Master's degree thesis

LOG950 Logistics

Mathematical Modelling of Safety Instrumented System for Pipeline Infrastructure Planning

Daria Golyzhnikova

Number of pages including this page: 123

Molde, 25.11.2016

Molde University College
Specialized University in Logistics

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: 25.11.2016

PREFACE

This master thesis is a final mandatory requirement for the Master of Science in Logistics Program in Molde University College – Specialized University in Logistics. The thesis addresses the domain of problems of petroleum production facility design and instrumentation network design for such facilities from the perspective of Safety Instrumented Systems.

The topic of the research project is "Mathematical Modelling of Safety Instrumented System for Pipeline Infrastructure Planning" and is written with provided data by Rosneft, one of the largest oil producing companies in Russia. The thesis is based on a literature study described in the project thesis and a case study of a Safety Instrumented System (SIS) design. It is assumed that the reader of this thesis has taken an introduction course in system reliability theory and risk management, or has similar knowledge.

The research project has been fulfilled under the guidance of supervisor Yury Redutskiy, and I would like to express my gratitude first and foremost to Yury Redutskiy for being my supervisor and for providing professional guidance, constructive feedback, valuable critique, comments and professional advices during the course of the thesis.

Furthermore, I would like to thank all professors from Molde University College for teaching and giving me competent knowledge for complex research and writing this master thesis. I would like to express my endless gratefulness to my family for all they are doing for me. Without your support I would not be where I am now. Your strength, encouragement, care and belief in me give me everlasting inspiration and motivation. And finally I would like express my gratitude goes to God, who bestowed upon me this opportunity to study at Molde University College and who guided all the way. "Except the Lord build the house, they labour in vain that build it". (Psalm 127:1).

A research proposal was presented and accepted in December 2015 and constituted the basis for this thesis. The work itself was performed from January through May 2016.

SUMMARY

The operation of many industrial processes involve inherent risks due to the presence of dangerous materials, gases and chemicals. Safety instrumented systems and their funtions are crucial to manage the risk in a lot of industries. There is therefore a demand for a detailed anasysis of the process course and facilities performance for the sake of identification and weighing of risks, hazards and benefits of the process outcomes.

There are millions of dollars in damages and economic losses every year in oil and gas companies, due to occurrence of dangerous toxic emissions, fire-ignitions and explosions. It is necessary for industry functioning to employ Safety Instrumented Systems (SIS), given the availability of a potential for probable damages. Such safety systems' goal is to ensure safe isolation and to maintain required protection functions for chemically hazardous materials, flammable liquids and potentially toxic gases in case of emergency event.

In land-based industry, as well as in offshore facilities, safety instrumented systems are employed for purpose to keep up the risk at tolerable level. The performance of the instrumented protective measures is crucial for achieving the necessary risk reduction. The Safety Instrumented Systems (SIS) are applied for safety functioning and ensuring that in case of hazardous event, for instance explosion, harm to personnel, machinery, processes or loss of expensive raw materials, the technological process have to be stopped within certain reasonable time. It should be obvious that a safety system, which will never failure, does not exist, however such systems should provide conditions as secure as they can possibly be. Safety Instrumented Systems (SIS) are purposefully developed for reducing the likelihood of emergency events and mitigating the severity of the identified accidents effects and they aim to prevent personnel from injuring, to protect the environment and to secure the necessary equipment for technological process.

The proposed research will contribute to the problem of instrumentation design for oil and gas industry. Many infrastructure planning projects lack comprehensive specification for safety system design, which leads to incidents and significant losses of various nature. The main objective of this research is to study the reliability assessment of SIS and implementation of optimization procedure to SIS design with respect to

economic efficiency and reliability of the system. This master thesis aims to develop a framework of economically efficient safety systems design based on mathematical modelling of those system and their interaction with hazardous industrial facilities.

A literature study of infrastructure planning in petroleum industry was carried out in order to describe organizational structure and related activities. Before implementing any operations, it is crucial to establish networks properly, where flow of materials and information will take place. Reliability theory was carried out in order to identify the main parameters of safety concept, their measuring and meaning. It is important to study different attributes of reliability concept before quantitative assessment. It is considered very significant to analyse the petroleum production infrastructure; analyse and assess risks and address the issues of mitigating those risks.

The risk management theory has become an essential part of infrastructure planning. The research project goals to develop and substantiate an approach for risk management, which can provide the company possibility to prevent hazards and eliminate expenses of accidents. The security system of the technological process becomes the most important tool for mitigating hazards and risks. Implementation of Safety Instrumented System as a layer of protection needs large amount of investment, approximately 80% of total investment. Deployment of the diagnostics and protection system for the pipeline involves investments into hardware, software and service work for installing and maintaining it, which implies a certain cost. However, this cost is not a fixed figure for a given pipeline. It highly depends on specific design of SIS is and how elaborate the diagnostics/protection system is, which is a managerial decision. Therefore, the purpose of research is to implement the procedure of selection the optimal safety system design with respect to economic criterion based on ALARP principle and achieve increases of reliability performance of pipelines together with risk reduction for the company.

A safety system model is to be described with qualitative and quantitative indices, recommended by the effective international standards. Decades ago, the Safety Instrumented Systems were constructed based on the German standards DIN V VDE 0801 and DIN V 19250 during several years before IEC standards came to be. Nowadays, IEC 61508 and IEC 61511 work as a basis for all operational security concerning systems with numerous electronic components, and electrical and programmable devices for any types of industry. These standards cover all safety systems related to

electronic basis of devices. In this research, detailed level of modelling has been achieved in the process modelling and optimization algorithms, where, in addition, the requirements of international standard (IEC 61508) have been incorporated.

The project implements optimization of safety-instrumented system design with the help of genetic algorithm in multi-objective application. This optimization is based on safety and reliability indicators along with lifecycle cost. System design problem also considers common cause failure, as well as accounting for dangerous detected failures and safe failures. The requirements for safety integrity are addressed in accordance with international standards IEC 61508 and IEC 61511, as well as the modelling details necessary for this research. The problem addresses the safety in parallel and series systems. The objectives to optimize are the average average probability of SIS's failure on demand, mean down time of the technological facility and lifecycle cost.

Novel contributions include implementation of modelling by Markov Analysis with flexibility for evaluation of multiple solutions; a model for quantification the reliability characteristics for each particular subsystem: average probability of failure on demand and downtime; and the integration of system modelling with optimization by multi-objective genetic algorithms with lifecycle cost assessment. Thus, this work intends to contribute to the state-of-the-art in modelling for a particular alternative of SIS specification and solution of multi-optimization of design and testing of safety systems with Genetic Algorithms based on principle of compromise between the costs of risk reduction and the achieved level of safety.

Table of Contents

LIST OF ACRONIMS AND ABBREVIATIONS

APCS	Automated Process Control System
CCF	Common Cause Failure Analysis
DD	Dangerous Detected failures
DDC	Dangerous Detected Common-cause failures
DDN	Dangerous Detected Normal (independent) failures
DF	Dangerous Failures
DT	Downtime
DU	Dangerous Undetected Failures
DUC	Dangerous Undetected Common-cause failures
DUN	Dangerous Undetected Normal (independent) failures
DVs	Decision Variables
ESD	Emergency Shutdown System
FMEDA	Failure Modes Effects and Diagnostic Analysis
FTA	Fault Tree Analysis
GA	Genetic Algorithm
MA	Markov Analysis
MOCO	Multi-objective Combinatorial Optimization
MOP	Multi-objective Problem
MILP	Mixed-integer linear programming
PES	Programmable Electronic Systems
PFDavg	Average Probability of Failure on Demand
PID	Proportional-integral-derivative controller
PLC	Programmable Logic Controller
RAMS	Reliability, Availability, Maintainability and Safety
RBD	Reliability Block Diagrams
SF	Safe failures
SIS	Safety Instrumented Systems
STR	Spurious Trip Rate
TMR	Triple Modular Redundant

LIST OF ORGANIZATIONS

ANSI/ISA	International Society of Automation
CCPS	Center for Chemical Process Safety. Safe and Reliable Instrumented Protective Systems
DIN	Deutsches Institut für Normung e.V. (English, the German Institute for Standardization)
IEC	International Electrotechnical Commission,
NTNU	The Norwegian University of Since and Technology
SINTEF	The Norwegian Foundation for Scientific and Industrial Research
UK HSE	Health and Safety Executive http://www.hse.gov.uk

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 Background

All technological processes in the oil and gas industry belong to the category of dangerous production processes. These processes are characterized by the fact that occurrence of incidents on the technological facilities can lead to the dangerous consequences: to injure the industrial personnel, the population of nearby regions and, of course, the environment. Emergency situations can also lead to destruction of the technological equipment and the production facilities themselves, which constitute significant economic losses. One of the key functions, implemented within each technological solution is protection against hazards and the dangerous consequences. This function is incorporated into an automated process control system (APCS).

A problem of safety on the hazardous industrial facilities has been paid much attention to. For many decades experts from various fields of science were engaged in this area. Statistics, provided by different sources, such as the International Association of Oil & Gas Producers, World Wildlife Fund and others [1], demonstrate that the disaster in the Gulf of Mexico is not an exceptional occurrence in hydrocarbon extraction practice. Since 1975 there were more than 60 major incidents on the offshore oil platforms all over the world, and even the relatively small-scale ones demanded enormous efforts for recovery. If we turn to the statistics for Russian oil and gas industry, we see that the Federal Environmental Industrial and Nuclear Supervision Service of Russia reports dozens of accidents happen in the oil and gas industry annually. According to their information, in 2012 eighteen accidents happened on hazardous industrial facilities of the oil and gas industry on the territory of the Russian Federation, and the reported damages for each accident can be up to several million dollars.

The causes of the incidents have been partially analysed by researchers and engineers. According to the information which is available in open access (HSE 2003), as well as (Fedorov 2008) many of the incidents could be avoided and severity of their

[1] examples can be found in:

Krasheninnikov et al. (2011); International Association of Oil & Gas Producers (2010).

consequences could be reduced if the technical requirements to the safety systems were developed adequately. The analysis of data in the sources reveal that nearly 50% of hazardous situations happen due to mistakes in the specification and design of the systems ensuring safety of technological processes (see Figure 1).

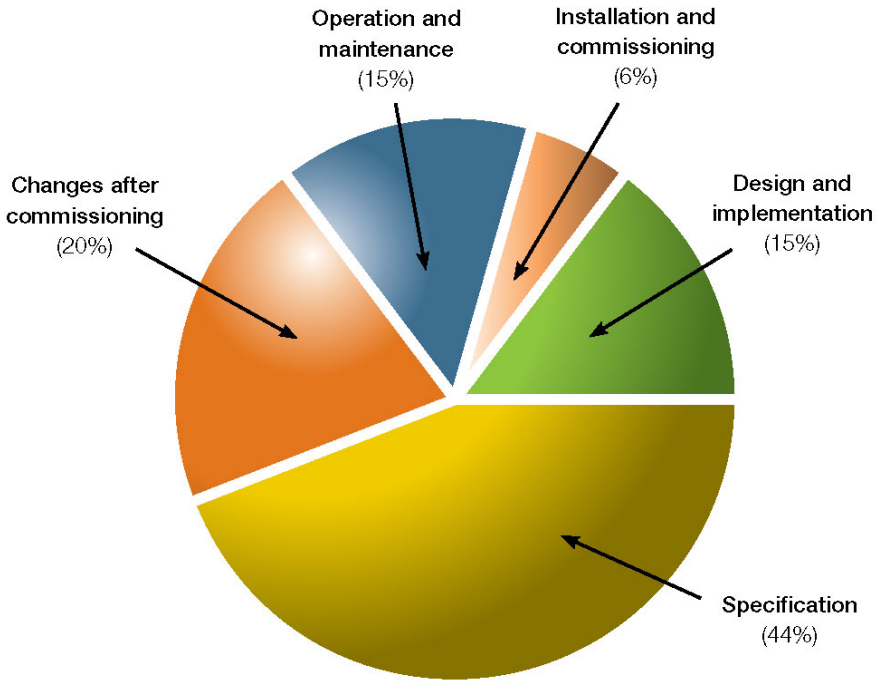

Figure 1. Primary causes of incidents in petroleum industry according to HSE "Out of control" (2003).

The problem of inadequate specification for the safety system design and their further implementation is especially critical for Russian energy industry. According to (Fedorov 2008), (Shershukova 2013a, 2013b), (Teluk and Shershukova 2011, 2012a, 2012b, 2012c, 2012d, 2012e) methods and techniques of risk analysis developed by the present time have been used only perfunctorily in the engineering and design of safety systems in Russian petroleum industry. Thus, we see that improving the level of safety for hazardous industrial facilities is a problem of significant importance.

1.2 Objectives of the Research

The main objective of this research is to develop a comprehensive approach to mathematical modelling of safety systems functioning for the purpose of optimizing the systems design from the reliability and economic perspectives.

In order to fulfil the set goal, we will take the following steps:

- The typical infrastructure for a petroleum production site will be analysed, which in terms of oil and gas business, is equivalent to infrastructure solutions for *upstream* and *midstream* sector [2].
- The safety systems, applied in petroleum industry will be analysed; the areas of responsibilities for the safety systems will be identified, as well as their particular structures, the structures of their subsystems, their behaviour and characteristics will be considered.
- An overview of research on the issues of designing the safety systems for oil and gas industry will be conducted. This overview will include the requirements to the safety systems, provided in the international standards, and the standards adapted for process industries in Russia.
- The theoretical background of the *reliability theory* will be provided, which is important for this research. This background will later be employed in the overview of mathematical modelling techniques, currently used for the purpose of safety systems design.
- A mathematical model of safety system's functioning will be proposed, and interaction of safety system with a technology, implemented and operated by a facility, or a unit, within a petroleum production process will be discribed. The model will consider a stochastic process of occurrence of failures and technology's critical modes. The issues of collecting and computing the data for this model will also be addressed.
- An optimization approach for obtaining the safety system's specification based on mathematical model of the safety system and the technologywill be investigated. The algorithm will incorporate the safety and reliability indicators, as well as the economic ones.
- The methodology of designing the safety systems, that is currently employed by petroleum engineering organizations in Russia, will be studied.
- A particular instance of safety system design based on a project of a field infrastructure development provided by Rosneft will be addressed. The

[2] definitions can be found in:

Bradley (1987); Macini and Mesini (2008); Schlumberger (2016).

documentation of the engineering project will be analysed, the stages of the project when the relevant decisions on safety system specification are made will be considered, as well as the safety requirements to the system, incorporated in the documentation and the assessment of safety system's performance provided within this project will be examined. Comparison of the results of implementing the technique, proposed in this research with the results of the methodology, currently used in Russian engineering practice will be presented.

- Finally, conclusions will be proposed and drawn graphically, also suggestions for further research on the addressed issues will be made.

1.3 Methodology of the Research

This research is conducted in the field of risk management. The methods and approaches within this field are conventionally divided into two groups: *risk assessment* techniques and *risk reduction* measures. The latter, in their turn, are represented by *hazard prevention* measures and *mitigation of consequences*. Elimination the hazardous scenarios of events is the first and most effective means of risk reduction. It is aimed at analysing the process and identifying the scenarios that may lead to hazards' occurrence for the purpose taking a preventive action, i.e. implementing a series of measures for avoiding the potential dangers, in the most severe cases the whole process can be stopped. The "barriers" responsible for mitigating the consequences are measures that take action after the hazardous event's occurrence. They are aimed at reducing the potential damage for such situations.

In this work we will address the issues of design for the systems aimed at preventing the hazards. The importance of the proper decisions on the design stage has been underlined earlier in this work. The systems aimed at mitigating the consequences of the hazards are not completely ignored in this work. This type of risk barriers involves various types of systems, some of which can be designed with application of exactly the same algorithmic approach that is proposed in this work. At the same time, there are barriers, for example, the evacuation procedures, that employ a different level of thinking and research in terms of design and implementation, and thus, in author's opinion, should be studies within a different research framework. Further in this work a few references to risk assessment techniques will be provided for the purpose of

evaluation of system's safety level with and without the safety system. This is done in order to evaluate the efficiency of the applied measures.

In this work we will be modelling functioning of a safety system and its interaction with the technology as a stochastic process. The thechnology we will address in the research is a part of oil and gas production infrastructure.

We can generally conclude that the research mainly involves quantitative methods and algorithms. The risk analysis leads to identifying the studied systems' safety level, which implies using the quantitative safety indicators, specified in international standards. Ultimately, the research project will result in suggestions for economically efficient safety system design, which implies runnung an optimization algorithm on a discrete set of elements.

In the researh we will use primary data – infrastructure project documentation, automation system deployment, risk assessment, reliability calculations. Besides, secondary data includes consideration of governmental regulations / industrial standards for pipeline systems construction and operations.

2 THEORY OVERVIEW

2.1 Infrastructure planning in petroleum industry

Before implementing any operations, the organizational structure must be designed first. In other words, the networks, where flow of materials and information will take place, should be properly established. The material flows take place between physical facilities, machines or units. Decisions regarding establishment of those networks are extremely important, because they represent most of capital expenditures (Baker, Croucher, and Rushton 2006).

Infrastructure planning is a problem that finds applications in many different environments and problem settings. When we're speaking of oil and gas production infrastructure, we imply a number of facilities and technological units, that are connected with short or long pipeline segments transporting the necessary raw materials and chemicals in order to produce petroleum and treat it for the purpose of further export (Restrepo, Simonoff and Zimmerman 2009). In general, the different types of infrastructure are named in accordance with the pipelines classification and they are divided in three categories depending on purpose: *Gathering lines and facilities:* Group of smaller interconnected pipelines forming complex networks with the purpose of bringing raw hydrocarbons or natural gas from several nearby wells to a treatment plant or processing facility. *Long-distance transportation lines and facilities* (export pipelines): Mainly long pipes with large diameters, moving products (oil, gas, refined products) between cities and countries. These transportation networks include several pump or compressor stations. *Distribution lines:* Composed of several interconnected pipelines with small diameters, used to take the products to the final consumer. Simplified diagram of petroleum industry infrastructure is given on the figure below.

