost, CU	25	20	5	5
Installation cost, CU	25	25	5	5
Consumption cost, per year CU	10	12	12	12
Maintenance cost, per year CU	100	100	50	50
Repair cost, per hour CU	5	5	5	5
Test cost, CU	4	3	3	3

Table 17: Data for the subsystem, PLCs

Alternatives:	PLC1	PLC2	PLC3
Dangerous failure rate, $[1/h]$	$9{,}11 \cdot 10^{-7}$	$1{,}25 \cdot 10^{-6}$	$5{,}96 \cdot 10^{-6}$
Spurious trip rate, $[1/h]$	$8{,}33 \cdot 10^{-7}$	$1{,}09 \cdot 10^{-6}$	$5{,}5 \cdot 10^{-6}$
Diagnostic coverage, %	90	98	97
Purchase cost, CU	22500	12500	7500
Design cost, CU	2000	1000	600
Installation cost, CU	500	250	500
Consumption cost, per year CU	500	500	400
Maintenance cost, per year CU	200	250	200
Repair cost, per hour CU	5	5	5
Test cost, CU	100	100	75

Table 18: Data for safety valves (SVs)

Alternatives:	**SV1**	**SV2**	**SV3**
Dangerous failure rate, $[1/h]$	$6{,}67 \cdot 10^{-5}$	$3{,}6 \cdot 10^{-7}$	$9 \cdot 10^{-6}$
Spurious trip rate, $[1/h]$	$3{,}33 \cdot 10^{-5}$	$1{,}8 \cdot 10^{-7}$	$5 \cdot 10^{-6}$
Diagnostic coverage, %	20	75	30
Purchase cost, CU	1300	1750	1400
Design cost, CU	650	900	900
Installation cost, CU	500	250	500
Consumption cost, per year CU	250	200	100
Maintenance cost, per year CU	50	50	50
Repair cost, per hour CU	45	40	25
Test cost, CU	50	50	50

The alternatives of voting architectures (redundancy) are given for subsystems, in Table 19.

The repair rate for a subsystem is estimated as $\mu = 0{,}125\ [h^{-1}]$ due to the constraint on the repair time maximum 8 hours.

The restoration rate for the technology is given as $\mu^t = 0{,}0625\ [h^{-1}]$.

Regarding the Common Cause Failure factor β, the following data is given:

- $\beta = 0{,}02$ is given for the solution of additional electrical separation of devices
- $\beta = 0{,}05$ is given for the solution of electrical separation of the circuits of devices

The different cost modifiers are defined for the decision-making on the additional electrical separation, in Table 20.

The duration of the lifecycle of the systems is assumed as 12 years.

The start-up cost is 2 500 000$[CU]$, cost of hazard is 125 000 000$[CU]$, and production losses is 500 000$[CU/h]$.

The start-up time T_{SU} , after the shutdown necessary for maintenance before the technology can be restarted is 12 hours, and the losses of shutdown are estimated 250 $[CU/h]$.

The discount factor for the cost model, δ is given 5% (0, 05).

Table 19: MooN architectures for the subsystems

Subsystems	Voting architectures (M-out-of-N)
Temperature sensor (TS)	1oo1; 1oo2; 1oo3; 1oo4; 1oo5
Flame detector (FD)	1oo1; 1oo2; 1oo3
Logic solver controllers (PLC)	1oo1; 1oo2; 1oo3; 1oo4; 2oo3
Final control elements (SVs)	1oo1; 1oo2; 1oo3; 1oo4

Table 20: Cost modifiers for additional electrical separation

Subsystems	Standard value	Additional electrical separation
Purchase cost modifier, $\boldsymbol{\beta^{purch}}$	1	1,15
Design cost modifier, $\boldsymbol{\beta^{design}}$	1	1
Consumption cost modifier, $\boldsymbol{\beta^{design}}$	1	1,3

6.0 Results and Analysis

The results given by the solutions of multi-objective optimization problem are the Pareto-front solutions presented below. These results represent the problem solving without imposing the restrictions on a SIL level for the developed solution.

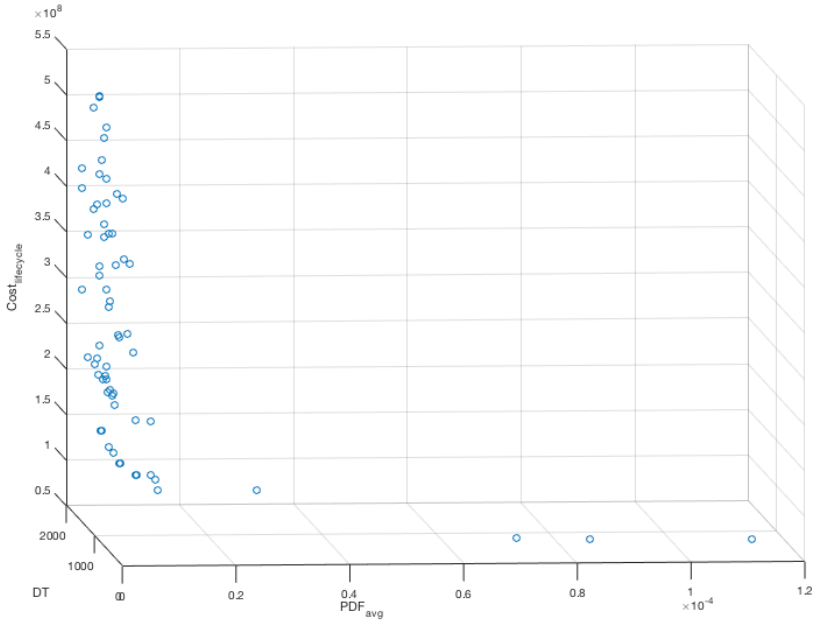


Figure 19: Pareto-front solutions

In Figure 19, Pareto-front of 71 solutions obtained as a result of the multi-objective optimization with *gamultobj* solver in Matlab. The optimization was run without the SIL3 restrictions. When the SIL3 restrictions have been applied to the multi-objective optimization results, this produced eight solutions, which will be studied and discussed further. The solutions of the Markov model and lifecycle cost model for the defined objective functions (i.e. the outputs of the model) demonstrated in Table 21.

The results obtained from the solutions of Markov model of the process, provide the following recommendations in Table 22 that can be used in the requirements specification, as a starting point to the detailed design of an engineering solution for safety system. In addition, “b” stands for baseline solution while “e” stands for additional electrical separation.

For the given problem setting, the results show that the field devices, i.e., sensors and valves, with higher reliability characteristics are preferred despite their higher costs.

In addition, the option, adding “additional electrical separation” for reducing the occurrence of common cause failure in the components is considered over the alternative.

Further, for the subsystem of temperature sensors, TT4 with 1oo2 architecture and TS5with 1oo3 architecture are equally preferred. Compared to other alternatives, they are more expensive, but the optimization algorithm preferred them to the alternative due to their component reliability, see in Table 15 and Table 20.

For the flame detectors, the alternative FD4 with 1oo3 architecture is preferred over the others, see in Table 16 and this 1oo3 is the highest redundancy architecture for such subsystem see Table 20. In comparison to devices in other subsystems, flame detectors are generally cheaper.

For the logic programmable controllers, the optimization algorithm suggested two alternatives such as PLC1 with 1oo2 and PLC2 with 1oo3, but the latter one is preferred, because it has a higher percentage of diagnostic coverage (98%) and its costs are reasonable compared to PLC1, see Table 18.

For the subsystems of final controls, in this case safety valve, only one device model SV2 is preferred. Besides the two types of redundancy architectures are considered: architecture 1oo3 for TI either 12 weeks correspond to 3 months, 16 weeks correspond to 3,5 months, and 24 weeks correspond to 4,5 months whereas architecture 1oo4 is for at least one valve subsystem when TI is 24 weeks.

Table 21: the outputs of the optimization model

#	$\boldsymbol{PFD_{avg}}$	*DT, [h]*	$\boldsymbol{Cost_{lifecycle}}$,*[CU*
1	$1{,}509 \cdot 10^{-7}$	1245	14 141 224,90
2	$2{,}917 \cdot 10^{-7}$	705	12 478 522,65
3	$2{,}720 \cdot 10^{-7}$	705	12 809 454,25
4	$2{,}649 \cdot 10^{-7}$	933	14 144 003,47
5	$2{,}673 \cdot 10^{-7}$	629	15 148 724,01
6	$5{,}014 \cdot 10^{-7}$	518	12 783 512,95
7	$4{,}364 \cdot 10^{-7}$	580	12 366 906,19
8	$4{,}290 \cdot 10^{-7}$	518	13 712 005,72

Table 22: Optimization results: Recommendations for the subsystems of SIS

#	*Temperature*	*Flame*		*Safety*	*Safety*	*Safety*	*TI*
	Sensor (TT)	*Detector (FD)*	*PLC*	*Valve1 (SV1)*	*Valve2 (SV2)*	*Valve3 (SV3)*	*[w]*
1	{TS4; 1oo2; e; seq}	{FD4; 1oo3; e; seq}	{PLC2; 1oo3; e; par}	{SV2; 1oo3; e; seq}	{SV2; 1oo3; e; seq}	{SV2; 1oo3; e; par}	12
2	{TS4; 1oo2; e; seq}	{FD4; 1oo3; e; seq}	{PLC1; 1oo2; e; par}	{SV2; 1oo3; e; seq}	$\{SV2; 1oo3; e; par\}$	$\{SV2; 1oo3; e; seq\}$	16
3	{TS4; 1oo2; e; seq}	{FD4; 1oo3; e; seq}	{PLC2; 1oo3; e; par}	{SV2; 1oo3; e; seq}	$\{SV2; 1oo3; e; seq\}$	$\{SV2; 1oo3; e; par\}$	16
4	{TS5; 1oo3; e; par}	{FD4; 1oo3; e; seq}	{PLC2; 1oo3; e; par}	{SV2; 1oo3; e; par}	$\{SV2; 1oo3; e; seq\}$	$\{SV2; 1oo3; e; par\}$	16
5	{TS5; 1oo3; e; par}	{FD4; 1oo3; e; seq}	{PLC2; 1oo3; e; par}	{SV2; 1oo3; e; par}	$\{SV2; 1oo3; e; par\}$	$\{SV2; 1oo4; e; par\}$	16
6	{TS4; 1oo2; e; par}	{FD4; 1oo3; e; seq}	{PLC1; 1oo2; e; par}	{SV2; 1oo3; b; par}	$\{SV2; 1oo4; e; par\}$	$\{SV2; 1oo3; e; par\}$	24
7	{TS5; 1oo3; e; seq}	{FD4; 1oo3; e; seq}	{PLC2; 1oo3; e; par}	{SV2; 1oo4; e; par}	$\{SV2; 1oo3; e; par\}$	$\{SV2; 1oo3; e; par\}$	24
8	{TS5; 1oo3; e; par}	{FD4; 1oo3; e; seq}	{PLC2; 1oo3; e; par}	{SV2; 1oo4; e; par}	$\{SV2; 1oo3; e; par\}$	$\{SV2; 1oo4; e; par\}$	24

Regarding the maintenance policies, the algorithm decided that PLCs should be maintained in parallel. This decision might be taken due to its largest repair time, see Table 14.

For the temperature sensors both policies are applied equally, but at least one of the temperature sensors subsystems should be maintained in sequential when TI is 24 weeks.