Natural gas production, transmission, storage, and distribution system have different components. These components include production wells, gathering lines within the production fields, processing plants, transmission pipelines, compressor stations, pump stations and heaters (periodically placed along the transmission pipelines), storage wells and associated gathering pipelines, metering stations and city gate at distribution centers, distribution piping, and meters at distribution sites (residential or industrial). Along transmission pipeline there are normally a number of

other components and systems, including: pump stations, compressor stations, heaters, coolers and else. Hazardous liquid systems include production wells and gathering lines for crude oil production, processing plants, transmission pipelines, pump stations, valve and metering stations, and aboveground storage facilities.

The paper focuses on research problem considering infrastructure of gathering pipeline systems. Network are an estimated hundreds thousands miles of onshore "gathering" and "long-distance" pipelines, which transport products to processing facilities and larger pipelines. (GAO 2012)

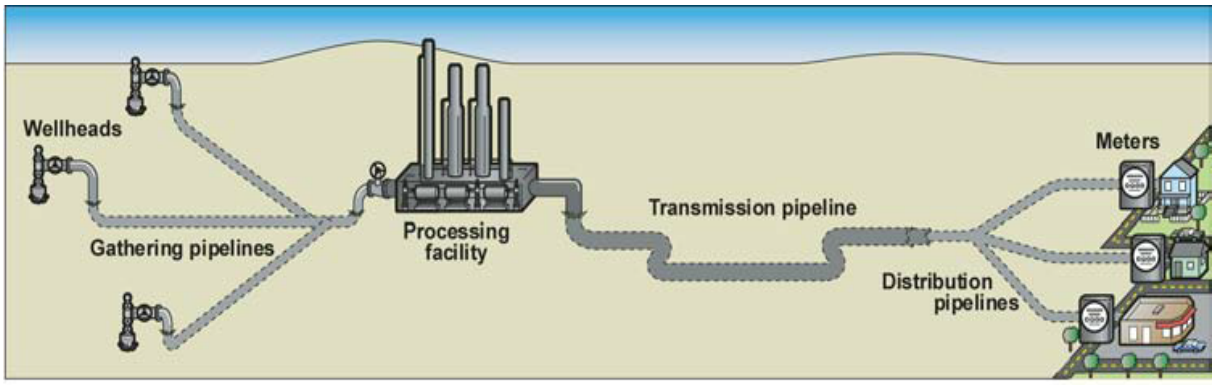

Figure 2. Three basic types of pipeline transport system.
Source PHMSA, Research & Development (2016).

Current research covers many aspects of the considered problem includes combining the infrastructure design, scheduling models, incorporating the consideration of uncertainties and potential hazards, implying moving into stochastic domain, which is more difficult but at the same time it would provide a more realistic view on problems (Gupta and Grossmann 2014).

Most of the decision regarding the petroleum production infrastructure planning are done on the design stage, when the efforts of building a particular solution for particular purposes are coordinated. The importance of decision-making on the design state is critical to the whole lifecycle of the process that the infrastructure is built for. For example, building a facility of a small operational capacity can result in a limit for further production processes, and thus, become an unnecessary constraint for petroleum production. Shortcoming of the safety decision, and the imperfection of the designed safety systems can result in significantly great losses due to the damages, and thus have a negative impact on company's revenues and its social stance.

Network design and infrastructure planning are significantly complicated problems for engineers. There has been a lot of research on the issue, many optimization models were developed and presented, many approaches for the investment and operations planning of oil and gas field infrastructure were suggested over the last 5 decades.

2.1.1 Oil and Gas Production Infrastructure Planning

Early developments in the area of infrastructure planning included the research on network design issues, most of which were presented as Linear Programs. The works (Lee and Aronofsky 1958) and (Aronofsky and Williams 1962) consider the scheduling problems for petroleum production. They used a simple linear reservoir model to describe the reservoir behaviour within the context of the oilfield investment and operation planning problem for the five deposits of petroleum and a gathering pipeline. In (Frair 1973) a mixed-integer linear programming (MILP) is used to solve the offshore oilfield infrastructure planning problem and crude-oil producing problems for the purpose of economic planning of coordinated operations. The linear interpolation is used for incorporating the non-linear model of the reservoir behaviour into the set of constraints. Those papers were obtained under curtain assumptions for the purpose of making the models computationally executable for that era of information technology. Later the problem was addressed by a number of researchers, among which is (Bohannon 1970), who formulated the LP models combined with data obtained from numerical reservoir simulation during the course of the development of the deposit. This approach involved several stages of modelling, resulting in construction of a new LP model incorporating the improved influence functions for economic-based criterion optimisation. (Sullivan 1982) and (Haugland, Hallefjord, and Asheim 1988) addressed the simultaneous optimization of the investment and operating decisions using MILP formulations with different levels of details. They investigated the problem of usage discrete (integer) variables resulting in Mixed-Integer Programming (MIP) models for improved representation of the non-linear decision variables by means of simplified representation of the reservoir parameters.

The amount of investment depends on the parameters of the system, including pipe diameter, thickness, pressure, length, and compression ratio. A large number of articles have tried to optimize this system from various aspects. Ruan and others

presented a mathematical model that took into account all of the parameters important to the amount of investment (Ruan et al. 2009). Based on the characteristics of networks system, optimization for investment becomes indispensable to networks design. A comprehensive and optimal mathematic model of a gas networks system is established. In that paper all the factors influencing the total investment of the networks system were considered and a comprehensive and optimal mathematic model of a networks system was established. From the point of the characteristics of a model comprising both continuous and discrete variables, a rank-optimization methodology was presented. To solve optimization of the mainline system in network, a simulation modelling approach was provided as an effective method in that paper.

Kabiriana and Hemmati presented a strategic planning model to determine the type, location, and installation schedule with a cost-minimization objective function (Kabirian and Hemmati 2007). They proposed an integrated nonlinear optimization model for design and development of pipeline networks problem. This model provides the best development plans for an existing network over a long-run planning horizon with least discounted operating and capital costs. To solve the model a heuristic random search optimization method was also developed. The authors showed in that paper that non-economic objectives may also be incorporated into model.

Cheboubaa and others proposed a metaheuristic algorithm called ant colony optimization to determine the number of compressor stations and the discharge pressure for each (Chebouba et al. 2009). The results were compared with those obtained by employing dynamic programming method. Proposed approach enables to design a fast, effective and robust decision aid tool based on the suggested method. That tool suggests the most appropriate decision to operators within a short time.

One of the first researches, that proposed a model which includes both fiscal rules and endogenous (geophysical) uncertainty in the field parameters, was conducted by Vijay Gupta and Ignacio E. Grossmann (2014). Their approach considered both of these complexities/parameters in an efficient manner. In that paper, the authors deeply examine the life cycle of a typical offshore oilfield project. The oil and gas project consists of the following five steps: a) exploration, b) appraisal, c) development, d) production and e abandonment. The most of the critical investments are usually associated with the development-planning phase of the project. Therefore, it is very important to focus on the key strategic/tactical decisions during this phase of the

project. Moreover, optimal investment and operating decisions are essential for cost-savings problem to ensure the highest return on the investments over the time horizon considered. Vijay Gupta and Ignacio E. Grossmann (2014) proposed the mathematical modelling for optimization and planning investments and operation activities. The paper provides multistage stochastic programming approach for offshore oilfield infrastructure planning.

2.1.2 Overview of Safety Issues for Infrastructure Planning

Every construction activity in pipeline construction projects, particularly large projects, attracts risk in some respect. Risk management is a complicated and crucial tool for the modern technological processes. In particular, in a situation such as the pre-contracting stage, in which there are numerous uncertainties that should be considered but there is not currently enough detailed information available, identifying the vital risks in a new environment is extremely important. An effective risk management method can help in understanding not only what kinds of risks are faced, but also how to manage these risks at the stages of contracting and construction. (Zhi 1995).

A simple, common and systematic approach to risk management, suggested by Berkely and others (Berkeley, Humphreys and Thomas 1995), has four distinct stages: (I) risk classification, (II) risk identification, (III) risk assessment, and (IV) risk response. In the first stage, risks should be classified into different groups with certain criteria in order to clarify the relationships between them. The second stage entails the identification of the risks pertaining to risk management. The third stage is to assess and evaluate the effects of these risks. In the final stage, appropriate risk response policies should be developed to reduce and control the risks.

The lack of accessible guidance with respect to conducting pipeline risk assessments creates a situation where it is critical that pipeline operators readily assess their systems in a transparent manner and be in a position to share this information when needed. This way, local governments can be provided with appropriate information for land use planning purposes allowing for informed and balanced decision making. Risk can be defined as the product of the likelihood of an event and its consequence (Henselwood and Phillips 2006).

The existing method of pipeline health monitoring, which requires an entire pipeline to be inspected periodically, is both time-wasting and expensive. This issue was

also considered by P. K. Dey, who developed and proposed the risk-oriented model for monitoring. A risk-based model aimed at optimizing the inspection time has been presented. The model proved to reduce the cost of maintaining petroleum pipelines, and also suggested an efficient design and operation "philosophy": construction methodology and logical insurances plans. The risk-based model uses Analytic Hierarchy Process, a multiple attribute decision-making technique, to identify the factors that influence failure on specific segments and analyses their effects by determining probability of risk factors. (Dey 2001)

Important component of contemporary industrial applications employed in many industry sectors is long-distance transportation of liquids and gases via transmission pipelines. Pipeline incidents are the prime source of danger for successful delivery of hazardous materials. Example of such incidents can be loss of pipeline integrity and release of hazardous substances to the environment. According to Dziubinski, Fratczaka and Markowski (2006), the level of risk involved in operating large and condense-located production facilities is roughly similar to those of sparsely located pipeline facilities and units, according to the statistics that the authors examine. The authors also point out that despite the statistics, pipeline transportation systems are often considered to be the safest in the industry.

For the purpose of analysing risks and assessment of level of hazardous risk, three methods can be perform: (I) quantitative, (II) semi-quantitative and (III) qualitative. The second ones are used in order to identify accidents and to figure out the possibilities of failure occurrence. The results of semi-quantitative methods provide an easy and useful approach for level of risks identification, since they are presented in the form corresponding to categories of risk form. The main objective of qualitative methods is to confirm the relevance of a safety level deemed acceptable by the given norms, which are described in standards and legislation. Such documentation is most often provided for each device separately and it contains the information about minimum safety requirements for component. Such indespesable requirements must be fulfilled in order to achive a certain reasonable level of safety. Nevertheless, there are usually other requirements for pipelines speading across long distances, thus the so-called probabilistic methods are often applied. These approaches based on the concept of risk constitute to quantitative techniques of risk assessment. The comprehensive varieties of computational and analytical methods represent the quantitative risk assessment. This method is employed in many stochastic models, particularly while

analysing the physical phenomena. Conducting such complex analysis of risk is a sophisticated task. Arendt and Lorenzo (2000) point out that such assessment of selected objects requests certain specialized software, such as PHAST, EFFECT, SAFETI. Moreover, knowledge of theory and experience in practice are mandatory for correct results interpretation of similar problems (Arendt and Lorenzo 2000).

Consideration of the causes and consequences of the hazardous event in long and spread pipeline systems is very essential for analysing accidents and examinations of reasons that can lead to accidental release of dangerous liquids. Knowledge about the relation between diverse reasons for pipeline problems, breakdowns and associated with them consequential mitigating measures contribute a substantial input into risk management activities for critical infrastructure systems.

Researchers Restrepo, Simonoff, and Zimmerman (2009) focus on consequences of process interruptions, their causes and various costs and losses associated with these pipeline accidents. The authors examined different economic consequence measures associated with costs of accidents: the value of the production losses; public and private property damage; clean-up, recovery and other costs. For the purpose of determination what factors, circumstances are relared to nonzero product loss cost, nonzero property damage cost and nonzero clean-up and recovery costs, the logistic regression modelling is employed by authors. (Restrepo, Simonoff, and Zimmerman 2009).

The scale of consequences such as property damage, value of product lost, clean-up and recovery costs are greatly determined by cause of hazardous event and other accident characteristics. Application models for safety systems, design of protection systems applies in risk management comprise an important analytical tool for industry functioning. The decision-makers can use such tools in order to forecast and estimate the possible consequences of hazardous event in pipeline systems by causes of accident (and other characteristics) and then to allocate resources for maintenance and to reduce risk factors in pipeline systems.

As it becomes clear, the scope of safety issues relevant to the projects in oil and gas industry is very broad. However, it is obvious that most of the important decision in the sphere of Risk Management are made during the early stages of a particular project: most of them have to be done on initiation and planning phases of the project.

Further the overview of the risk-related issues, covered by the safety systems, will be conducted.

2.2 Overview of the Basic Concepts of Reliability Theory

2.2.1 Modelling of Reliability Characteristics of One Device

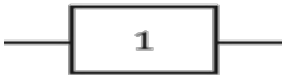

Figure 3. One device/component represented with reliability block diagram (RBD). Main principles of RBD and examples of the diagrams can be found in Goble (1998), Lewis (1996), IEC 61508 (1998-2005) and other resources.

Any device can fail and probability of those failure is stochastic value. At any time, device can be in one of two states: working condition or failure.

$$R(t) + F(t) = 1 \qquad (1)$$

where *R(t)* is reliability (probability of the device working), *F(t)* is the probability of failure of the device.

In addition to consideration of probability of failure, failure rate is often used.

$$\lambda(t) = \frac{F'(t)}{R(t)} \qquad (2)$$

On the curve below, the behaviour of the failure rate of any device during long working period is described. Graphically three periods of the failure rate behaviour is demonstrated in Figure 4. First period ("burn-in") and last one ("wear-out") are characterized by volatile value of failure rate, decreasing in first case over the operating time since start, and increasing in wear-out zone due to the items ageing. In this work the useful life time will be considered. This period characterized by practically constant failure rate of device.

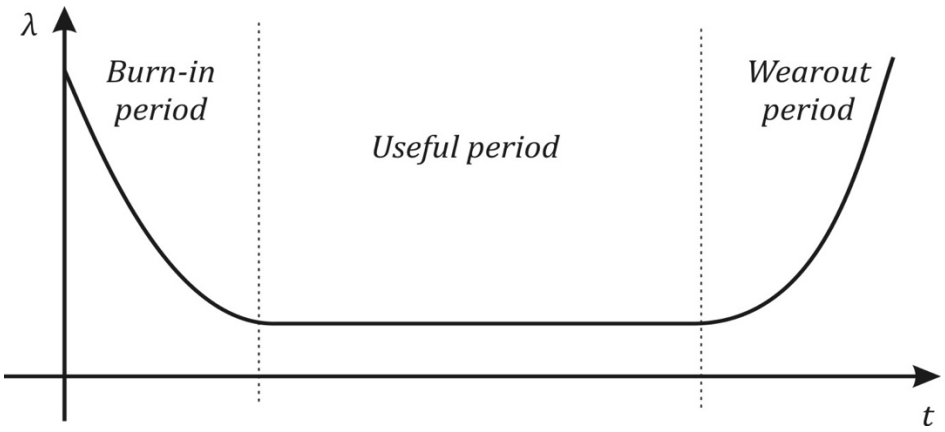

Figure 4. Failure rate over lifecycle (Lewis, 1996).

In this research, complex system will be addressed. For such systems constant failure rate is usually assumed (Goble et al. 1998). As a result of this assumption probability of failure is determined by the exponential distribution:

$$F(t) = 1 - e^{-\lambda t}, \quad (3)$$

If further very small values of λ are assumed ($\lambda \ll 0{,}01$), therefore probability of failure can be describes as following:

$$F(t) \approx \lambda t. \quad (4)$$

- **Diagnostic Coverage**

As a rule, modern devices implemented in safety systems have built-in diagnostics. Therefore, the systems for automatic detection will detect some of failures, but other failures will go undetected. The percentage of detected failure by the diagnostic mechanism called the diagnostic coverage ε (CCPS, 2007). Therefore, in application to failure rates, we obtain:

The fraction of the total failure rate that can be detected:

$$\lambda^{detected} = \varepsilon \cdot \lambda^{total} \quad (5)$$

All the rest failures are undetected by the diagnostics:

$$\lambda^{undetected} = (1 - \varepsilon) \cdot \lambda^{total}. \quad (6)$$

- **Spurious Tripping Rate**

Failures can be not only detected and undetected, they also are divided into dangerous failures and spurious trips (ST). The safety systems have their own advantages and disadvantages. The purpose of such systems is to deal with incidents

and decrease risks of harm, which corresponds to the benefits. On the other hand, the safety systems have negative impact on the technology by spuriously activating without any real reason for that (Hauge et al., 2006a).

Further in this work, dangerous failures for one device will be lettered λ, and spurious trip rate - λ^S.

- **Data procurement of the reliability parameters for each device**

The documentation for the devices (sensors, logic solvers, and final control elements) for safety system provided information on the parameters of the items. This more detailed information is required to further design of the project and assessment of reliability parameters of the safety system. The required information about the devices is provided by the manufacturer in the form of the three following parameters:

  - average time until dangerous failure
  - average time until spurious trip
  - diagnostic coverage (%)

In the device documentation, diagnostic coverage is expressed in percentage, which is convenient for further calculations. However, the first two parameters (average time until dangerous failure, average time until spurious trip) are presented as time measurements. Given the fact that the assumption of exponential distribution has been accepted, the calculations of the failure rates for the parameters can now be made based on average time measures until the event of the failure. The computations are made according to the formulas below.

The dangerous failure rate is obtained as:

$$\lambda^{danger} = \frac{1}{T_{avg}^{danger}},$$

The spurious tripping rate is found as:

$$\lambda^S = \frac{1}{T_{avg}^{ST}}.$$

2.2.2 Reliability of Complex Systems

The reliability characteristics of the system depends on its particular structure. There are different forms of system structuring, for instances series or parallel (the most basic structures), or another k-out-of-n structure. Applying Reliability Block Diagrams (RBD) gives the opportunity to determine reliability quantification for system.