For the safety valves, the parallel testing is applied when TI is 24 weeks, considering the higher repair time for valves compared to other field devices, Table 14. This also may be attributed to the large number of workers required for parallel testing.

Regarding the workforce scheduling, during the normal operations four workers are required to be present at the facility to monitor and do the continuous maintenance. This demand is mostly covered by 4-week trips with 8 hours of work and 16 hours of rest correspond to 3 workers, see Table 12 and Table 13.

For proof test, more workers are required. The number of workers depends on the maintenance policy either parallel or sequential. This number varies between 9 and 18.

The work schedule for maintenance workers during proof tests is covered by 1 week trip with 12 hours work and 12 hours of rest, this schedule corresponds to a crew consists of two workers, in Table 15. The optimization algorithm appears to keep the total number of workers required fewer than 20.

In addition, the importance of workforce considerations is that the costs associated with maintenance personnel salaries and their transportation costs are a significant share (more than 90%, see COST labor in Table 23) of the operational expenditures of the safety system in this particular case. The cost estimations of the results are shown in below Table 23.

Table 23: Costs of the safety system

	***COST** LIFECYCLE*	***COST** PROCUREMENT*	***COST** OPERATIONS*		***COST** RISK*
			total	*incl. COST labor*	
1	14 141 224,90	2 142 833,53	11 998 371,10	10 875 683,98	20,27
2	12 478 522,65	2 030 149,73	10 448 336,25	9 473 656,59	36,66
3	12 809 454,25	2 033 915,56	10 775 504,32	9 797 482,06	34,37
4	14 144 003,47	2 077 557,04	12 066 412,04	11 059 721,52	34,39
5	15 148 724,01	1 903 904,68	13 244 768,70	12 277 563,03	50,63
6	12 783 512,95	1 997 469,01	10 785 978,05	9 996 526,06	65,89
7	12 366 906,19	1 588 585,56	10 778 278,38	9 990 363,62	42,25
8	13 712 005,72	1 706 361,17	12 005 599,22	11 127 316,23	45,33

Overall, the obtained results given the multi-objective problem are “a Pareto-front” of optimal solutions for the problem, which similar to the one in (Redutskiy 2017a). However, expanded with personnel organization issues (e.g. work schedule, staffing size, personnel transport, etc.) which influences the Markov model of the process (e.g. incidents/repairs and failures/restorations), and the life cycle cost model.

7.0 Conclusions

The petroleum industry is facing a shift towards the operations in unpredictable environments and remote locations; therefore, the processes in such conditions must run smoothly and be economically efficient. The development and operation of automated safety systems (i.e. IT-solutions) are crucial to the oil and gas processes in such circumstance. The decisions related to the safety systems design (include the architectures and the instrumentation choices for the system’s components), and maintaining the safety systems as well as the facility’s personnel and their transportation to the remote locations and back are highly considerable. Because these issues are the main cost drivers to the capital investments into the safety systems. This thesis addressed the issues related to the design and maintenance planning of the safety system, in this case a small-automated ESD system, with a focus on workforce scheduling for remotely located oil and gas processing facilities. Therefore, the objective of this research has been to address the problem of SIS design and maintenance modelling to optimize the set of safety measures inherent in the SIS and simultaneously to determine the staffing size and their working schedules as well as the maintenance policy for SIS performance. The multi-objective optimization of the SIS design and maintenance planning considered both safety and economic indicators in order to explore the trade-off between the cost of using safety measures and the obtained safety level for SIS performance.

The modelling in this research is to ensure the safety of operations by simultaneously evaluating the decisions on the safety system`s components and structures, the facility maintenance frequencies, the staffing size of maintenance personnel and transportation of staff, as well as the schedules of their work shift. The Markov model applied for safety quantification, i.e. addressing the device failures and repairs, technological incidents and restorations, and the periodic maintenance policy, while a black-box optimization algorithm was used in the decision-making process. This research based on the results obtained from the optimization models provides a conceptual framework in Figure 20 that points the importance of SIS design and aims to contribute to the decisions made by the E&P operators (engineering department) and the engineering design contractors regarding the formulation of straightforward requirements for the safety systems. This suggested decision-making approach is not only for formulating requirements specification but also advisable to use as a basis for detailed engineering design as well as a research for reasonable engineering solutions. The solution methods and models that are used in this research can be transferable to other process industries, considering the safety system problems.

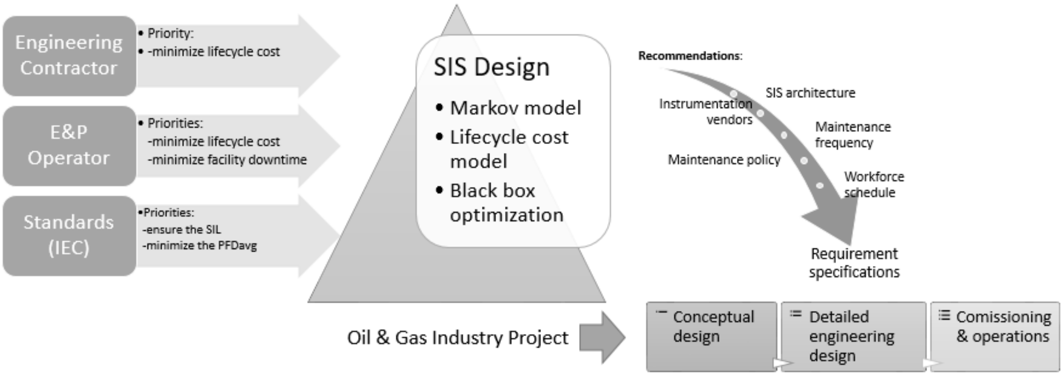


Figure 20: A conceptual framework for SIS design and maintenance planning

7.1 Research limitations

The limitations of this research might be as follows. Firstly, regarding the safety system design, the diverse redundancy is not considered for the subsystems, as well as aging of the system out of consideration. Secondly, some limitations relates to the maintenance planning. Refer to the literature review, in 2.4.5, several strategies can be applied to the proof tests, and this research is limited to only partial and sequential. Another limitation relates to workforce scheduling, the consideration of maintenance crews is only on the E&P operator side, i.e. the issues on contractor`s side not considered at all. Since there are several automated control systems, which also need to be maintained, installed on the oil and gas facility there will be need for more workers to do the necessary maintenance.

7.2 Further research

For the further research, considering diverse redundancy (e.g. different devices into a subsystem) for the subsystems in the modelling can improve the proposed model. The aging of the system must be taken into account in the modelling regarding to system reliability (failure rate in 3.2.1.2 and Figure 10). For the maintenance planning, introducing more detailed proof testing policies can improve the models, and the workforce scheduling may be modelled other than a set-covering problem. As seen during the computational experiment 6.1, the genetic algorithm is not quite efficient, thus, developing a heuristic for this particular problem is recommended. From the logistics perspective, introducing inter modal options for transportation of the maintenance crew in the model that could be a research direction, which will be especially relevant for offshore locations. For the remotely located O&G facilities, transporting the maintenance crews to and from the facilities cost significantly. Thus, the expanding the transportation cost in the modelling can ensure more reliable proposed approach to the design decisions of safety systems.

8.0 References

Abraha, Haftay Hailay. 2011. *Optimization of Maintenance Performance for Offshore Production Facilities.* Master Thesis, University of Stavanger.

Ahmad, Rosmaini, and Shahrul Kamaruddin. 2012. "An overview of time-based and condition-based maintenance in industrial application." *Computers & Industrial Engineering* 63 (1): 135-149.

Alaswad, Suzan, and Yisha Xiang. 2017. "A review on condition-based maintenance optimization models for stochastically deteriorating system." *Reliability Engineering and System Safety* 157: 54-63.

Altiparmak, Fulya, Mitsuo Gen, Lin Lin, and Turan Paksoy. 2006. "A genetic algorithm approach for multi-objective optimization of supply chain networks." *Computers & Industrial Engineering* 51 (1): 196-215.

Anderson, Kristanna, and Luiza Oancea. 2016. *Analysis of urgent deliveries in Upstream Petroleum Logistics: A case study of Haltenbanken area.* Master`s degree thesis, Molde, Norway: Molde University College.

Anderson, W. E. 2005. "Risk analysis methodology applied to industrial machine development." *IEEE Trans. Ind. Appl.*, Jan./Feb.: 180-187.

Avison, David, and Guy Fitzgerald. 2003. *Information Systems Development: Methodologies, Techniques, and Tools.* Third Edition. UK: McGraw-Hill Education.

Avizienis, A., J. C. Laprie, and B. Randell. 2000. *Fundamental Concepts of dependability.* 3rd. Boston, Massachusetts: Information Survivability Workshop (ISW-2000).

Barone, Giorgio, and Dan M. Frangopol. 2013. "Life-cycle maintenance of deteriorating structures by multi-objective optimization involving reliability, risk,availability, hazard and cost." *Stuctural Safety* 48: 40-50.

Barone, Giorgio, Dan M. Frangopol, and Mohamed Soliman. 2014. "Optimization of Life-Cycle Maintenance of Deteriorating Bridges with respect to Expected Annual System Failure Rate and expected Cumulative Cost." *Journal of Structural Engineering* 140 (2).

Barros, Anne, Christophe Berenguer, Hai Canh Vu, and Phuc Do. 2015. "Maintenance grouping for multi-component systems with availability constraints and limited maintenance teams." *Reliability Engineering and System Safety* (142): 56-67.

Barusco, P. 2002. "The accident of P-36 FPS." *Offshore Technology Conference.* Housten.

Berendes, Kees. 2007. "Engineering and construction projects for oil and gas processing facilities : Contracting, uncertainty and the economics of information." *Energy Policy* 35: 4260-4270.

Berenguer, Christophe, and Phuc Do Van. 2012. "Condition-Based Maintenance with Imperfect Preventive Repairs for a Deteriorating production System." *Quality and Reliability Engineering International* 28 (6): 624-633.

Bouvard, K., S. Artus, C. Berenguer, and V. Cocquempot. 2011. "Condition-based dynamic maintenance operations planning & grouping. Application to commercial heavy vehicles." *Reliablility Engineering and System Safety* 96 (6): 601-610.

BP. 2010. *Deepwater Horizon Accident Investigation Report.* BP. bp.com.

—. 2017. "Oil reserves." *bp Global.* 11 19. https://www.bp.com/en/global/corporate/energy-economics/statistical-review-of-world-energy/oil/oil-reserves.html.

Brandao, J., and A. Mercer. 1998. "The multi-trip vehicle routing problem." *Journal of the Operational Research Society* 49 (8): 799-805.

Bryman, Alan, and Emma Bell. 2015. *Business research methods.* USA: Oxford University Press.

Bukowski, J. 2001. "Modelling and analyzing the effects of periodic inspection on the performance of safety-critical systems." *IEEE Transactions on Reliability* 50 (3): 321-329.

Bukowski, J. 2006. "Incorporating process demand into models for assessment of safety system performance." *RAMS`06 Annual Reliability and Maintainability Symposium.* Newport Beach, California USA: IEEE. 577-581.

Carazas, F. G., and G. F.M. Souza. 2010. "Risk-based decision making method for maintenance policy selection of thermal power plant equipment." *Energy* (35): 964-975.

Castillo-Salazar, Arturo, Dario Landa-Silva, and Qu Rong. 2016. "Workforce scheduling and routing problems: Literature survey and computational study." *Annals of Operation Research* 239 (1): 39-67.