It is a method that illustrates conveniently simple structures. Other methods of illustrating structures of the system are more more suitable for more complex ones.

Reliability Block Diagrams reveals the functional connections of the elements, describes the structures of the system necessary for the system to operate. One component in the system is represented by each square block in Figure 5. The basics system structures with three items shown in the illustration of the RBDs below:

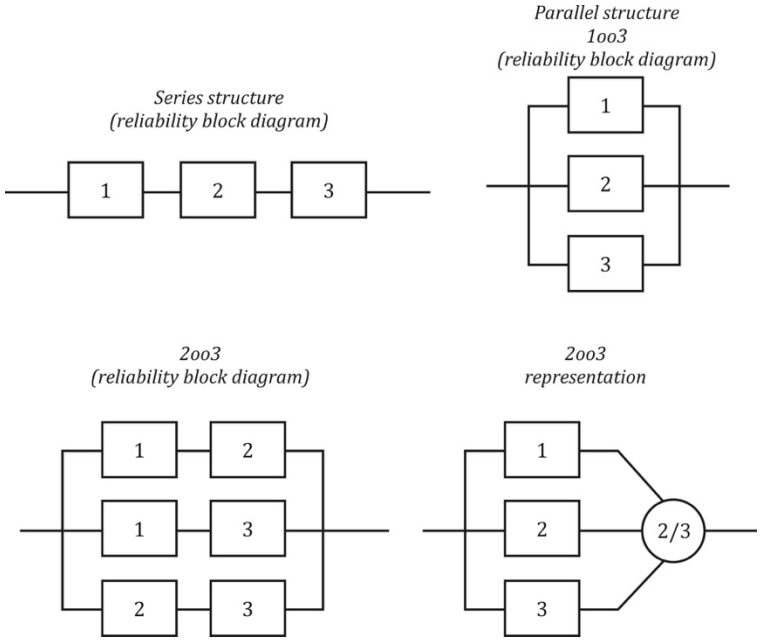

Figure 5. Basic systems structures. The standard examples can be found in Goble (1998), Lewis (1996), IEC 61508 (1998-2005) and other resources.

Thus, the Reliability Block Diagrams helps to define reliability characteristics of those structures. Reliability of each device of the system is denoted by R_i.

For series architecture of the safety system, the reliability is defined as:

$$R_{sys} = \prod_{i=1}^{N} R_i. \qquad (7)$$

For parallel structure, the reliability of the system is computed as following:

$$R_{sys} = 1 - \prod_{i=1}^{N}(1 - R_i). \quad (8)$$

For general case of safety system with *KooN* architecture, the reliability is calculated as (Lewis, 1996):

$$R_{sys} = \sum_{i=K}^{N} \binom{N}{i} \cdot R^i \cdot (1 - R)^{n-1}. \quad (9)$$

Many technical systems or subsystems have *k-out-of-n* structure, which consist of *n* identical components. This system configuration is a particular instance of a series-parallel redundancy (in terms of reliability block diagrams). There are two types of k-out-of-n structure. If in order to be in operating mode, the system requires at least *k* items succeed out of the total *n* parallel components, it is defined as so called a *k-out-of-n*: G system. If the entire system fails, in case of at least *k* of the *n* components do not functioning, it is called a k-out-of-n: F system.

The consideration of *k-out-of-n* structure is not limited only as a special case of parallel redundancy as it was classified above, the *k-out-of-n* configuration can also be examined from other points of view. Both parallel and series system structures are special cases of the *k-out-of-n* system. As long as the amount of components needed for keeping up the system to properly function reach the total number of items in the whole system, the description of the system's behavior represent the series configuration. Thus, when the amount of components necessary for system to be in operating mode is equal to the number of items in the entire system, it is defined as series system. Namely, a series system of statistically independent components is an *n-out-of-n*: G system or an *1-out-of-n*: F system. While a parallel system of statistically independent items is equivalent to a *1-out-of-n*: G system and to an *n-out-of-n*: F system (Kuo and Zuo 2003).

A *M-out-of-N* structure implies proper system function if at least *M* of any *N* components that comprise the system are in proper operating condition (*k-out-of-n*: G system described above). In other words, the entire system is working if and only if at least *M* of its *N* components are operating. It fails if *N – M + 1* or more components fail. Hence, a *M-out-of-N* system become inopearble at the same time when the $(M - N + 1)^{th}$ component failure (Cramer and Kamps).

Example. 1-out-of-4 structure: For example, examine distribution link in pipeline with four valves. Additionally, to pipeline falicilty design includes the following requirement for the facility to keep the integrity of the transportation link. Distribution station design makes it possible to properly and safely operate if at least one safety valve is properly functioning ensuring the structural integrity of the transportation system. This means that the safety valves form in a k-out-of-n architecture in the sence of safety system's reliability, and M = 1 and N = 4. In other words, they work in a 1-out-of-4 redundancy configuration.

Example: 2-out-of-3 structure: For example, consider a natural gas metering station with three identical meters, computing the amount of gas flowing through the station. The meters operate simultaneously. The measurements of the three devices are transmitted to the operator's workstation where they are compared, and in if two or three of measurements are similar, then outcome is considered valid. This is also sometimes called a majority vote system, and in this case only one meter is allowed to fail without resulting in the failure of the entire measurement system. In other words, this is a system with 2-out-of-3 redundancy configuration.

- **Common Cause Failure**

The failure of the complex safety system can be due to common cause failure or independent failures of devices. Thus, if failure several elements, these failures of items can be dependent or independent. The failure of more than one device as a result of the same event is called Common Cause Failure (CCF) (Goble and Brombacher 1999).

The fraction of the total failure rate that can be impute to a common stress represented as following:

$$\lambda^{CCF} = \beta \cdot \lambda^{total}. \qquad (10)$$

where λ^{CCF} is a percentage of failures due to common cause in total failures, and β is common cause failure factor.

- **Downtime**

The time during which the system is unavailable or the devices can not be used is called downtime. This period is characterized by inoperable condition of the items or unavailability of the entire system with several elements. It therefore splits the total

downtime period between two contributed reasons for unavailable system: dangerous failures and spurious trips. Downtime of the system is determined as following:

$$DT = \int_0^T \left(1 - e^{-\lambda^{dangerous} \cdot t}\right) dt + \int_0^T \left(1 - e^{-\lambda^{s} \cdot t}\right) dt \qquad (11)$$

2.2.3 Classification of Failures

It is very important to clarify the different failures that can take place in the system.

All the failures of the ESD can be either *dangerous failures* or *safe failures*. IEC 6108 gives the following definition of dangerous failures: they are failures that "put the safety-related system in a hazardous or fail-to-function state''. In other words, dangerous failures prevent the safety system from implementing its function when it is required to do so. Safe failures on the other hand do not threat the safety system's capabilities to perform when needed. What those failures imply is that the system begins taking action without any actual demand; and as a result we observe spurious tripping of the safety system. The dangerous failures contribute to the indicator called the *probability of failure on demand*, whereas the safe failures contribute to the another indicator called *spurious tripping rate* (STR) of the system.

If we think in terms of the interaction between the technology and the safety system, deployed for ensuring the safety of the process, then a good illustration of the generalized classification can be represented by the figure below, where the process of technological incidents occurring is depicted to split into the "stop"-command generation by SIS, and the process of failures to implement the safety function. The SIS itself is generating the process of spurious tripping events.

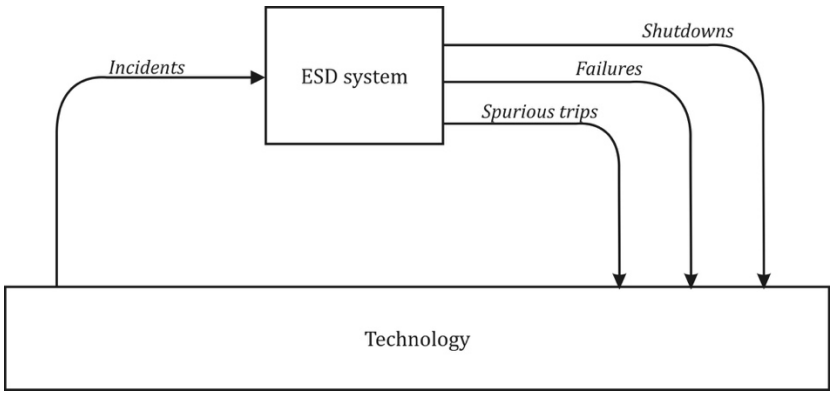

Figure 6. The representation of risk classification used in this research.

Besides the division of failures to dangerous and safe, we can consider other approaches to the classification. The diagnostics that are built-in to SIS divide the failures into

- *detected failures* – those that are revealed by the diagnostic function, and
- *undetected failures* which are not revealed by the self-diagnostic subsystem.

The detected failures are considered to be fixed as soon as possible, when the diagnostic system signals the failure. The undetected failures are not fixed right away. Such failures are revealed during the proof testing procedures, that happen periodically.

From the perspective of the cause for any particular failure, we can speak of the *independent failures* of the components, and the *failures due to the common-cause*.

In this research we will consider the classification of failures, represented on the figure below.

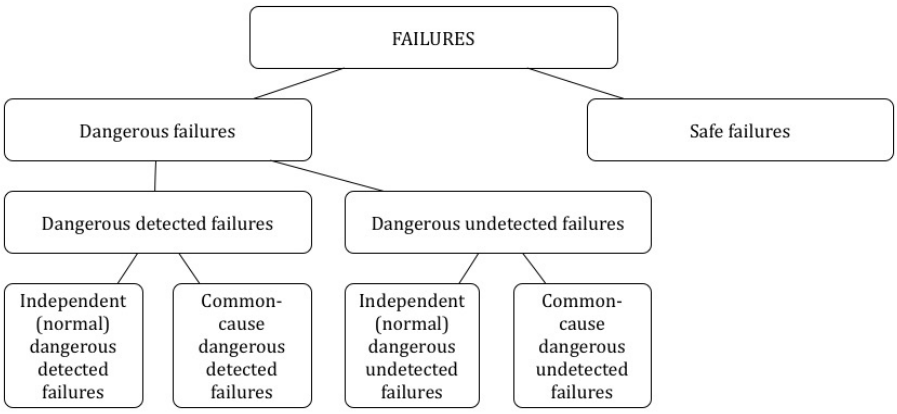

Figure 7. The classification of risks adapted for the research.

The provided classification is described by the following relations between the failure rates:

$$\lambda = \lambda^{DDN} + \lambda^{DDC} + \lambda^{DUN} + \lambda^{DUC} + \lambda^{ST}. \quad (12)$$

- **Probability of Failure on Demand**

Probability of failure on demand (PFD) is a measure of unavailability of the safety system for performing its function when it's required to. So, we see that it's a measure of decrease in safety (Hauge et al. 2006a). It is a highly important safety indicator and this indicator will be one of those used in this work. It is crucial to clarify that PFD does not in any way incorporate to the probability of the system's failure caused by the inquiry for being (unwantedly) actuated by itself. Only the failures that initiate the demand for the whole system's function contribute to PFD.

$$PFD = \mathrm{P}\,(\mathcal{J}|\mathcal{F}), \quad (13)$$

where $\mathcal{J}$ is the probabilistic notation of the event of technological incident, and $\mathcal{F}$ is the notation for the event of dangerous failure occurrence. Further in the text the technological incident will be described by the rate of the incidents d^t.

PFD will be calculated as a result od complex Markov modelling further in the work. A comprehensive classification of failures was presented above, in the context of safety systems description in application to petroleum industry.

Since probabilities considered in this work are time dependent, it follows that the *PFD* is a function of time. Fixing the time interval at a certain value *TI* (test interval), the average value of *PFD* is over a defined time interval *TI* as following:

$$PFD_{avg} = \frac{1}{TI}\int_0^{TI} PFD(t)dt. \quad (14)$$

2.3 Risk Management in Petroleum Industry

2.3.1 General Description of the Systems

Processes inherent in modern technology are highly complex, and, as a result, in case of emergency situations there can be dangerous consequences. In particular, the

hazardous situations can occur as a result of a certain technological parameter's deviation from its nominal values. Among other potential reasons for hazards we can mention earthquakes, natural disaster and other external disturbances, which can cause the destruction of the technological equipment.

A process plant usually has several layers of risk reduction. A layer of risk reduction is a measure put in place as a "defence", or a "barrier" to reduce the risk the facility is exposed to. The functions of those layers are executed in a hierarchical, or stated another way, in a consequential way. The main idea of the way to risk reduction layers structuring is to maintain the secure state, safe condition of the factory, in case if the previous protection barrier has failed to do so. It is worth mentioning that each particular solution for each particular facility, or a part of the technology requires a specific solution, however the generalized representation of risk reduction layers and their generic responsibilities is given below in Figure 8. Among those layers are:

- the Automated Process Control System (APCS) – this is a basic system that control over the technology, it intends to keep the parameters within the tolerable ranges so that the necessary quality of produced flows would be ensured.
- the Emergency Shutdown (ESD) system – this is also an automated control system, however its only function is to shutdown the technology when one or more critical parameters move into the range of critical values.
- the Fire and Gas (F&G) detection system– this is an automated system, that alarms the personnel about the fire or the excess of gas concentration on the atmosphere, so that the evacuation procedure would begin
- the active fire protection systems– this is an automated system that is run for the purpose of extinguishing the fire, in case it started.
- the additional measures in case of emergencies, the evacuation plan, and so on.

These protection layers usually would take action in the mentioned order.

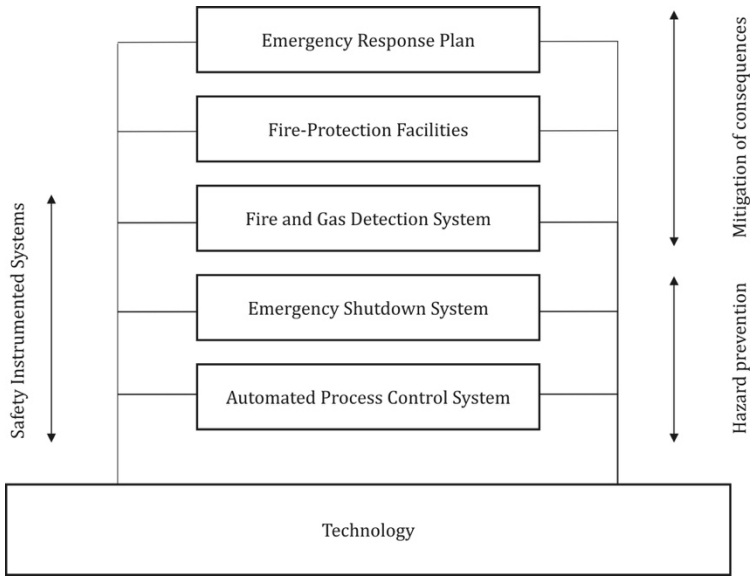

Figure 8. Position of SIS with the plant protection layers.
Source ABB "Best practices for avoiding common cause failure and preventing cyber security attacks in Safety systems" (2012).

As a result of contact with dangerous chemical liquids and toxic gases, the operations in oil and gas industries or industries related to chemical process become very risky and hazardous. Due to this fact the Safety Instrumented System (SIS) are purposefully developed for reducing the probability of emergency events and mitigating the affects of severity of identified accidents. The main target of such designed applications, as a SIS, is to prevent personnel from injuring, to protect the environment and to secure the necessary equipment for technological process.

Oil and gas industrial processes have quite hazardous technological processes, these industry sectors are exposed to dangerous toxic emissions, fire-ignitions and explosions. Due to this fact, there are millions of dollars of damages and economic losses every year in oil and gas companies. It is essential for industry functioning to apply Safety Instrumented Systems (SIS), given the presence of a potential for probable damages. Such safety systems aim to ensure safe isolation and to provide required protection functions for chemically hazardous materials, flammable liquids and potentially toxic gases in case of accidental release of fluids or any emergency event.

The inability to prevent risks to the systems' safety integrity, and respectively the failure to cope with these risks or mitigate the consequences from accidents, can lead to significant amount of expenses, losses of both economic and human: this is reflected in loss of the assets of a company, costs of damaged facilities, widespread

damage to the environment, harm to personnel and people around the facilities, and even loss of life.

Safety Instrumented Systems play a vital role in providing the protective layer functionality in many industrial process and automation systems. Process facilities (e.g., petrochemical plants) should be equipped with safety instrumented systems (SIS) to complement their process control systems. A safety instrumented system is a tool for ensuring functional safety, when safety is achieved by means of the correct operation of a system or equipment.

A SIS is utilized when the risk of an accident needs to be reduced. SIS is defined by ISA S84.01 and IEC 61508 as:

- SIS loop: "An SIS is a distinct, reliable system used to safeguard a process to prevent a catastrophic release of toxic, flammable, or explosive chemicals."
- SIS loop scope: "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."

Each device in the control loop is implementing a safety instrumented function, must be adressed while cunducting analysis of the safety systems. SIS includes sensors of level, flow, temperature and pressure, a programmable logic controlers, regulating and safety valves, pump drives and other final control equipment.

Sensors implement the safety function of monitoring potentially hazardouys scenarios in the course of the process (i.e. process demands), controlers' function is to implement a safety algorithm, and the actuators' safety function is to take the necessary action in case of an emergency (Honeywell 2002).

A SIS has the objective of detecting and preventing plant hazardous conditions, which could develop into catastrophic events. If they were not mitigated catastrophic events could have consequences such as loss of assets and production, widespread damage to the environment and loss of life. Gruhn & Cheddie (1998) give another definition: 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".