Castillo-Salazar, Arturo, Dario Landa-Silva, and Rong Qu. 2016. "Workforce scheduling and routing problems: literature survey and computational study." *Annals of Operations Research* 239 (1): 39-67.

Catelani, M., L. Ciani, and V. Luongo. 2011. "A simplified procedure for the analysis of safety instrumented systems in the process industry application." *Microelectronics Reliability* (51): 1503-1507.

Catelani, Marcantonio, Lorenzo Ciani, and Valentina Luongo. 2010. *Safety Analysis in Oil & Gas Industry in compliance with Standards IEC61508 and IEC61511: Methods and Applications.* research paper, Department of Information Engineering, Florence, Italy: University of Florence.

CCPS. 2005. *Building Process Safety Culture: Tools to Enhance Process Safety Performance.* New York: Center for Chemical Process Safety of the American Institute of Chemical Engineers.

—. 2007. *safe and Reliable Instrumented Protective Systems.* Edited by Center for Chemical Process Safety. New Jersey: Wiley Interscience.

CCPS, Centre for Chemical Process Safety. 2010. *Guidelines for Safe Process Operations and Maintenance.* New York: John Wiley & Sons.

Chang, Kwangpil, Sungteak Kim, Daejun Chang, Junkeon Ahn, and Enrico Zio. 2015. "Uncertainty analysis for target SIL determination in the offshore industry." *Journal of Loss Prevention in the Process Industries* (34): 151-162.

Chen, Yanghou. 2011. "Reliability Analysis of a Fire Alarm System." *Procedia Engineering* (24): 731-736.

Cho, Danny I., and Mahmut Parlar. 1991. "A survey of maintenance models for multi-unit systems." *European Journal of Operational Research* 51 (1): 1-23.

Cimarron Energy. 2018. "Line Heaters." *Cimarron energy.* 5 5. www.cimarronenergy.com/products/line-heaters/.

Dadashzadeh, Mohammad, Rouzbeh Abbassi, Faisal Khan, and Kelly Hawboldt. 2013. "Explosion modeling and analysis of BP Deepwater Horizon accident." *Safety Science* 57: 150-160.

Deb, Kalyanmoy, Samir Agrawal, Amrit Pratap, and T. Meyarivan. 2000. "A Fast Elitist Non- dominated Sorting Genetic Algorithm for Multi-objective Optimization: NSGA-II." *Parallel Problem Solving from Nature PPSN VI.* 849-858.

Dekker, Rommert. 1996. "Applications of maintenance optimization models: a reveiw and analysis." *Reliability Engineering and System Safety* 229-240.

Dekker, Rommert, Ralph E. Wildeman, and Frank A. van der Duyn Schouten. 1997. "A review of multi- component maintenance models with economic dependence." *Mathematical Methods of Operations Research* 45 (3): 411-435.

Delfmann, Werner, Wilhelm Dangelmaier, Willibald Gunthner, Peter Klaus, Ludger Overmeyer, Werner Rothengatter, Jurgen Weber, and Joachim Zentes. 2010. "Towards a science of logistics: cornerstones of a framework of understanding of logistics as an academic discipline." *Logistics Research* 2 (2): 57-69.

Desrochers, M, J Desrosiers, and M Solomon. 1992. "A new optimization algorithm for the vehicle routing problem with time windows." *Operation Research* 40 (2): 342-354.

Devold, Håvard. 2013. *Oil and gas production handbook.* ABB Oil and Gas.

Doerr, Benjamin, Carola Doerr, and Franziska Ebel. 2015. "From black-box complexity to designing new genetic algorithms." *Theoretical Computer Science* 567 (16): 87-104.

Doerr, Benjamin, Timo Kotzing, Johannes Lengler, and Carola Winzen. 2013. "Black-box complexities of combinatorial problems." *Theoretical Computer Science* 471 (3): 84-106.

Droste, S., T. Jansen, and I. Wegener. 2006. "Upper and lower bounds for randomised search heuristics in black.box optimization." *Theory of Computing Systems* 39: 525-544.

Duijm, N. J. 2008. "Safety-barrier diagrams." *Proceedings of the Institution of Mechanical Engineers* 222: 439-448.

Dutuit, Y., F. Innal, A. Rauzy, and J.-P. Signoret. 2008. "Probabilistic assessments in relationship with safety integrity levels by using fault trees." *Reliability Engineering & System Safety* 93 (12): 1867-1876.

Elegbede, C., and K. Adjallah. 2003. "Availability allocation to repairable systems with genetic algorithms: a multiobjective formulation." *Reliability Engineering and System Safety* 82: 319-330.

Eliassen , Igor. 2013. *Management of change - with the main focus on Safety Instrumented Systems* . Master`s Thesis, Stavanger: University of Stavanger.

Esparza, Alejandro, and Monica Levy Hochleitner. 2010. *A brief discussion over safety costs in new enterprises.* www.exida.com/images/uploads/CCPS_LA_2010_SIS_EsparzaHochleitner.pdf.

Eti, M. C., S. O.T. Ogaji, and S. D. Probert. 2007. "Integrating, reliability, availability, maintainability and supportability with risk analysis for improved operation of the Afam thermal power-station." *Applied Energy* (84): 202-221.

Firesmith, Donald. 2004. "Engineering Safety Reguirements, Safety Constraints, and Safety- Critical Requirements." *Journal of Object Technology* 3 (3): 27-42.

Frangopoulos, C., and G. Dimopoulos. 2004. "Effect of reliability considerations on the optimal synthesis, design and operational of a cogeneration system." *Energy* 29 (12): 309-329.