A safety instrumented system (SIS) is a specially engineered system that implements the necessary protective functions, which are required to reach and maintain safe conditions for equipment and keep the secure state of the facilities. There are different types of SISs, which are often applied in the process industry. For instance, such typical terms for Safety instrumented system are emergency shutdown systems (ESD), safety shutdown systems (SSD) and safety interlock systems. Although SISs can be implemented for some applications for mitigating of hazardous consequences, such as fire and gas detection (F&G). Safety instrumented system by their definition given in IEC61508 are employed to perform one or more safety instrumented functions. Each safety function, which a SISs implements, has a specified safety integrity level, this particularized level is required to obtain functional safety. Safety functions are usually implemented for low-demand mode of operations (i.e. they are in standby and operate only as a response of a demand, not continuously), with their architectures limited to a few practical options (Torres-Echeverria 2009).

The general structure of any safety instrumentation system can be represented by a control loop, depicted in Figure 9.

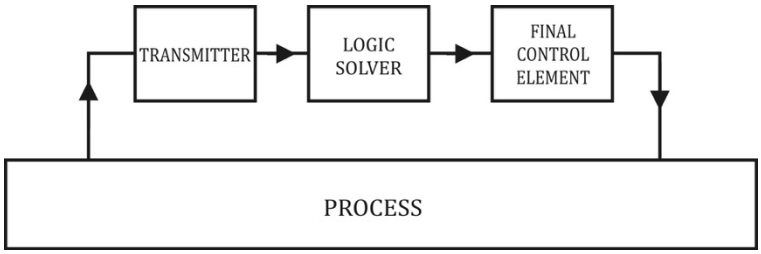

Figure 9. Structure of one control loop of SIS (IEC 61508, 1998-2005).

Process value transmitters are basically sensors perform monitoring process values of technological parameters. Most of the measured parameters are pressure, temperature, level, flow rate and concentration. *Logic solver* is a programmable logical controller (PLC), which receives the signals from the transmitters/sensors, and, in its turn, according to the programmed control algorithm, generates an output control signal to actuators. The latter represent the *final control elements*, which directly affect the process by assigning the operating modes to the production units, open or close valves, start or stop pumps and compressors. Process control system uses discreet (interlock subsystem within DCS; ESD system) and continuous (proportional-integral-derivative, or PID) control algorithms. The final element subsystem doesn't necessarily consist of

only technological equipment, for example, in Fire and Gas systems the final elements come in the form of alarms.

Now let's turn to the characteristics of the technology itself. Generally speaking, at any given point of time, any parameter can be in one of the value ranges, depicted in Figure 10. If the considered parameter is in the area of precarious values, then DCS starts using control algorithms and alarms in order to return the parameter the range of nominal values. If DCS fails, the parameter transitions to the critical values range; in this case ESD system initiates the stop of technological process. In case ESD fails, parameter enters the range of prohibited values; further risk-reduction layers should be activated.

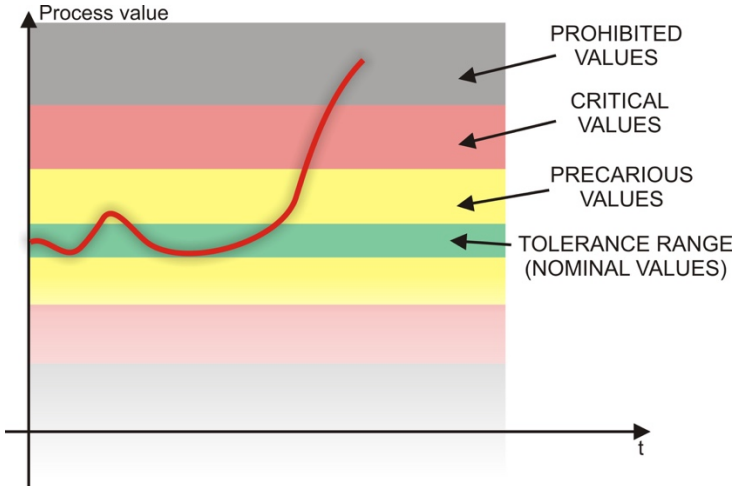

Figure 10. Ranges of DCS and ESD responsibility. Source ABB "Best practices for avoiding common cause failure and preventing cyber security attacks in Safety systems" (2012).

The ranges are usually defined as the following thresholds:

L (or Lo) – the low threshold of beginning of the precarious region.

LL (or LoLo) – the low threshold of beginning of the critical region.

H (or Hi) – the high threshold of beginning of the precarious region.

HH (or HiHi) – the high threshold of beginning of the critical region.

The particular value ranges for each area on Figure 10 are established by the technology engineers and are based on the characteristics of the process, of the equipment and of the parameter itself. For example, pressure, unlike temperature, can change quickly over time, almost abruptly, and project engineers consider this specificity when they determine the range of the parameter's fluctuation.

Let us point out some observations, which are important for further considerations of the safety issues and modelling the system's performance.

We can see, that the continuity of the processes inherent in the petroleum production industry obliges occurrence of an incident to be represented by the process value passing through the critical area. This is considered to be one of the main features of technological processes in petroleum industry. Its importance is due to the fact that role of ESD as a barrier for risk-reduction becomes obvious: by reducing the frequency of a parameter's achieving the values within its critical range, the probability hazards' occurrence decreases and so does the severity of the consequences.

We also make an assumption for the considered processes that the accidents, that might occur can't lead to mass mortality of people, due to the hazardous industrial facilities, included in the infrastructure under the development, are located on the isolated territory with protection zone.

Processes are continuous in time, i.e. any interruption of the technological process can lead to certain dangerous consequences, for example, to losses of production. At the same time these processes have a considerable volume of controlled, measured and registered technological parameters. In particular, a total number of such parameters for one oil or gas field can be 8 000 – 12 000.

The consequences of hazardous situations can vary greatly. Among such consequences, for example, are violations of product quality at the output of the facilities. There could be more serious consequences, in particular, explosions, which can cause not only destruction of the equipment, but also death of personnel member. Even though the former might seem insignificant in comparison to the latter from the safety point of view, in fact, any dangerous consequences influence an outcome of the production, so the losses to the company operating a particular field and the hydrocarbons treatment infrastructure, can be accumulated over time, and as a result be just as significant as any other hazardous event. Therefore, it is very important to estimate all dangerous consequences at the design stage, and to classify them according to the specification of the safety standards.

2.3.2 Standards for Safety

2.3.2.1 Evolution of International Standards

In the 1980s and before that, the companies were responsible for managing the safety issues of their operations themselves. The largest companies eventually introduced some common guidelines that with time were included and generalized into industrial guidelines and standards. Since that time great effort has been put into developing the National standards within many countries, the European standards and International standards for engineering and process control. In the early 1980s the International Electrotechnical Commission (IEC) and the German Institute of Standardization (DIN) investigated the fundamental requirements for protective systems using measurement and control techniques.

Among earliest known standards to cover the safety issues are two German standards (German Institute of Standardization (DIN)):

DIN V 19250:1989-01 - Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen (Basic safety issues for control and instrumentation protective devices. Berlin, 1994) and

DIN V VDE 0801:1990-01 - Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben (Basic rules for computers in systems with safety-related tasks. Berlin, 1990).

The IEC was mainly concerned with computer processors technology. DIN was concerned with risk assessment (DIN V 19250), the general requirements for safety devices (DIN V 19251) and computers in systems with safety functions (DIN V VDE 0801). In 1989, these German standards were integrated into the European standards, e. g. the EN 1050 for risk assessment and the EN 954-1 in scalable requirements for safety-relevant controller components.

EN 954 was developed in parallel with DIN V 19250. It addresses (on the basis of DIN V VDE 0801) microprocessor-based systems and a modified version of this specification has been adopted as a safety standard for factory automation. Certification of a system to DIN V 19250 and DIN V 19251 along with DIN V VDE 0801 therefore provided qualitative but not quantitative verification. Clarification was still required for assessing residual risk.

The Safety Instrumented Systems were constructed based on the German standards (DIN V VDE 0801 and DIN V 19250) for several years before IEC standards. These German standards were approved by the global safety community for years, and after that these standards provoked the attempts to establish another global standard.

Another relevant standard in their evolution is ISA[3] S84.01-1996 "Application of Safety Instrumented Systems for the Process Industries". This one was developed and applied in the USA since 1996.

Finally, in the late 1990s – early 2000s, the International Electrotechnical Commission (IEC) generalized all the previously available expertise in the form of the standards on functional safety that are now relevant to oil and gas sector.

- IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems; and
- IEC 61511 Functional Safety: Safety Instrumented Systems for the Process Industry Sector.

Nowadays these safety standards work as a foundation for all operational security concerning systems with many electronic components, and electrical and programmable devices for any kind of industry (IEC 61508, 1995-2010). These standards cover all safety systems related to electronic basis of devices.

The International standards (IEC 61508 and IEC 61511) methodically deal with the whole life cycle activities of a Safety Instrumented System's (SIS). These standards are oriented on the necessary system performance, required operating capabilities from the safety system. Namely, it is up to the managers to make the structural redundancy decisions and choose the testing interval, as long as the predetermined *safety integrity level* is achieved.

IEC 61508 seeks for potential improvements for Programmable Electronic Safety (PES), contaiting microprocessor-based devices, for instance, distributed control systems (DCS), the programmable logic controllers (PLCs), integrated processor-based sensors and processor-based valves and pumps, and so forth.

IEC 61508 comprises seven parts, being a fairly complex standard. However, the first three parts are the most important ones. It can be said that Part 1 addresses

[3] ISA - International Society of Automation

management, mainly nontechnical, requirements, while Part 2 deals with technical requirements for the hardware realisation and Part 3 with technical requirements for software. The basic scope of the standard, provided in the document itself, is presented on the Figure 11 below.

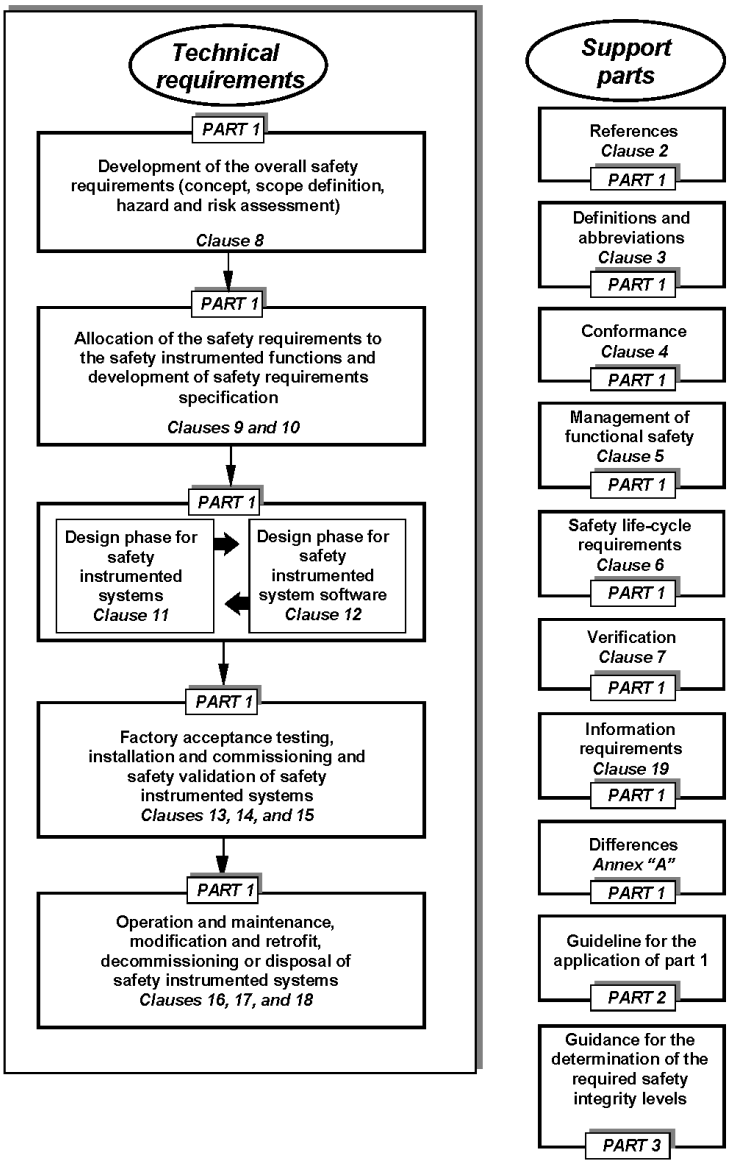

Figure 11. Framework of IEC 61508 (1998-2005).

The elaboration of the international standards on the SIS is substantial for development of the functional safety of the industry processes, project design and maintenance. One of the important standards, IEC 61508, which considers numerous process industries, has already been described. It is essential to mention, the second one, but not less important, the standard IEC 61511, which is concentrating more on industries with gases, liquids, and continuous production process.

It is exceedingly significant for hazardous technological processes that specialists, who employed in projects design or daily equipment operations, have to be competent and skilled. Since the expansion of implementation and application of automated instrumentation and machinery, there has been a demand for the experienced professionals, who have the knowledge of the necessary process automation equipment performance, operating quality, required process execution by the safety systems, and who also have expertise in computational tools and who are capable of evaluating tolerable, acceptable and unacceptable ranges for the hazard rates.

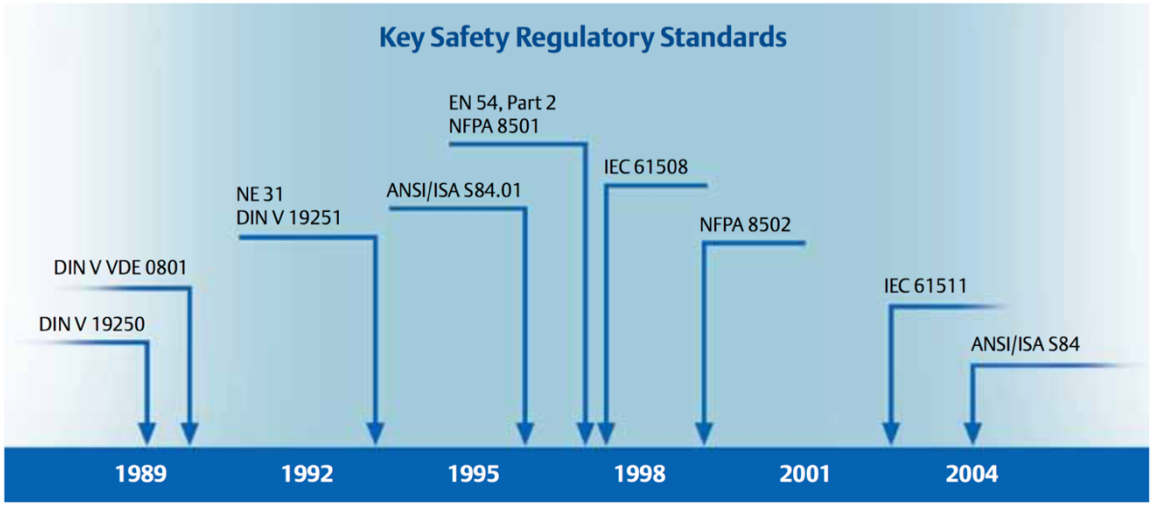

Figure 12. Evolution of functional safety standards. Source YOKOGAWA, Research & Development (2016).

2.3.2.2 Concept of Risk. Safety Integrity Level as a Measure of Risk

Risk, in a broad sense, is an expected value of damage usually in monetary form, given the occurrence of a specific hazard with its dangerous consequences during a predetermined time period [0, t]. For the i^{th} hazard and its dangerous consequences the risk can be estimated as follows:

$$R_i(t) = C_i \cdot F_i \cdot t, \qquad (15)$$

where C_i is the average value of damage in monetary form implying the full recovery from a dangerous consequence of i^{th} hazard;

F_i is the frequency of the of i^{th} dangerous consequence occurrence or, in other words, an average number of this consequence occurrence per year, the unit is [1/year];

t is the Lifecycle of a particular hazardous system, for which the value of risk is evaluated, the unit is [years].

In the engineering literature on industrial safety we can find a different definition of risk. In a narrow sense the risk of i^{th} dangerous consequence can be understood as a value F_i of frequency of i^{th} dangerous consequence occurrence. Sometimes instead of frequency, the probability of a dangerous event within a given time period taking place is considered.

In order to conduct an assessment, the following assumptions are made. At a design stage only those dangerous consequences which appear as a result of incident emergence are analysed. At the same time an *occurrence of an incident* is understood as at least one of the parameters of the technology shifting into the range of its critical values, which implies that under such values of a technological parameter, further operation of the technology is forbidden. According to IEC 61508, the dangerous consequences can be classified in the manner presented in the table below, hence the division into four groups: A, B, C and D.

Table 1. Classification of dangerous consequences. Source Macdonald (2004).

Groups of consequences	Names of groups of consequences according to IEC 61508	Content and interpretation of a group
A	Negligible	Violation of quality of products, discrepancy of production to requirements of industrial standard specifications, etc.
B	Marginal	Losses of oil and gas which don't lead to serious consequences, shutdown of the equipment, violation of a technological mode.
C	Critical	Explosions which lead to injuries of the personnel, break of pipelines, emergency depressurization of the equipment and pipelines, destruction of the equipment.
D	Catastrophic	Explosions, fires, mortality of people, ecological damage due to oil spill and fire.

Note that interpretation of each group of dangerous consequences is one of the fundamental facts when forming the specification, adequacy of this interpretation will influence the adequacy of assessment results.

As an example, let's address such factor as the geographical location of a particular facility. For example, if a production unit is located near a settlement of people, then the consequences as explosions should be referred to the group D. However, if production is in the place which is remote from the populated areas, then the consequences of explosions can be referred to the group C.

Classification of risks in which four classes of risks are stated is recommended by the standard specification IEC 61508 are given below. The determination of Safety Integrity Levels (SIL) and the clarity of the safety become the fundamental principles for IEC 61508. Each safety function has to obtain a certain SIL, as stated in the requirements of the standard. That specific SIL is determined in advance and based on a conducted risk assessment. Each class of risks is characterized by two parameters: a group of dangerous consequences and a range of the frequency of their occurrence.