Gabriel, Angelito. 2017. "Design and Evaluation of Safety Instrumented Systems: A Simplified and Enhanced Approach." *IEEE Access*, March 7: 3813-3823. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7873320.

Gen, M., and YS. Yun. 2006. "Soft computing approach for reliability optimization: state-of-the-art survey." *Reliabilty Engineering and System Safety* 91: 1008-1026.

Giuggioli Busacca, P., M. Marsequerra, and E. Zio. 2001. "Multiobjective optimization by genetic algorithms: application to safety systems." *Reliability Engineering & System Safety* 72 (1): 59-74.

Goble, W.M. 1998. *Control Systems Safety Evaluation & Reliability*. NC: The Instrumentation, Systems and Automation Society. Research Triangle Park.

Goble, WM, and AC Brombacher. 1999. "Using a failure modes, effects and diagnostic analysis(FMEDA) to measure diagnostic coverage in programmable electronic systems." *Reliability Engineering and System Safety* 66 (2): 145-8.

Golyzhnikova, Daria. 2016. *Mathematical Modelling of Safety Instrumented System for Pipeline Infrastructure Planning.* Master Thesis, Molde: Molde University College.

Gruhn, P., and H. Cheddie. 1998. *Safety Shutdown Systems: Design, Analysis and Justification.* NC: The Instrumentation Systems and Automation Society.

Hauge, Stein, Mary Ann Lundteigen, and Marvin Rausand. 2009. *Updating failure rates and test intervals in the operational phase: A practical implementation of IEC61511 and IEC61508.* Conference Paper, ResearchGate.

Hauge, Stein, Mary Ann Lundteigen, Per Hokstad, and Solfrid Håbrekke. 2010. *Reliability Prediction Method for Safety Instrumented Systems: PDS Method Handbook.* Trondheim: SINTEF Technology and Society Safety Research. www.sintef.no.

Hollnagel, Erik . 2008. "Risk + barriers = safety?" *Safety Science* (46): 221-229.

Hollnagel, Erik. 2004. *Barriers and Accident Prevention.* London: Ashgate.

Honeywell. 2002. *Safety Instrumented Systems (SIS), Safety Integrity Levels (SIL), IEC61508, and Honeywell Field Instruments.* Honeywell International Inc. www.honeywellprocess.com/imc.

Horenbeek, Adriaan Van, and Liliane Pintelon. 2013. "A dynamic predictive maintenance policy for complex multi-component systems." *Reliability Engineering & System Safety* 120: 39-50.

HSE. 2010. *Major Hazards.* The British Health and Safety Executive (HSE).

HSE. 2014. *Offshore Oil and Gas Sector Startegy 2014 to 2017.* Health and Safety Executive. www.hse.gov.uk/offshore/offshore-oil-and-gas.pdf .

—. 2003. *Out of control: Why Control Systems go Wrong and How to prevent Failure.* Ed 2. UK: Sheffield.

IEC 61508. 1998. "61508 Functional safety of electrical /electronic/programmable electronic safety-related systems." Geneva, Switzerland.

IEC 61508. 2010. "Functional safety of electrical/electronic/programmable electronic safety related systems.part 1-7."

IEC 61511. 2003. "61511 Functional safety - safety instrumented system for the process industry sector." Geneva, Switzerland.

Innal, Fares, Mary Ann Lundteigen, Yiliu Liu, and Anne Barros. 2016. "PFD avg. generalized formulas for SIS subject to partial and full periodic tests based on multi-phase Markov models." *Reliability Engineering and System Safety* 150: 160-170.

Innal, Fares, Yves Dutuit, and Mourad Chebila. 2015. "Safety and operational integrity evaluation and design optimization of safety instrumented system." *Reliability Engineering and System Safety* 134: 32-50.

ISA, Instrument Society of America. 1997. *Application of Safety Instrumented Systems for the Process Industries.* USA: Instrumentent Society of America.

Jahromi, Abdolhamid Eshraghniaye, and Mohammad Feizabadi. 2017. "Optimization of multi-obejctive redundancy allocation problem with non-homogeneous components." *Computers & Industrial Engineering* 108: 111-123.

Jalote, P. 1994. *Fault Tolerance in Distributed Systems.* New Jersey: PTR Prentice Hall.

Jigar, Abraham Almaw, Yiliu Liu, and Mary Ann Lundteigen. 2016. "Spurious activation analysisof safety- instrumented systems." *Reliability Engineering and System Safety* (156): 15-23.

Jin , Hui. 2013. *A contribution to reliability assessment of safety- instrumented systems.* PhD Thesis, Trondheim: Norwegian University of Science and Technology.

Jin, Hui, Mary Ann Lundteigen, and Marvin Rausand. 2011. "Reliability performance of safety instrumented systems: a common approach for both low- and high-demand mode of operation." *Reliability Engineering and System Safety* (51): 365-373.

Kahn, F., and M. Haddara. 2004. "Risk-based maintenance of ethylene oxide production facilities." *Journal of Hazardous Materials* 3 (12): 147-159.

Kaszniak, Mark, and Donald Holmstrom. 2008. "Trailer siting issues: BP Texas City." *Journal of Hazardous Materials* 159 (1): 105-111.

Kim, Man Cheol. 2011. "Reliability block diagram with general gates and its application to system reliability analysis." *Annals of Nuclear Energy,* November: 2456-2461.

Konak, Abdullah, David W. Coit, and Alice E. Smith. 2006. "Multi-objective optimization using genetic algorithms: A tutorial." *Reliability Engineering & System Safety* 91 (9): 992-1007.

Kosmowski, Kazimierz T. 2006. "Functional safety concept for hazardous systems and new challenges." *Journal of Loss Prevention in the Process Industries* (19): 298-305.

Kvasov, Dmitri E., and Yaroslav D. Sergeyev. 2015. "Deterministic approaches for solving practical black-box global optimization problems." *Advances in Engineering Software* 80: 58-66.