Table 2. Classification of accidents according to IEC 61508 (1998-2005).

Frequency range, year $^{-1}$		Consequences			
		Catastrophic	Critical	Marginal	Negligible
Frequent	>1	I	I	I	II
Probable	$1…10^{-1}$	I	I	II	III
Occasional	$10^{-1}…10^{-2}$	I	II	III	III
Remote	$10^{-2}…10^{-3}$	II	III	III	IV
Improbable	$10^{-3}…10^{-4}$	III	III	IV	IV
Incredible	$<10^{-4}$	IV	IV	IV	IV

In this table a four-group classification of risks (with numbers from I to IV) is given with two parameters: *consequences* and *frequency*. The *consequences* are understood as four groups entered by IEC standard: catastrophic, critical, marginal and negligible, according to the Table 1. At the same time each group has a set of specified negative consequences which includes into this group and is inherent in the considered technological process. The *frequency* is understood as qualitative evaluation of frequency of dangerous consequences occurrence, also the range of numerical values for the frequencies is provided. For example, if a technological process has the second class of risk, then dangerous consequences of the group C appear on this process with a frequency belonging to a range $10^{-1} \div 10^{-2}[year^{-1}]$.

The SIL is a quantitative index that demonstrates the acceptable probability of dangerous failure that a system can have to consider it appropriate for a given specific safety integrity requirement. Distinction is made between two different kinds of systems: low-demand mode and high-demand/continuous mode of operation. Safety Instrumented Systems are usually in low-demand mode of operation. This mode of operation is defined by IEC 61580-4 as the one 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. For these, the SIL levels are defined in terms of average probability of failure on demand (Table 3).

Table 3. SIL for systems with low-demand mode of operation

(IEC 61508, Part 1, 1998-2005)

SIL	PDF_{avg}
IV	$[10^{-5}; 10^{-4})$
III	$[10^{-4}; 10^{-3})$
II	$[10^{-3}; 10^{-2})$
I	$[10^{-2}; 10^{-1})$

2.3.2.3 Standards for Safety Instrumented Systems applied in Petroleum Industry in Russia

The two main standards IEC 61508 and IEC 61511 are adapted as the State standards in Russian (in Russian language: *Государственные стандарты*): GOST MEK 61508 and GOST MEK 61511.

The Federal Law "On Industrial Safety of Hazardous Production Facilities" specifies the terminological scope of Risk management and SIS and covers the legal and economic principles of ensuring the safety of hazardous facilities functioning. The law established the safety integrity level for the facilities of several industrial branches, including oil and gas industry:

For hazardous production facilities of oil and gas condensate drilling and development the following classes of hazard are established:

- II class of hazard – for hazardous production facilities with regard to discharge of product with the content of hydrogen sulphide more than 6% of such product volume;
- III class of hazard – for hazardous production facilities, hazardous with regard to discharge of product with the content of hydrogen sulphide more than 1% of such product volume;
- IV class of hazard – for hazardous production facilities which are not specified in sub-items 1 and 2 of the present item.

For gas distribution stations, for gas distribution and gas consumption networks the following classes of hazard are established:

- II class of hazard – for hazardous production facilities intended for transportation of natural gas under pressure more than 1.2 MPa, or liquefied petroleum gas under pressure of more than 1.6 MPa

III class of hazard – for hazardous production facilities which are not specified in sub-item 1 of the present item."

Figure 13. Risk class requirements according to Federal Law (2014) on industrial safety.

For the classification, provided in section 2.3.2.3 of this work, the following values can be presented for the technology of oil and gas production and preliminary treatment. Table 4 and Table 5 below demonstrate the values of the damages and classes of risks.

Table 4. Example of assessment of damage for each group of consequences (in US dollars). Adopted from Shershukova (2013c).

	Consequences			
	Negligible A	Marginal B	Critical C	Catastrophical D
Range of values of damage, millions of USD	10 000 – 100 000	100 000 – 1 000 000	1 000 000 – 10 000 000	10 000 000 – 100 000 000
Average value of damage, millions of USD	45 000	450 000	4 500 000	45 000 000

Table 5. Example of assessment of damages over the classes of risks from (Shershukova 2013c).

	Consequences			
	Negligible A	Marginal B	Critical C	Catastrophical D
I	–	450 000	2 250 000	4 500 000
II	45 000	225 000	225 000	450 000
III	4 500	4 500	4 500	22 500
IV	450	2 250	2 250	4 500

In Table 5 an acceptable class of risk is chosen for SIS, deployed for the facilities and units of the oil and gas production infrastructure. For such processes the third class of risk (or SIL III) is specified.

Table 6. Example of choice of an acceptable risk class.
Adopted from (Shershukova 2013c).

SIL III	Consequences			
	Negligible A	Marginal B	Critical C	Catastrophical D
Frequency rage, year^{-1}	Improbable 10^{-3}…10^{-4}	Improbable and remote 10^{-2}…10^{-4}	Remote and occasional 10^{-1}…10^{-3}	Occasional and probable 1…10^{-2}

One of the issues addressed in the procedure of choosing the acceptable risk class in Table 6 is quantitative interpretation of risk itself, i.e. the table clearly specifies the frequency for every group of hazardous consequences that can appear.

Hazardous industrial facilities operated for the purposes of oil and gas production are characterized by the class of risk which is lower than the one specified in

the requirements. In such a case a safety system should be deployed so that the facilities would gain the acceptable risk class.

Another important document is GOST R 51330.5-99: Electrical apparatus for explosive gas atmospheres, which is an adaptation of IEC 60079-4-75. The purpose of this standard is assessment of the hazardous areas on the industrial facilities, given the properties of explosive gases and vapours, as well as probability of the occurrence of hazardous, explosive atmospheres in hazard-zones.

Additionally, other documents could be mentioned:

- Rules for electrical installations in hazardous areas.
- GOST 27.002-89 "Reliability in engineering. Terms and definitions".
- GOST 27.301-95 "Reliability in engineering. Calculation of reliability. The main provisions".
- GOST 27.310-95 "Reliability in engineering. Analysis of types, consequences and criticality of failures. The main provisions".
- GOST R 51901-2002 Reliability managment. Risk analysis of technical systems.

The detailes of those stanards cover many issues of engineering design, however the most important issues with regards to our work are covered in the standards 61508 and 61511.

2.3.2.4 ALARP Principle of Risk Reduction

According to the IEC 61508, a safety system can be presented structurally in the form of the following consecutive layers of protection represented in Figure 14 below.

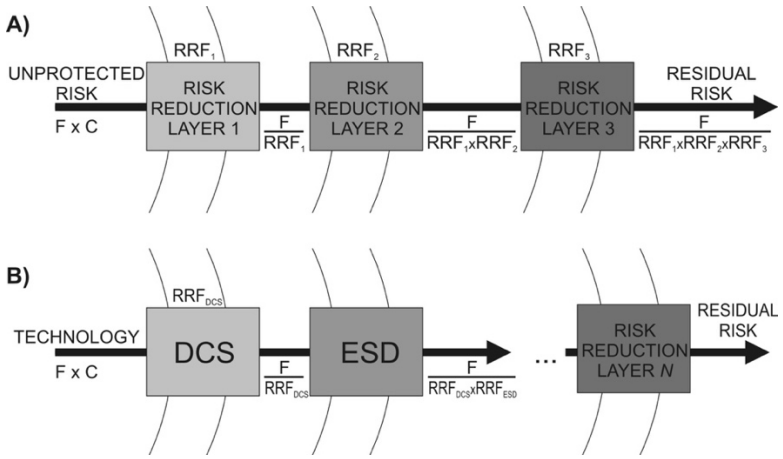

Figure 14. Risk reduction model. A) General case, shown in (Macdonald 2004)
B) Petroleum industry process, adapted for this research

On the left-hand side of the diagram we have the pairs of hazardous events' frequencies and consequences for the facilities without any risk reduction measures. On the right hand side we see the residual risk, i.e. the risk remaining after all taken measures of protection from a dangerous consequence.

Risk reduction layer 1 represents a distributed control system (DCS) which is one of parts of an automated process control system. This layer incorporates the control over the technological operation of the facilities with discreet (on/off) control and with continuous (proportional-integral-derivative, or PID) control, the interlock system, the alarm system and the necessary actions operators that can be done in order to avoid the system's shutdown. Note that protection function of DCS has non-specific character as the main function of a DCS is control over a technological process. DCS is designed for realization of this function, however it possesses several fixed safety indicators as well.

Layer 2 carries out a substantial reduction in risk from dangerous consequences due to the function of an Emergency Shutdown (ESD) system. The detailed specification of this system is the focus of this work, because this system is designed in particular for the purpose of reducing the risk of operating the facilities of oil and gas production infrastructure to an acceptable level.

A generalized Layer N characterizes the further risk-reduction measures, some of which are not included in the APCS.

Generally speaking, we came to the problem of making a decision on how many of the risk-reduction measures we should apply, and how elaborate, and thus effective

and expensive those measures should be. Standards IEC 61508 and IEC 61511 describe the ALAPR principle of reducing the total risk. The acronym stands for "as low as reasonably practicable", which implies that the risk-reduction measures are applied further and further as long as there's a payoff (i.e. the benefits of their application are greater than their costs). The general idea of the principle is to determine three broad categories of risk for the whole system we're designing: *negligible* risk, *tolerable* risk and *unacceptable* risk.

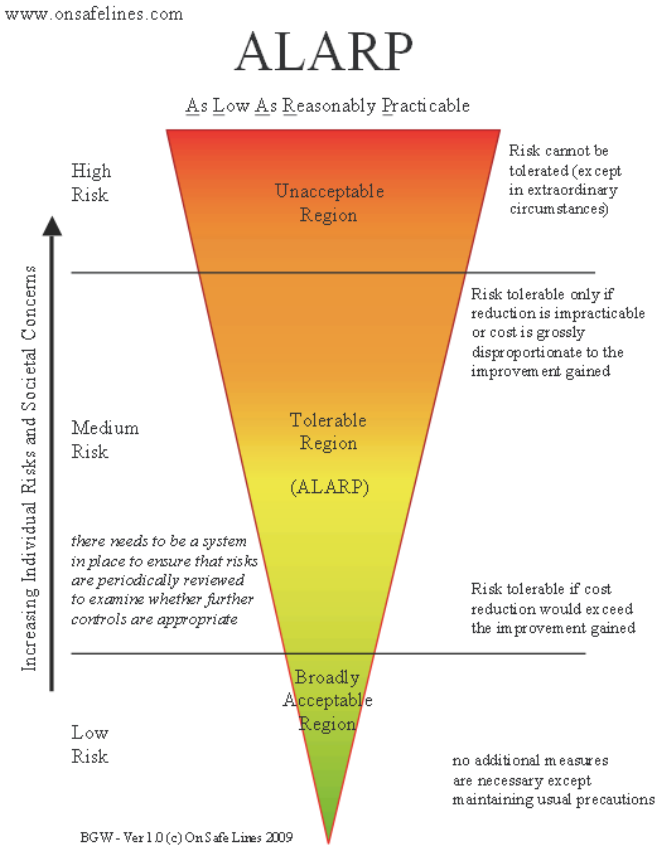

Figure 15. ALARP principle illustration.

Source On Safe Lines Quality, QHSE Software (2009).

The meaning of those three categories of risks:

Negligible risk. It is assumed that this level of risk is the one people live with everyday, i.e. it covers frequency of a lightning stroke or a brick falling on someone's head. A probability of these events is so small that those are neglected.

Tolerable risk. It is a risk which exists, but its value is approved of, because there are advantages of accepting this risk surpass the disadvantages of the dangerous consequences.

Unacceptable risk. A risk is so high that severity of the dangerous consequences outweighs any possible advantages.

The analysis of benefits from risk reduction measures will lead the decision-maker to the area of tolerable risk, which represents a compromise between the investment into risk reduction and the benefits of potentially hazardous activity.

With regards to specifics of oil and gas production branch of industry, the reduction of the risk up to the required level is provided by the Emergency Shutdown System, an automated system, performing the safety function.

2.3.3 Proof Testing

There are two general ways used to check and maintain the availability of SIS and its components. One of those ways is, as it has been stated previously, a continuous self-diagnostic function of the equipment of SIS. The other way is conducting a periodic proof tests. The obvious purpose of proof testing is to detect dangerous undetected failures. International standard defines the proof testing in the following manner: those are "periodic test performed to detect failures in a safety-related system so that the system can be restored to an "as new" condition or as close as practical to this condition" (IEC 61508, 1998-2005).

The proof tests play an important role in the necessary level of safety in the system. According to IEC 61508 and IEC 61511, the frequency of proof tests has a considerable influence on the target value of SIL. IEC 61508 Part 6 provides tables to determine *PFDavg* for the systems under the proof testing every 6 months, every year, every 2 and every 10 years intervals. However, the standard does not provide and further.

When we are describing a proof testing policy, we imply the following spesifics:

- the type of test,
- the test interval (which corresponds to the frequency),
- the test strategy.

The type of the test can either be a *full test* or a *partial test*. This classification is derived from the fact that sometimes different test frequencies may be required for different items of the SIS. The full test implies conducting the proof test to confirm the operability for the entire SIS loop: transmitters, logic solver and final control elements all together.

Some researchers and engineers suggest that preferably to perform the integral test, which analyze the entire safety loop at once. American Petroleum Institute's API RP-14C, establishes the necessity of carrying out performance testing for examining the ability of the systems to perform the intended safety function. It establishes as a requirement for the frequency of tests should not be less than once a year. The standard suggests monthly test for pneumatic devices, and quarterly for electronic sensors.

Partial testing is examining components of the system at different times and with different frequencies.

The proof testing is a periodical activity, that is executed with the period of TI (test interval). There are several states along the whole cycle that the component goes through. These states are testing, repair and further operations.

The testing strategies determine the particular scheduling strategies, i.e. how to explore the redundant elements in regard to each other. Several different strategies can be used to implemented proof testing. Among the strategies can be *simultaneous test*, when all the components of a redundant subsystem are tested at exactly the same time. This implies that there are several crews available to test every element of a subsystem independently. *Sequential test* implies that the elements are tested consecutively in time. *Staggered test* is a situation when the equipment is tested with a fixed time difference. And finally, the *idependent tesing* is when the equipment is examined without a predefined schedule, rather with a random time difference between one another.

2.3.4 Quantitative Indicators of SIS Performance

In this research we will use the following system of SIS functioning indicators, presented below. Those indicators include both qualitative reliability indicators and the requirements to the system's total risk class provided by the standards. So, for the description of the interaction between the technological process and SIS while it's performing its function, the following indicators will be used:

Safety Integrity Level (SIL) – this is a generalised indicator that specifies risk reduction level and the severity of the consequences. The levels SIL 1, 2, 3 and 4 can be regarded as risk classes provided in Table 2;

Risk Reduction Factor (RRF) – the ratio of hazards frequency without a SIS deployed on the facility to the frequency of hazards given a particular version of SIS is deployed;

Average Probability of Failure on Demand (PFD_{avg}) – a probability of the following event: a certain parameter of the technology transitioning to the its range of critical values, and at the same time the SIS deployed on the facility doesn't perform its function.

Aside from the risk reduction as a result of implementing SIS, there is a potential for the negative impact of SIS itself. Spurious tripping of ESD system can lead to unmotivated shutdown of the technology. The following indicators can be used to characterize the influence of SIS's on the technological process:

- mean down time due to the incidents during the technological process;
- mean down time due to the spurious trips of SIS.

2.4 Overview of Methods for Modelling SIS

The mathematical modelling techniques for analysis of safety systems can include various approaches. Comprehensive analytical models provided in reliability theory are the basis for any quantitative assessment, however, they are only easily applicable for the systems with only a small number of components (up to 10). In case we want to improve the details of our models by introducing the features such as common cause failures, diagnostic coverage level, and so on, those analytic models become rather complex and difficult to obtain. Many research groups made significant contributions to the topic. We would like to highlight some of the those researches, the contribution and conclusions from which are heavily applied for SIS modelling for the purpose of quantification of reliability parameters such as PFD_{avg} , *STR*, unavailability and so on.

The most popular methods are presented below:

- Methods based on simplified equations,
- Reliability Block Diagrams (RBD),
- Fault Tree Analysis (FTA),
- Markov Analysis (MA),

- other methods (Petri Nets, Bayesian Networks and so on).

Reliability Block Diagrams (RBD) and Fault Tree analysis (FTA) are two methods that are static and thus they allow only the average values of the characteristics to be calculated. RBD is generally used for modelling processes without restorations. FTA can include restoration actions into system modelling. Nevertheless, another more sophisticated approaches have to be applied for systems which have complicated repair actions policies or dependencies of time. These are methods that incorporate time and transitions (event occurrence) over time. Among them are Markov Analysis (MA), Petri Nets and Bayesian Networks (Goble 1998). Such methods are suitable for modelling, however many researchers (e.g, Goble 1998, Torres-Echeverria and Carlos 2009, and others) point out that these methods are computationally complex with exponentially growing complexity (e.g., in a Markov model for n deviced has 2^n states).

IEC 61508 Part 6 proposes a technique of PFD_{avg} quantification on the back of obtained from RBD simplified equations. The disadvantages of the simplified equations method are also introduced: the models can appear to be oversimplified and not adequate for detailed analysis for many systems.

Another approach that incorporates simplified equations is the PDS Method (acronym in Norwegian language, that stands for "Reliability of Computer-Based Systems"). Incorporating failure causes and categories which had not been considered in the previous methods is the target of this technique. With purpose to study the reliability and availability of computer-based safety systems, the Norwegian Foundation for Scientific and Industrial Research SINTEF (in Norwegian: Stiftelsen for industriell og teknisk forskning) initiated the PDS project. SINTEF is the largest independent research organisation in Scandinavia and it also plays the role of a parter to The Norwegian University of Since and Technology (NTNU), which has a long history of studying SIS. The products of the PDS project are periodically updated SIS reliability assessment method handbook (Hauge et al. 2010b) and reliability data handbook (Hauge and Onshus 2010).