Langeron, Y, A Barros, A Grall, and C Berengeur. 2008. "Combination of safety integrety levels(SILs): a study of IEC61508 merging rules." *Journal of Loss Prevention in the Process Industries* 21 (4): 437-449.

Lapa, C., M. Pereira, and M. de Barros. 2006. "A model for prventive maintenance planning by genetic algorithms based in cost and reliability." *Reliability Engineering & System Safety* 91 (2): 223-240.

Laprie, J. C. 1992. *Dependability: Basic concepts and terminology.* Vienna: Springer-Verlag.

Lewis, E.E. 1996. *Introduction to reliability engineering.* 2nd ed. New York: John Wiley & Sons.

Lim, A., B. Rodrigues, and L. Song. 2004. "Manpower allocation with time windows." *Journal of the Operational Research Society* 55: 1178-1186.

Limbourg, Philipp, and Hans-Dieter Kochs. 2006. "Preventive maintenance scheduling by variable dimension evolutionary algorithms." *International Journal of Pressure Vessels and Piping* 83 (4): 262-269.

Liu, Yiliu, and Marvin Rausand. 2011. "Reliability assessment of safety instrumented systems subject to different demand modes." *Journal of Loss Prevention in the Process Industries* (24): 49-56.

Liu, Yiliu, and Mary Ann Lundteigen. 2015. "Reliability Importance of the Channels in Safety Instrumented Systems." *Industrial engineering, Management Science and Applications 2015 (ICIMSA2015).* 1041-1054.

Lundteigen, Mary Ann. 2008. *Safety instrumented systems in the oil and gas industry: concepts and methods for safety and reliability...* PhD Thesis, Trondheim: Norwegian University of Science and Technology.

Lundteigen, Mary Ann, and Marvin Rausand. 2009. "Architectural constraints in IEC 61508: Do they have the intended effect?" *Reliability Engineering & System Safety* 94 (2): 520-525.

Lundteigen, Mary Ann, and Marvin Rausand. 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 (3): 218-229.

Lundteigen, Mary Ann, and Marvin Rausand. 2008. "Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas." *Reliability Engineering & System Safety* 93 (8): 1208-1217.

Markeset, T., and U. Kumar. 2001. "Integration of RAMS information in design processes - a symposium." *20-24 January.* Tampa, FL.

Marseguerra, M., E. Zio, and S. Martorell. 2006. "Basics of genetic algorithms optimization for RAMS applications." *Reliability Engineering and System Safety* 91 (9): 977-991.

Martorell, S., A. Sanchez, S. Carlos, and V. Serradell. 2004. "Alternatives and challenges in optimizing industrial safety using genetic algorithms." *Reliability Engineering & System Safety* 86 (1): 25-38.

Mechri, W., C. Simon, F. Bicking, and K. Ben Othman. 2013. "Fuzzy multiphase Markov chains to handle uncertainties in safety systems performance assessment." *Journal of Loss Prevention in the Process Industries* (26): 594-604.

Mechri, Walid, Christophe Simon, and Kamel Ben Othman. 2015. "Switching Markov chains for a holistic modeling of SIS unavailability." *Reliability Engineering & System Safety*, January: 212-222.

Milakovic, Aleksandar-Sasa, Soren Ehlers, and Peter Schutz. 2014. *Offshore upstrean logistics for operations in Arctic environment.* Conference paper, ResearchGate.

Modarres, M. 1993. *What every engineer should know about reliability and risk analysis.* New York: Marcel Decker.

Moss, M. A. 1985. *Design for minimal maintenance expense.* New York, USA: Marcel Dekker Inc.

Nachmias, David, and Chava Nachmias. 1993. *Research methods in the social sciences.* New York: St. Martin's.

Nguyen, Kim-Ahn, Phuc Do, and Antoine Grall. 2015. "Multi-level predective maintenance for multi-component systems." *Reliability Engineering and System Safety* 144: 83-94.

NOGA, Norwegian Oil and Gas Association. 2004. *070 - Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry.* ed. 2. Sandnes, Norway: Norsk olje og gass. www.norskoljeoggass.no.

Perrow, Charles. 1999. *Normal Accidents: Living with High-Risk Technologies.* updated edition. Princeton University Press.

PetroWiki. n.d. "Oil Facility." *PetroWiki.* Accessed March 18, 2018. http://petrowiki.org/Oil_facility.

Piesik, E., M. Sliwinski, and T. Barnert. 2016. "Determining and verifying the safety integrity level of the safety instrumented systems with the uncertainty and security aspects." *Reliability Engineering and System Safety* (152): 259-272.

PSA. 2013. "Focus: Major accidents." *Petroleum Safety Authority Norwat* . Februar 20. Accessed May 3, 2018. www.ptil.no.

Rahimi, Maryam, and Marvin Rausand. 2013. "Monitoring human and organizational factors influencing common-cause failures of safety -instrumented system during the operational phase." *Reliability Engineering and System Safety* (120): 10-17.

Rausand, Marvin, and Arnljot Høyland. 2004. *System Reliability Theory.* 2nd. New Jersey: John Wiley &Sons, Inc.

Reason, James T. 1990. *Human Error.* Cambridge, UK: Cambridge University Press.

Redutskiy, Yury. 2017c. "Modelling and Design of Safety Instrumented Systems for Upstream Processes of Petroleum Sector." *Procedia Engineering* 182: 611-618.

Redutskiy, Yury. 2017a. "Optimization of Safety Instrumented System Design and Maintenance Frequency for Oil and Gas Industry Processes." *Management and Production Engineering Review* 8 (1): 46-59.

Redutskiy, Yury. 2017b. *Startegic planning problems for smart solutions in oil and gas industry.* Public presentation, Molde University College.