Langeron et al. (2008) study the merging rules in SIS reliability assessment. The results of the group of researches at University of Technology of Troyes in France confirm the needs for advanced methods for complex SISs, and they point to Markov method.

Japanese researches (Misumi and Sato 1999) apply fault tree to model SIS performance. Zhang, Long and Sato (2003) from the Tokyo University of Marine Science and Technology apply Markov method to study SIS reliability and derive expressions for equivalent mean downtimes (EMDTs). Zhang, Long and Sato (2003) suggest to use EMDTs derived from Markov model.

Bukowski (2001, 2006a, 2006b), Bukowski et al. (1997) from Villanova University in the US and her collaborators apply mainly Markov method to study SIS reliability and investigate the Common Cause Failure (CCF) contribution from different architectures.

There are several comparative studies on the reliability modelling methods. Examoples of such research are (Goble 1998, Goble and Cheddie 2005, IEC 61508). Similar results are achieved in those works on comparative analysis. The two methods FTA and MA were proved to be the best by Goble. The author (Goble, 1998) stated that they have similar modelling outcomes. Goble and Cheddie (2005) also make a note that MA is more versatile because it allows to address the probabilities of failure over time, as well as to incorporate different modes of failure and other event, for example, systematic failrues or technological incidents. The methods RBD and FTA are both static. And the defference between them is the focus of their consideration: RBD is concerned with modelling the realibility (i.e., absence of failure) of the system, and the point of FTA is the failure of the system. The authors Goble and Cheddie (2005) consider FTA to be a better method than RBD, because FTA visually represent how device failures escalate to the failure of the entire system. Moreover, RBD is considered to be a method resulting in pessimistic assessments (Rouvroye and Brombacher, 1999). Despite the demonstrated advantages of FTA in comparison to other modelling techniques, which provide similar results, FTA is not flexible enough to incorporate interactions of failures, systematic failures and other random events, e.g., incidents. For such complex modelling, MA would be a better tool. In the work (Andrews and Ericson, 2000) the authors study FTA and MA by the example of different structures. It was observed that the accuracy of those two methods are very similar.

From the research presented above, one can conclude that both FTA and MA are good methods, however MA is better because it is more flexible. The obvious disadvantage of choosing MA lies in its complexity that was proved to exponentially increase (Goble, 1998). The size of MA problem is dependent not only on the number of

devices in the modelled system, but also on the variety of failure modes and additional events that are considered. So, even for relatively small problem instances the model can become significantly large. There are other modelling techniques (i.e., hybrid methods) that can be applied to reliability and system design problems (for instance, Schneeweiss (2001) describes Petri nets, and Dugan et al. (1992) writes about dynamic fault trees), however they also have the issues with complexity.

In this study we will represent the operations of the technological process and the Safety Instrumented System performing its function as a stochastic process, and we will apply the Markov analysis to evaluate the reliability characteristics of the process. Markov analysis is a versatile technique, that allows to incorporate many particular traits of the considered process. In our case, we will conduct the modelling of SIS performing its function given its interaction with the technology.

3 MATHEMATICAL MODELLING

In this chapter we will address the issues of mathematical modelling of the Emergency Shutdown system. In order to obtain the necessary characteristics for a particular solution of ESD, we will implement several stages of modelling:

Stage 1. Modelling a particular subsystem of ESD for the purpose of obtaining the characteristics of the entire subsystem with a particular structure.

Stage 2. Modelling the ESD consisting of three subsystems and interacting with the technology.

Stage 3. Optimization of the ESD specification with regards to feasible architectures and the databases of possible tools.

3.1 Problem Setting and Modelling Assumptions

In the previous chapter we have described s structure of SIS. The whole system consists of a number of units, or control loops, that perform the safety function. Each loop consists of the three subsystems (transmitters, logic solvers and final control elements) which are connected in a series from the point of view of reliability diagrams (see figure below).

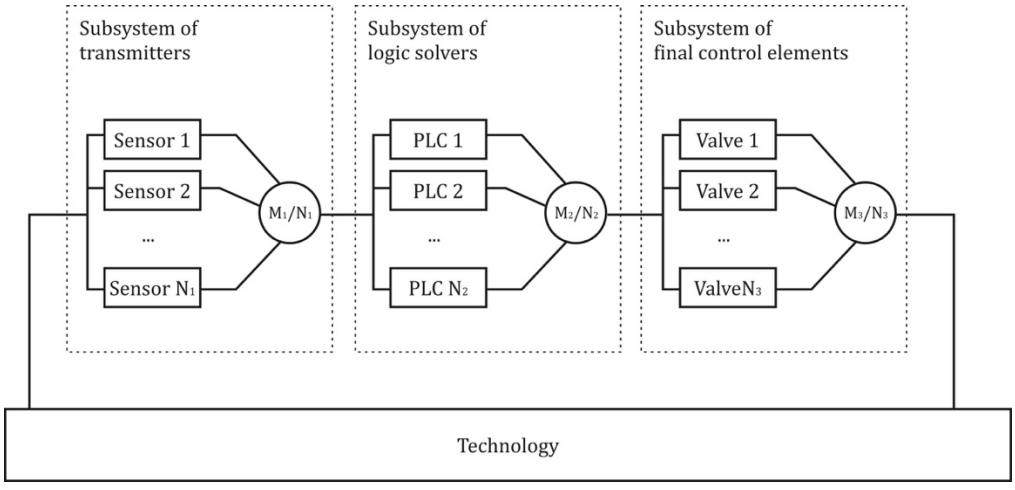

Figure 16. Detailed structure of a SIS loop, considered for this research.

The following assumptions are in place for further modelling purposes:

The failure rate of each particular element of any subsystem is a constant value.

We are ignoring the burn-in and wear out periods. Ignoring the burn-in period is reasonable because all the defected components are revealed during the commissioning work.

For the purpose of modelling the behaviour of the ESD implemented for a particular process risk, the classification of failures, presented earlier (see Figure 7), is applied.

The behaviour of ESD deployed for the technological process is described by a Markov process, for which the stationarity is implied.

The redundancy schemes are non-diverse, i.e. in case of several options for the components to use, we make separate decisions of the type of the component and its redundancy scheme.

3.2 Mathematical Model of a Subsystem

Each subsystem is characterized as follows:

1. The particular device, which is characterised by:
    a. The name of the manufacturer, the device model, technical characteristics
    b. Reliability characteristics of the device:
        i. failure rate – the rate of dangerous failures for one element,
        ii. diagnostic coverage – this demonstrates the share of the total number of failures revealed by a diagnostic system of refusals,
        iii. spurious tripping rate – the rate of safe failures of one element.
2. The architecture of the subsystem, which is generally defined by a block diagram of a subsystem and its standard Moo$N$ characteristic, where M is a minimum number of the devices in the usable, or healthy state, from a total number of channels N necessary in order that the ESD system would execute its safety function. Types of architecture and their characteristic are analysed in detail in the IEC 61508, 61511.
3. β-factor for a subsystem. This factor implied the fraction of Common Cause Failure in the total failure rate. A more elaborated structure results in decreasing the likelihood of Common Cause Failure, and consequentially, a lower value of β.

The two design options that will be featured further in the computations will be addressed: the design with no electrical separation of the devices in a subsystem and the design with an electrical separation.

4. Restoration rate μ for the subsystem. This is the qualitative measure, that shows how quickly the failed component can be restored, if the failure was detected.

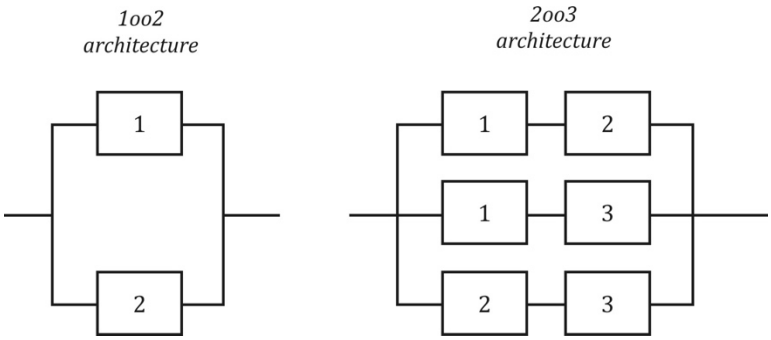

Figure 17. Examples of architectures. 1oo2, 2oo3.

Main principles of RBD and examples of the diagrams can be found in Goble (1998), Lewis (1996), IEC 61508 (1998-2005) and other resources.

A block diagram of a subsystem with the characteristic 1oo2 represents "one-out-of-two" architecture. In this case a subsystem consists of two channels. At the same time each channel in the operating state can execute safety function. The system will fail if both channels become inoperable.

3.2.1 Failure Rate for Dangerous Undetected Failures

Since we're considering the undetected failures, then the process of restoration, i.e. maintenance or replacement the failed components with the spare parts, does not take place. The stochastic process of dangerous undetected failures of the devices in a particular subsystem can be represented by the "pure death process", which is a special case of Markov birth-death processes. The graph of the process is presented on the figure below.

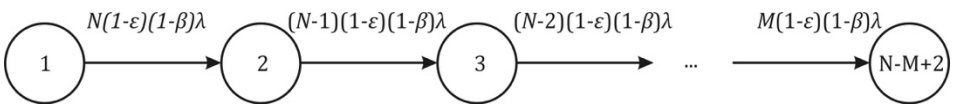

Figure 18. Dangerous undetected failures in a subsystem with MooN architechture. Main principles of MA and examples of the diagrams can be found in Goble (1998), Lewis (1996), IEC 61508 (1998-2005) and other resources.

Given that $(N - M + 1)$ components in a subsystem should fail so that the failure of the whole subsystem would happen, the stochastic process will consist of N-M+2 states. The realization of the stochastic process is considered during the time interval between two consecutive proof tests. This time interval is called the *test interval* denoted by *TI*.

Table 7. States of the stochastic process, describing the dangerous undetected failures in a subsystem

State	Description
1	All the components of a subsystem are in operating state
2	Dangerous undetected failure of one component occurred. All the rest are in operating mode
…	…
$N–M+2$	Dangerous undetected failure of at least N-M+1 component has occurred.

Considering (9), the probability of independent failures of $(N - M + 1)$ components during the test interval (TI) is calculated as follows:

$$P^{DU}(TI) = \sum_{i=N-M+1}^{N} \binom{N}{i} \cdot \left(1 - e^{-\lambda\cdot(1-\varepsilon)\cdot(1-\beta)\cdot TI}\right)^{i} \cdot e^{-\lambda\cdot(1-\varepsilon)\cdot(1-\beta)\cdot TI\cdot(N-i)}. \qquad (16)$$

Given (16) and the definition of the failure rate (3), we can obtain the failure rate for the dangerous undetected failures:

$$\lambda^{DU} = -\frac{log\left(1 - P^{DU}(TI)\right)}{TI} + \lambda \cdot (1 - \varepsilon) \cdot \beta \qquad (17)$$

The first term in (17) is describing the dangerous undetected independent failures, whereas the second term provides evaluation for dangerous undetected common-cause failures, both of which contribute to the λ^{DU} failure rate.

3.2.2 Failure Rate for Dangerous Detected Failures

Here we will be considering the detected failures, which implies that the restoration processes of the failed components will also be considered in our model.

First, let us consider the independent failures. The stochastic process of independent dangerous detected failures of the devices in a particular subsystem is represented by a Markov "birth-and-death" process. The graph of the process is presented on the figure below.

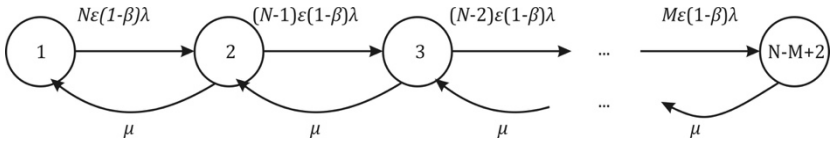

Figure 19. Dangerous detected failures in a subsystem with MooN architechture.

Given that $(N - M + 1)$ components in a subsystem should fail so it would result in the failure of the whole subsystem, the stochastic process will consist of N-M+2 states. The realization of the stochastic process is considered during the time interval between two consecutive proof tests, the duration of the interval is *TI*.

Table 8. States of the stochastic process, describing the dangerous undetected failures in a subsystem

State	Description
1	All the components of a subsystem are in operating state
2	Dangerous undetected failure of one component occurred. All the rest are in operating mode
…	…
$N–M+2$	Dangerous undetected failure of at least N-M+1 component has occurred.

The transitions of a subsystem between its states will be described by a system of ordinary differential equations:

$$\frac{dP^{DDN}(t)}{dt} = P^{DDN}(t) \cdot \Lambda^{DDN} \qquad (18)$$

Here, $P^{DDN}(t) = (p_1^{DDN}(t) \quad p_2^{DDN}(t) \quad \dots \quad p_{N-M+2}^{DDN}(t))$ is a vector of probabilities of the subsystems' being in a particular state, and A is the transition matrix containing the transition rates between the states:

$$\Lambda^{DDN} = \begin{pmatrix} \lambda_{11}^{DDN} & \cdots & \lambda_{1,(N-M+2)}^{DDN} \\ \vdots & \ddots & \vdots \\ \lambda_{(N-M+2),1}^{DDN} & \cdots & \lambda_{(N-M+2),(N-M+2)}^{DDN} \end{pmatrix} \qquad (19)$$

For the transitions depicted on the graph (see Figure 19), the components of the matrix Λ^{DDN} are non-zero. All the rest components are zeros. The non-zero components are described below:

$$\lambda_{11}^{DDN} = -N \cdot \varepsilon \cdot (1-\beta) \cdot \lambda, \quad \lambda_{12}^{DDN} = N \cdot \varepsilon \cdot (1-\beta) \cdot \lambda,$$

$$\lambda_{i,i-1}^{DDN} = \mu, \quad \lambda_{i,i}^{DDN} = -\big((N-i+1) \cdot \varepsilon \cdot (1-\beta) \cdot \lambda + \mu\big), \qquad (20)$$
$$\lambda_{i,(i+1)}^{DDN} = (N-i+1) \cdot \varepsilon \cdot (1-\beta) \cdot \lambda,$$
$$i = \{2,3,4, \dots, (N-M+2)\}.$$

The starting point of the stochastic process is state 1, or node 1 on the graph (see Figure 19), which corresponds to the following initial distribution of the probabilities:

$$P^{DDN}(0) = (1 \quad 0 \quad \dots \quad 0). \qquad (21)$$

We denote probability of the subsystem's failure by the end of the test interval by $p_{(N-M+2)}^{DDN}(TI)$. This value is last component of the vector $P^{DDN}(t)$ of the solution of ODEs in (18), for the moment of time at end of the test interval. After obtaining this solution we can calculate the failure rate for the independent dangerous detected failures:

$$\lambda^{DDN} = -\frac{\log\left(1 - p_{(N-M+2)}^{DDN}(TI)\right)}{TI}. \qquad (22)$$

The rate of common-cause failures is calculated as follows:

$$\lambda^{DDC} = \lambda \cdot \varepsilon \cdot \beta. \quad (23)$$

The total value of dangerous detected failures rate is:

$$\lambda^{DD} = -\frac{log\left(1 - p^{DDN}_{(N-M+2)}(TI)\right)}{TI} + \lambda \cdot \varepsilon \cdot \beta. \quad (24)$$

3.2.3 Failure Rate for Spurious Tripping

Here we will be considering the safe failures of a subsystem.

First, let us consider the independent failures. The stochastic process of independent safe failures of the devices in a particular subsystem is represented by a Markov "birth-and-death" process. The graph of the process is presented on the figure below.

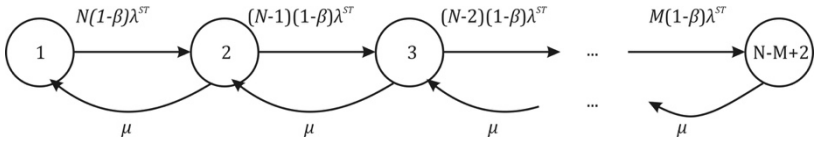

Figure 20. Safe failures in a subsystem with MooN architechture.

Given that $(N - M + 1)$ components in a subsystem should fail so it would result in the failure of the whole subsystem, the stochastic process will consist of N-M+2 states. The realization of the stochastic process is considered during the time interval between two consecutive proof tests, the duration of the interval is *TI*.

Table 9. States of the stochastic process, describing the dangerous undetected failures in a subsystem

State	Description
1	All the components of a subsystem are in operating state
2	Dangerous undetected failure of one component occurred. All the rest are in operating mode
…	…
N-M+2	Dangerous undetected failure of at least N-M+1 component has occurred.