Regis, Rommel G. 2016. "Multi-objective constrained black-box optimization using radial basis function surrogates." *Journal of Computational Science* 16: 140-155.

Safeopedia. n.d. "Safety Requirements Specifications (SRS)." *safeopedia.* Accessed May 08, 2018. https://www.safeopedia.com/definition/5012/safety-requirements-specifications-srs.

Shafiee, Mahmood, and John Dalsgaard Sørensen. 2017. "Maintenance optimization and inspection planning of wind energy assets: Models, methods and strategies." *Reliability Engineering & System Safety* 1-19.

Sintef. 2006. *Reliability prediction methods for safety instrumented systems- PDS method handbook.* Trondheim, Norway: SINTEF.

Sklet, Snorre. 2006. "Safety barriers: Definition, classification, and performance." *Journal of Loss Prevention in the Process Industries* (19): 494-506.

Skogdalen, Jon Espen, and Jan Erik Vinnem. 2012. "Combining precursor incidents investigations and QRA in oil and gas industry." *Reliability Engineering & System Safety* 101: 48-58.

Storey, N. 1996. *Safety-critical Computer Systems.* New York: Addison Wesley Longman.

Tian, Zhigang, Daming Lin, and Bairong Wu. 2012. "Condition based maintenance optimization considering multiple objectives." *Journal of Intelligent Manufacturing* 23 (2): 333-340.

Torres-Echeverria, A, S Martorell, and H Thompson. 2009. "Modelling and optimization of proof testing policies for safety instrumented systems." *Reliability Engineering and System Safety* 94 (4): 838-54.

Torres-Echeverria, A. C., S. Martorell, and H. A. Thompson. 2011. "Modeling safety instrumented systems with MooN voting architectures addressing system reconfiguration for testing." *Reliability Engineering & System Safety* 96 (5): 545-563.

Torres-Echeverria, A. C., S. Martorell, and H. A. Thompson. 2012. "Multi-objective optimization of design and testing of safety instrumented systems with MooN voting architectures using a genetic algorithm." *Reliability Engineering and System Safety* 106: 45-60.

Torres-Echeverria, Alejandro Carlos. 2009. *Modelling and optimization of Safety Instrumented Systems based on dependability and cost measures.* PhD Thesis, The University of Sheffield.

Tutorials Point. n.d. "System Development Life Cycle." *tutorialspoint.* Accessed May 08, 2018. https://www.tutorialspoint.com/system_analysis_and_design/system_analysis_and_design_development_life_cycle.htm .

USDI. 2010. *Increased safety measures for energy development on the outer continental shelf.* . US Department of the Interior.

USEPA. 2001. "Giant oil rig sinks." *The Journal of the U.S. EPA Oil Program Center* 5: 1-3.

Usher, John S., Ahmed H. Kamal, and Wasim Hashmi Syed. 1998. "Cost optimal preventive maintenance and replacement scheduling." *IIE Transactions* 30 (12): 1121-1128.

Van, Phuc Do, Anne Barros, Christophe Berenguer, Keomany Bouvard, and Florent Brissaud. 2013. "Dynamic grouping maintenance with time liited opprotunities." *Reliability Engineering & System Safety* 120: 51-59.

Vinnem, J. E., R. Bye, B. A. Gran, T. Kongsvik, O. M. Nyheim, E. H. Okstad, J. Seljelid, and J. Vatn. 2012. "Risk modelling of maintenance work on major process equipment on offshore petroleum installations." *Journal of Loss Prevention in the Process Industries* 25 (2): 274-292.

Vu, Hai Canh, Phuc Do, Anne Barros, and Christophe Berenguer. 2015. "Maintenance planning and dynamic grouping for multi-component systems with positive and negative economic dependencies." *IMA Journal of Management Mathematics* 26 (2): 145-170.

Wacker, John G. 1998. "A definition of theory: research guidelines for different theory-building research methods in operations management." *Journal of operations management* 16 (4): 361-385.

Wang, Feng, Ou Yang, Ruibo Zhang, and Lei Shi. 2016. "Method for assigning safety integrity level (SIL) during design of Safety instrumented systems (SIS) from database." *Journal of Loss Prevention in the Process Industries* (44): 212-222.

Wiekema, B. J. 1984. "Vapour cloud explosions - an analysis based on accidents: Part II." *Journal of Hazardous Materials* 313-329.

WikipediA. 2017. *IEC 61508.* March. https://en.wikipedia.org/wiki/IEC_61508.

—. 2017. *IEC 61511.* March. https://en.wikipedia.org/wiki/IEC_61511.

Wildeman, R. E., R. Dekker, and A. C. J. M. Smit. 1997. "A dynamic policy for grouping maintenance activities." *European Journal of Operational Research* 99 (3): 530-551.

Yin, Robert K. 2003. *Case study research: Design and methods.* 3rd. Sage Publications.

—. 2014. *Case study research: design and methods. 5th ed.* Los Angeles: Calif: SAGE.

Yoset, David. 2017. *Safety Instrumented Systems vs Process Control Systems.* March 27. https://www.crossco.com/blog/safety-instrumented-systems-vs-process-control-systems.

Zolotukhin, Anatoly, Anton Sungurov, and Vlada Streletskaya. 2015. "Barents Sea hydrocarbon resource base and production potential." In *International Arctic Petroleum Cooperation: Barents Sea scenarios*, by Anatoli Bourmistrov, Frode Mellemvik, Alexei Bambulyak, Ove Gudmestad, Indra Overland and Anatoly Zolotukhin, 147-160. New York: Routledge.

Øien, K., I. B. Utne, and I. A. Herrera. 2011. "Building Safety Indicators: Part 1 - Theoretical foundation." *Safety Science* 49 (2): 148-161.