The transitions of a subsystem between its states will be described by a system of ordinary differential equations:

$$\frac{dP^{SN}(t)}{dt} = P^{SN}(t) \cdot \Lambda^{SN} \qquad (25)$$

Here, $P^{SN}(t) = (p_1^{SN}(t) \quad p_2^{SN}(t) \quad \dots \quad p_{N-M+2}^{SN}(t))$ is a vector of probabilities of the subsystems' being in a particular state, and A is the transition matrix containing the transition rates between the states:

$$\Lambda^{SN} = \begin{pmatrix} \lambda_{11}^{SN} & \cdots & \lambda_{1,(N-M+2)}^{SN} \\ \vdots & \ddots & \vdots \\ \lambda_{(N-M+2),1}^{SN} & \cdots & \lambda_{(N-M+2),(N-M+2)}^{SN} \end{pmatrix} \qquad (26)$$

The starting point of the stochastic process is state 1, or node 1 on the graph (see Figure 19), which corresponds to the following initial distribution of the probabilities:

$$P^{SN}(0) = (1 \quad 0 \quad \dots \quad 0). \qquad (27)$$

For the transitions depicted on the graph (see Figure 19), the components of the matrix Λ^{SN} are non-zero. All the rest components are zeros. The non-zero components are described below:

$$\lambda_{11}^{SN} = -N \cdot (1-\beta) \cdot \lambda^{ST}, \quad \lambda_{12}^{SN} = N \cdot (1-\beta) \cdot \lambda^{ST},$$

$$\lambda_{i,i-1}^{SN} = \mu, \quad \lambda_{i,i}^{SN} = -\big((N-i+1) \cdot (1-\beta) \cdot \lambda^{ST} + \mu\big), \qquad (28)$$
$$\lambda_{i,(i+1)}^{SN} = (N-i+1) \cdot (1-\beta) \cdot \lambda^{ST},$$
$$i = \overline{2, (N-M+2)}.$$

We denote probability of the subsystem failure by the end of the test interval by $p_{(N-M+2)}^{SN}(TI)$. This value is lase component of the vector $P^{SN}(t)$ of the solution of ODEs in (25), for the moment of time at end of the test interval. After obtaining this solution we can calculate the failure rate for the independent dangerous detected failures:

$$\lambda^{SN} = -\frac{log\left(1 - p^{SN}_{(N-M+2)}(TI)\right)}{TI}. \quad (29)$$

The rate of common-cause failures is calculated as follows:

$$\lambda^{SC} = \lambda^{ST} \cdot \beta. \quad (30)$$

The total value of dangerous detected failures rate is:

$$\lambda^{S} = -\frac{log\left(1 - p^{SN}_{(N-M+2)}(\mathrm{TI})\right)}{TI} + \lambda^{ST} \cdot \beta. \quad (31)$$

3.3 Mathematical Modelling of the Emergency Shutdown System as a Risk Reduction Layer

3.3.1 Model Representation

This section describes functioning of the Emergency Shut shown (ESD) system with three subsystems in a series structure (see Figure 9) and the occurrence of technological incidents during the functioning of a particular technology associated with production and treatment of oil and gas on within a facility. The considered scope of the processes and their interaction is described as a stochastic process. The system for which the modelling is implemented, will further be referred to as “ESD+technology”.

We consider the following possible states for each subsystem of the ESD:

- a subsystem is performing its function,
- a subsystem is under the maintenance due to a dangerous detected failure or due to a spurious tripping,
- a subsystem is in the dangerous undetected failure mode.

We consider the following possible states for the facility:

- the facility is in the operational mode,
- the facility is stopped due to the process value entering the range of critical values, or due to the detected failures of safety system,

The process of interaction between the SIS and the technology is described with the following states:

Table 10. States of the stochastic process for ESD failures and technological incidents

	EMERGENCY SHUTDOWN SYSTEM			Technology
	Transmitters	Logic Solvers	Final Control Elements	
1	working	working	working	working
2	failed (DU)	working	working	working
3	working	failed (DU)	working	working
4	working	working	failed (DU)	working
5	under maintenance	working	working	stopped
6	working	under maintenance	working	stopped
7	working	working	under maintenance	stopped
8	working	working	working	stopped (due to incident)
9	failure			incident

The graph of transitions is given in the figure below.

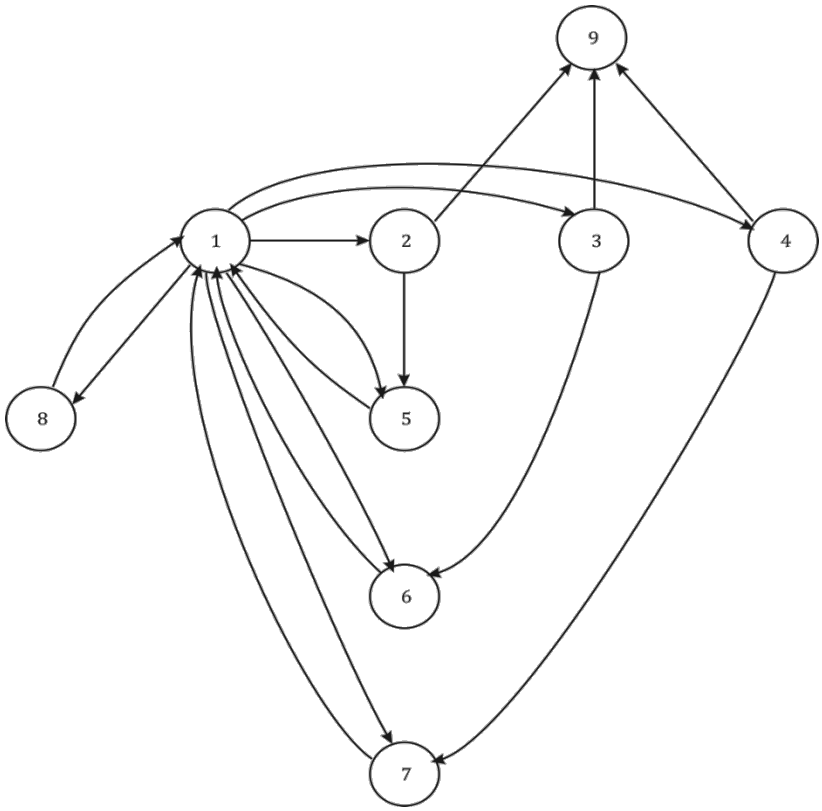

Figure 21. Model of SIS failure and its interaction with technology states.

The stochastic process the "ESD+technology" system transitioning from one state to another is modelled over the time of the entire lifecycle of the considered SIS. During the lifecycle time, several proof tests are performed. The time interval between the proof tests are equal to TI. During the proof tests all the previously undetected failures of the equipment are addressed and resolved. Literally speaking, it means that after the proof tests are performed, the stochastic process, depicted on Figure 21 cannot be in states 2, 3 or 4.

In this manner, we consider the following time horizon for the whole lifecycle of the system "ESD+technology":

$$LC: \big((0,\ TI)\quad (TI,\ 2\cdot TI)\quad (2\cdot TI,\ 3\cdot TI)\quad \dots\quad \big((K-1)\cdot TI,\ K\cdot TI\big)\big), \qquad K = \frac{LC}{TI}\ . \tag{32}$$

During each k^{th} period $\big((k-1)\cdot TI,\ k\cdot TI\big)$ of the presented time horizon, where $k = \overline{1,K}$, the behaviour of the system can be described by a system of ordinary differential equations:

$$\frac{dP(t)}{dt} = P(t) \cdot \Lambda \qquad (33)$$

Here, $P(t) = (p_1(t) \quad p_2(t) \quad \dots \quad p_9(t))$ is a vector of probabilities of the considered loop being in a particular state, and Λ is the transition matrix containing the transition rates between the states:

$$\Lambda = \begin{pmatrix} \lambda_{11} & \cdots & \lambda_{19} \\ \vdots & \ddots & \vdots \\ \lambda_{91} & \cdots & \lambda_{99} \end{pmatrix} \qquad (34)$$

For the transitions depicted on the graph (see Figure 21), the components of the matrix Λ are non-zero. All the rest components are zeroes. The non-zero components are described below:

$$\begin{gathered} \lambda_{11} = -\left(\lambda_{tr}^{S} + \lambda_{ls}^{S} + \lambda_{fc}^{S} + \lambda_{tr}^{DD} + \lambda_{ls}^{DD} + \lambda_{fc}^{DD} + \lambda_{tr}^{DU} + \lambda_{ls}^{DU} + \lambda_{fc}^{DU} + d^t\right) \\ \lambda_{12} = \lambda_{tr}^{DU}, \;\; \lambda_{13} = \lambda_{ls}^{DU}, \;\; \lambda_{14} = \lambda_{fc}^{DU}, \\ \lambda_{15} = \lambda_{tr}^{DD} + \lambda_{tr}^{S}, \;\; \lambda_{16} = \lambda_{ls}^{DD} + \lambda_{ls}^{S}, \;\; \lambda_{17} = \lambda_{fc}^{DD} + \lambda_{fc}^{S}, \;\; \lambda_{18} = d^t, \\ \lambda_{22} = -\left(\lambda_{ls}^{S} + \lambda_{fc}^{S} + d^t\right), \;\; \lambda_{25} = \lambda_{ls}^{S} + \lambda_{fc}^{S}, \;\; \lambda_{29} = d^t, \\ \lambda_{33} = -\left(\lambda_{tr}^{S} + \lambda_{fc}^{S} + d^t\right), \;\; \lambda_{36} = \lambda_{tr}^{S} + \lambda_{fc}^{S}, \;\; \lambda_{39} = d^t, \\ \lambda_{44} = -(\lambda_{tr}^{S} + \lambda_{ls}^{S} + d^t), \;\; \lambda_{47} = \lambda_{tr}^{S} + \lambda_{ls}^{S}, \;\; \lambda_{49} = d^t, \\ \lambda_{51} = \mu_{tr}, \;\; \lambda_{55} = -\mu_{tr}, \\ \lambda_{61} = \mu_{ls}, \;\; \lambda_{66} = -\mu_{ls}, \\ \lambda_{71} = \mu_{fc}, \;\; \lambda_{77} = -\mu_{fc}, \\ \lambda_{81} = \mu^t, \;\; \lambda_{88} = -\mu^t. \end{gathered} \qquad (35)$$

The initial distribution of probabilities for the period $k = 1$ corresponds to the "ESD+technology" system being in state 1 at the time $t = 0$:

$$P(0) = (p_1(0) \quad p_2(0) \quad \dots \quad p_9(0)) = (1 \quad 0 \quad \dots \quad 0). \qquad (36)$$

The initial distribution of probabilities for the subsequent periods $k = 2,3 \dots K$ can be derived from the concordance between the periods. Probability of the dangerous undetected failures exactly after the proof testing is equal to zero.

$$
\begin{aligned}
P\big((k-1)\cdot TI\big) &= (p_1^k \quad p_2^k \quad \dots \quad p_9^k),\\
p_1^k &= p_1(k-1)\cdot TI,\\
p_2^k &= 0,\ p_3^k = 0,\ p_4^k = 0,\\
p_5^k &= p_5\big((k-1)\cdot TI\big) + p_2\big((k-1)\cdot TI\big),\\
p_6^k &= p_6\big((k-1)\cdot TI\big) + p_3\big((k-1)\cdot TI\big),\\
p_7^k &= p_7\big((k-1)\cdot TI\big) + p_4\big((k-1)\cdot TI\big),\\
p_8^k &= p_8\big((k-1)\cdot TI\big),\\
p_9^k &= \mathrm{p}_9\big((k-1)\cdot TI\big).
\end{aligned}
\qquad (37)
$$

As we can observe from (37), probabilities $p_1(t), p_8(t)$ and $p_9(t)$ are monotonic over the entire lifecycle of the considered system, and the remaining probabilities $p_2(t), p_3(t), p_4(t), p_5(t), p_6(t)$ and $p_7(t)$ have singularities (or, in other words, fail to be well-behaved) at the junctions of the intervals of the planning horizon (32).

3.3.2 Reliability Indicators for the Modelled System

After obtaining the solution $P(t) = (p_1(t) \quad p_2(t) \quad \dots \quad p_9(t))$ of probabilities of "ESD+technology" system being in all its states from the ODE in (33) for every period of the planning horizon (32) with initial distribution of probabilities (36) and (37), we can move on to obtaining the reliability indicators for the considered system.

Average probabilityof failure on demand is determined as the average probability of the modelled system being in the 9th stage (the negative state), when there is an incident in the course of the technology and at the same time the ESD system is unavailable because of its failure.

$$
PFD_{avg} = \frac{1}{LC}\cdot\int_0^{LC} p_9(t)dt \qquad (38)
$$

Risk reduction factor is determined as a ratio of unresolved incidents rate for the technology without the ESD system and with ESD deployed:

$$RRF_{ESD} = \frac{d^t}{\lambda^{ESD}}. \quad (39)$$

Here, the incidents rate λ^{ESD} is determined from the Markov analysis:

$$\lambda^{ESD} = -\frac{log\left(1 - p_9(LC)\right)}{LC}, \quad (40)$$

whereas the incidents rate d^t is must be determined based on the incidents rate d determined during risk assessment for a given process, and the risk reduction factor ensured by the DCS:

$$d^t = \frac{d}{RRF_{DCS}} \quad (41)$$

Mean down time due to the spurious trips of ESD can be pessimistically estimated as the mean time of the "ESD+technology" system being in the 5th, 6th and 7th states:

$$DT^S = \int_0^{LC} p_5(t)dt + \int_0^{LC} p_6(t)dt + \int_0^{LC} p_7(t)dt. \quad (42)$$

Mean down time due to the technological incidents can be calculated as the mean time of the "ESD+technology" system being in the 8th state:

$$DT^t = \int_0^{LC} p_8(t)dt. \quad (43)$$

The total mean down time of the process:

$$DT = DT^S + DT^t. \quad (44)$$

3.4 Collecting the Initial Reliability Data for Modelling

In order to estimate the risk presented by a hazardous facility, we must conduct a risk assessment for the considered technology (in our case, a facility within an oil and gas production infrastructure). As a result of the assessment, we will obtain the estimated frequency of dangerous events per year.

An example of estimation of hazardous even's frequency is provided in Appendix A. In order to correctly evaluate the incidents rate for a technological facility, we should not only evaluate the frequency of incidents on the technology itself, but also consider the risk reduction, provided by the DCS, that implements the control over the technology. Calculating the risk reduction factor for DCS is a complicated process, requiring mathematical modelling somewhat similar to the ESD system model descried above. Further, we will use the results of calculating the RRF_{DCS} obtained in (Teluk and Shershukova 2012a, 2012b, 2012c, 2012d, 2012e).

Restoration rate for technology is determined from the nominal time for restoration of a unit in case of an incident. The value of this time is provided in the project documentation to the facility.

$$\mu^t = \frac{1}{T^t_{restoration}}. \qquad (45)$$

The reliability characteristics for the transmitters, PLCs and actuators, necessary for the model, are failure rate, spurious tripping rate and diagnostic coverage. Those values are provided in the technical documentation to each device.

The restoration rate for the subsystems of transmitters, logic solvers and final control elements are calculated given the nominal time for restoration of the corresponding elements in case of their failure. The value of this time is provided in the project documentation to the facility.

$$\mu^{tr} = \frac{1}{T^{tr}_{restoration}}, \quad \mu^{ls} = \frac{1}{T^{ls}_{restoration}}, \quad \mu^{fc} = \frac{1}{T^{fc}_{restoration}}. \qquad (46)$$

3.5 Multiobjective Optimization of Specifications of SIS

The mathematical model described in the previous section allows to calculate the necessary reliability characteristics for a particular variant of the safety system's specification. Let us now finally clarify all the necessary parameters that we will use for making decisions with regards to SIS specification

3.5.1 Decision Variables

- For every subsystem of ESD system the decision on the **particular models of devices** is made. Every engineering company has a limited number of vendors, which supply a limited number of devices, that are suitable for this or that purpose. As a result, we have a finite set of all possible devices that can be applied in SIS.
    - a particular model of a transmitter from the set of possible transmitters,
    - a particular model of a logic solver from the set of possible PLCs,
    - a particular model of a final control element from the set of possible elements.
- For every subsystem of ESD system the decision on the **redundancy scheme** is made. This means that we determine:
    - MooN architecture of transmitters subsystem,
    - MooN architecture of logic solver subsystem,
    - MooN architecture of final control subsystem.
- For every subsystem we determine the **Common-Cause Failures factor**, or β-factor. By choosing a particular β-factor we make a decision on introducing additional electrical separation into a subsystem. Thus, the decisions are
    - β-factor for the transmitters subsystem,
    - β-factor for the logic solver subsystem,
    - β-factor for the final control subsystem.
- For the whole system we choose the **test interval**, which implies that we are determining our schedule of planned maintenance (proof tests). The test interval is chosen from a set of values from 1 month to 24 months in steps of 1 month.

3.5.2 Objective Functions

3.5.2.1 Safety Indicators

For every particular specification of the ESD system, uniquely determined by the specification, stated in the set of decision variables we can obtain the following:

- first of all, the reliability characteristics for each particular subsystem, using the models from Section 3.2 of this research

- and then, after introducing the parameters of technological incidents occurrence, we can model the system "ESD+technology", as demonstrated in Section 3.3 of this research.

When the modelling for a particular alternative of SIS specification is implemented, as shown before, we obtain the values of the following indicators for the facility, we're designing:

- *average probability of SIS's failure on demand*,
- *mean down time of the technological facility*.

3.5.2.2 Cost of SIS Lifecycle as an Objective

It is obvious that the best solution from the point of view of those two reliablility characteristics would be the one with the most elaborate MooN structures and the most faul-tolerant (and thus expensive) tools for every subsystem. However, we should not persue only the benefits in terms of reliability. It has already been suggested in this work, that Formalizing this principle of compromise between the costs of risk reduction and the achieved level of safety. The latter is covered by the models in Sections 3.2 and 3.3. It means that now we should determine the cost of the solution, suggested by this or that specification of SIS.

The cost calculation in this work is mostly based on the modelling the cost of the lifecycle provided in (Goble, 1998), and (Torres-Echeverria and Thompson 2007). The cost structure has been adapted to the specifics of our reasoning and the cost values, obtained and used in the computational example in the following chapter. The lifecycle cost of SIS functioning on a particular technological process is presented below, and it includes three main components: procurement, operation and risk costs.

$$C_{lifecycle} = C_{procurement} + \sum_{t=1}^{LC} \left({C^t}_{operations} + {C^t}_{risk} \right) \cdot \frac{1}{(1+\delta)^{t-1}}. \qquad (47)$$

Here, δ is the discount factor, used for calculating the the present value of the future expenses (for the upcoming years within the lifecycle).

Procurement cost is calculated as follows:

$$C_{procurement} =$$

$$= \left(C^{tr}_{purchase} \cdot \beta_{purch} + C^{tr}_{design} \cdot \beta_{des} + C^{tr}_{installation} \cdot \beta_{inst}\right) \cdot N^{tr} +$$

$$+\left(C^{ls}_{purchase} \cdot \beta_{purch} + C^{ls}_{design} \cdot \beta_{des} + C^{ls}_{installation} \cdot \beta_{inst}\right) \cdot N^{ls} + \quad (48)$$

$$+\left(C^{fc}_{purchase} \cdot \beta_{purch} + C^{fc}_{design} \cdot \beta_{des} + C^{fc}_{installation} \cdot \beta_{inst}\right) \cdot N^{tr} +$$

$$+C_{startup}.$$

Here, $C^{tr}_{purchase}$ - the cost of purchasing one sensor

C^{tr}_{design}- the contribution of a particular model of sensor into the project of SIS design

$C^{tr}_{installation}$ - the contribution of a particular model of sensor into the installation and commissioning cost

N^{tr}- total number of sensor in the subsystem

$C^{ls}_{purchase}$ - the cost of purchasing one PLC

C^{ls}_{design}- the contribution of a particular model of PLC into the project of SIS design

$C^{ls}_{installation}$ - the contribution of a particular model of PLC into the installation and commissioning cost

N^{ls}- total number of PLCs in the subsystem

$C^{fc}_{purchase}$ - the cost of purchasing one final control element (e.g., one valve)

C^{fc}_{design}- the contribution of a particular model of valve into the project of SIS design

$C^{fc}_{installation}$ - the contribution of a particular model of valve into the installation and commissioning cost

N^{fc}- total number of final control elements in the subsystem

$C_{startup}$- the startup cost, associated with the project initiation, preparing the project documentation, software development, and so on.

β_{purch}, β_{des}, β_{inst} - the cost modifiers, connected to the particular choice of electrical separation within the subsystems

The operations cost per year:

$$C^{t}_{operations} = C^{tr}_{consumption} \cdot \beta_{cons} \cdot N^{tr} + C^{ls}_{consumption} \cdot \beta_{cons} \cdot N^{ls} +$$

$$+C^{fc}_{consumption} \cdot \beta_{cons} \cdot N^{fc} + \quad (49)$$

$$+C^{tr}_{PM} \cdot N^{tr} + C^{ls}_{PM} \cdot N^{ls} + C^{fc}_{PM} \cdot N^{fc} +$$

$$+\frac{12}{TI}\cdot\left(C_{PTest}^{tr}\cdot N^{tr}+C_{PTest}^{ls}\cdot N^{ls}+C_{PTest}^{fc}\cdot N^{fc}\right).$$

The first three terms in the formula correspond to the electricity consumption, depending on the number of elements in each subsystem. The following three terms demonstrate the cost of yearly preventive maintenance. The last term corresponds to the cost of proof tests, implemented in step of *TI* (test interval).

$C_{consumption}^{tr}, C_{consumption}^{ls}, C_{consumption}^{ls}$ - the yearly consumption of the electrical energy by one element in the transmitters, controllers and valves subsystems respectively,

β_{cons}- the cost modifier, connected to the particular choice of electrical separation within the subsystems

$C_{PM}^{tr}, C_{PM}^{ls}, C_{PM}^{fc}$ - the yearly cost of preventive maintenance for one element in the transmitters, controllers and valves subsystems respectively,

$C_{PTest}^{tr}, C_{PTest}^{ls}, C_{PTest}^{fc}$ - the cost of conducting one proof test for one element in the transmitters, controllers and valves subsystems respectively.

The yearly risk costs represent the losses due to loss of production during the system's downtime and the losses due to the potential dangerous events of hazards:

$$C_{risk}^{t}=C_{ST}^{t}+C_{HAZ}^{t}. \quad (50)$$

$$C_{ST}^{t}=\left(\left(C_{repair}^{tr}+C_{repair}^{ls}+C_{repair}^{fc}+C_{prod.loss}\right)\cdot SD+ \right.$$
$$\left.+C_{spairs}^{tr}\cdot N^{tr}+C_{spairs}^{ls}\cdot N^{ls}+C_{spairs}^{fc}\cdot N^{fc}\right)\cdot STR. \quad (51)$$

Here, $C_{repair}^{tr}, C_{repair}^{ls}, C_{repair}^{fc}$ are hourly costs of repairing the elements in the transmitters, controllers and valves subsystems respectively.

$C_{prod.loss}$ is hourly losses of production

SD – standard down time needed for repairing after the spurious tripping

STR is the rate of spurious tripping for the modelled system of ESD+technology.

The coefficients, corresponding to the cost of the spare parts replenishment are set as a fixed percentage of the procurement costs.

$$C_{spairs}^{tr} = \%Pr \cdot C_{purchase}^{tr},$$
$$C_{spairs}^{ls} = \%Pr \cdot C_{purchase}^{ls}, \quad (52)$$
$$C_{spairs}^{fc} = \%Pr \cdot C_{purchase}^{fc}.$$

The losses due to the consequences of the hazardous event:

$$C_{HAZ}^{t} = C_{loss} \cdot d^{t} \cdot PFD_{avg}. \quad (53)$$

Here, d^t is the frequency of the dangerous event occurring without the ESD system securing the technological unit, i.e. in case when we're considering only the facility and the DCS that controls the process.

The losses due to the hazard occurrence and the dangerous consequences taking place, can be determined using different approaches and ideas. The most important factors to be considered are: loss of the facilities equipment, decline in production qualities, and of course the liability costs in case of fatalities. An interested reader can find more information about those calculations in (HSE 2001), where the Value of Preventing a Fatality approach is used.

Thus, we are considering the problem of optimizing the specification of SIS by the example of ESD system, with three objective functions:

- *average probability of SIS's failure on demand*,
- *mean down time of the technological facility*,
- *the lifecycle cost of SIS.*

3.5.3 Potential Constraints

Often when the problem of ESD system design is solved, some constraints can be present. The limitations can be put in place when we're considering the expenditures, losses, frequency of ESD's failures on demand and so on.

The constraint representing the upper bound for the SIS lifecycle cost:

$$C_{lifecycle}(ESD_{alt}) \leq \overline{\overline{C_{lifecycle}}}. \quad (54)$$

Here, it is implied that the lifecycle cost is calculated according to (47), and ESD_{alt} is a particular alternative among all possible ESD specifications.

The constraint representing the upper bound for the losses due to the dangerous events occurrence and the dangerous consequence of the hazards taking place. The upper bound on those losses over the entire lifecycle:

$$\sum_{t=1}^{LC} C_{HAZ}^{t} \leq \overline{\overline{C_{HAZ}}}. \qquad (55)$$

The constraint representing the upper bound for resulting value of failure on demand frequency, given the ESD system is deployed:

$$d^{t} \cdot PFD_{avg} \leq \overline{\overline{F_{incidents}}}. \qquad (56)$$

This constraint implies that a certain risk class, or Safety Integrity Level is to be achieved by the ESD system, that we're deploying. For most facilities in oil and gas production, the necessary level of safety integrity to be achieved is SIL III.

3.5.4 Multiobjective Genetic Algorithm

Many optimization problems revolve around several objectives that need to be optimized. In most of the cases such objectives are conflicting or complimenting e.g. profit maximization and cost minimization issues. It is quite possible that one solution may not satisfy more than one objective i.e. solution for one objective may not be the optimal solution for the other objective. Thus, it can be concluded that in most of such cases a set of solutions is required instead of one or two objectives. This issue is put forward by many researchers, for example, Arroyo (2003) states that a Multi-objective Combinatorial Optimization (MOCO) problem consists of minimizing or maximizing a set of objectives while satisfying a set of constraints. It should be noted that in a typical MOCO problem, there is no single solution that can satisfy the optimization criterion for each objective, instead there is a set of efficient solutions. Furthermore, in such

conditions no single solution can be considered better than another solution for all objectives. Pitombeira (2011) highlighted the method proposed by Vilfredo Pareto that introduced the dominance concept. He argued that an optimal solution for a MOCO problem should maintain a sort of balance between different conflicting objective functions. This is called Pareto optimal solution. The major aim of MOCO is to find the Pareto optimal set or in other words Pareto frontier. The Pareto-optimal set can be defined as "A solution is pareto-optimal if it is not dominated by any other solution in decision variable space"

Pareto optimal can be well understood with the explanation of Pareto dominance. Pareto dominance can be defined as when a given solution x_1 is dominating another solution x_2 if the values of the objective functions for x_1 are better than or equal to the functional values of x_2 and at least one of the functional values of x_1 is strictly better than the functional value of x_2 (Deb 2008).

The pareto-optimal is one of the best known solutions in regards that all objectives cannot be improved in any objective without making the other objectives worse. The set of all feasible solutions that are non-dominated by any other solution is called the pareto-optimal or in other words non-dominated set. If the non-dominated set is within the entire feasible search space then it is called globally pareto-optimal set. In other words, for a given Multi-Objective Problem (MOP), the pareto-optimal set P^*, is defined as:

$$P^* = \{x \in \Omega \mid \neg\exists\, x' \in \Omega\, F(x') \preccurlyeq F(x)\}. \qquad (57)$$

Another concept related to Pareto Optimality is known as Pareto-front that can be defined as the values of objective functions related to each solution of a pareto-optimal set in objective space is called pareto-front. In other words, for a given MOP, $F(x)$, and pareto-optimal set, P^*, the pareto-front, PF^* is given by:

$$PF^* = \{u = F(x) \mid x \in P^*\}. \qquad (58)$$

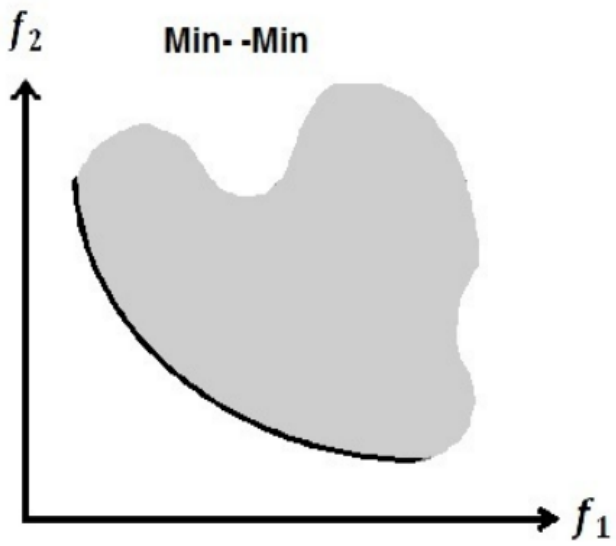

Figure 22. Pareto-front for two-objectives minimization problem, adopted from Konak, Coit and Smith (2006).

The above figure shows a typical pareto-front of a two objective minimizing type optimization problem in objective space. Since the concept of domination enables comparison of solutions with respect to multi-objectives, most of multi-objective optimization algorithms practice this concept to obtain the non-dominated set of solutions, consequently the pareto-front.

Deb (2008) says that in addition to finding a solution set near to the Pareto frontier, it is necessary that these solutions are well distributed, which allows a broader coverage of the search space. This fact facilitates the decision making, because, regardless of the weight assigned to each criterion, a quality solution will be chosen. Whereas, Deb (2001) states "there exist mutiple Pareto-optimal solutions in a problemonly if the objectives are conflicting to each other". Otherwise, if they are not conflict one single optimal solution is achievable.

There are two common requirements that should be met by an optimizer:

- Proximity
- Diversity

Purshouse (2003) formulated the additional objective of pertinence, meaning that the obtained Pareto set must provide solutions on the pertinent regions of interest. This, however, implies to guide the search based on previously expressed preferences.

According to other researches, in modern days Genetic Algorithms (GAs) are widely used and have proved to be a highly effective tool in order to solve hard optimization problems (Lukas et al. 2012). Genetic Algorithms are powerful general purpose optimization tools which model the principles of evolution.

Grefenstette (1993) states "A genetic algorithm is an iterative procedure maintaining a population of structures that are candidate solutions to specific domain challenges. During each temporal increment (called a generation), the structures in the current population are rated for their effectiveness as domain solutions, and on the basis of these evaluations, a new population of candidate solutions is formed using specific genetic operators such as reproduction, crossover, and mutation."

Whereas, Goldberg (1989) states "They combine survival of the fittest among string structures with a structured yet randomized information exchange to form a search algorithm with some of the innovative flair of human search. In every generation, a new set of artificial creatures (strings) is created using bits and pieces of the fittest of the old; an occasional new part is tried for good measure. While randomized, genetic algorithms are no simple random walk. They efficiently exploit historical information to speculate on new search points with expected improved performance."

Genetic Algorithms are established on the idea of Darwinian's evolutionary processes in accordance with survival of the fittest. This approach is based on the probabilistic theory and it employs the concepts of evolution and selection in order to generate a few solutions for particular problem. The algorithm simulates the process of evolution of a population of individuals whose genetic characteristics are inherited from those ancestors that were fittest for survival, the same as the natural evolution of species does.

It is important to emphasize that the fundamental concept of Genetic Algorithm comes up from the principle of “evolution”, that brings to Genetic Algorithm its flexibility and hardness. This Algorithm became widely used for optimization problems and investigation of real-life situations. In contradistinction to traditional approaches,

Genetic Algorithm is a method, which include determination of optimal parameters that provides the better opportunity for solving a lot of real-world practical problems. Genetic Algorithm allow to obtain the solution of the given problem with the help of an alternative technique. The traditional methods are well suited for problems with complex and broad searching area. While Genetic Algorithm outperforms them in obtaining "the optimumal" solution of the problem, as in surface scale as well as in a search of state-space. The entire architecture of Genetic Algorithm is built up on three stones: Elimination, Selection and Variation (Kanigolla 2014).

```
begin
generate randomly the initial population of chromosomes;
repeat
     calculate the fitness of chromosomes in population;
          repeat
               select 2 chromosomes as parents;
               apply crossover to the selected parents;
               apply mutation to the new chromosomes;
               calculate the fitness of new child chromosomes;
     until end of the number of new chromosomes
     update the population;
     until end of the number of generations
end
```

Figure 23. Pseudocode description of the Procedure Genetic Algorithm

Genetic Algorithms have the ability to create an initial population of feasible solutions, and then re-combine them in a way to guide their search to only the most promising areas of the state space.

Once the reproduction and the fitness function have been properly defined, a GA is evolved according to the same basic structure. It starts by generating an initial population of chromosomes, which is generated randomly to ensure the genetic diversity.

Each feasible solution is encoded as a chromosome (string) also called a genotype, and each chromosome is given a measure of fitness via a fitness (evaluation or objective) function. Then, the GA loops over an iteration process to make the next generation. According to the evaluation in the objective space, the individuals are

ranked and then assigned a fitness value, which determines their likelihood of reproduction in the next generation.

Each iteration consists of fitness evaluation, selection, reproduction, new evaluation of the offsprings, and finally replacement in population. Stopping criterion may be the number of iteration or the convergence of the best chromosome toward the optimal solution.

The fitness of a chromosome determines its ability to survive and produce offspring. The chromosomes are decoded into the real values of the variables they represent. This is the phenotype of the individuals. With this the objective functions are evaluated. According to the evaluation in the objective space, the individuals are ranked and then assigned a fitness value, which determines their likelihood of reproduction in the next generation. A finite population of chromosomes is maintained. For our finite domains, a fitness map is an exhaustive, uncompressed representation of the mapping between individuals and fitness values generated by a fitness function. It can be defined as the set of all ordered pairs (i, f (i)), where i denotes an individual in our domain and f(i) its fitness value (Montanez et al. 2013).

There are three basic rules:

- Biased Reproduction: selecting the fittest to reproduce;
- Crossover: combining parent chromosomes to produce children chromosomes;
- Mutation: altering some genes in a chromosome.

The cycle of evaluation, selection, reproduction and reinsertion is repeated until a certain condition to stop the algorithm is met. This condition may be the exhaust of a generation count or the compliance with a specific goal. At the end, the algorithm delivers a set of optimal solutions that is the Pareto-optimal front (Torres-Echeverria 2009).

The population of the GA is a group of N_{pop} individuals. The most common encoding is binary along with the use of numbers and integer codes. The population size N_{pop} is one of the parameters of the GA to choose. As Marseguerra et al. (2006) discuss, a too small or too large population can have serious consequences like problems in

genetic diversity. The initial population can be created following several strategies like random creation that is most simple way to do so. Although there can be many other strategies to create population.

The Single Point crossover is the simplest recombination, in which two strings are used as parents and new individuals are formed by swapping a sub-sequence between the two strings. The two parents exchange their portions of chromosome indicated by the crossover point.

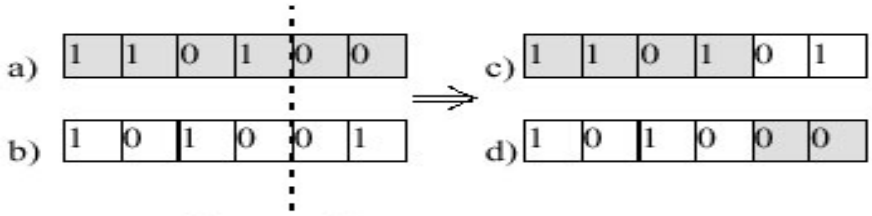

Figure 24. Bit-string crossover of parents a) & b) to form offspring c) & d). Source Angeline (1996).

Mutation is the second variability operator. This operator randomly changes one of the genes in the new offspring s chromosomes. Bit-flipping mutation is another commom operator in GA, in which a single bit in the string is flipped to form a new offspring string.

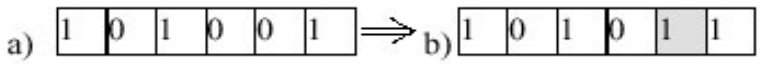

Figure 25. Bit-flipping mutation of parent a) to form offspring b). Source Angeline (1996).

The bitflipping mutation is the simplest binary mutation operator, where the bits of a chromosome are simply flipped with a certain probability pm.

As soon as the creation of the offspring by selection have been made, then the approach recombines and performs the mutation of the individuals from initial population, after that the determination of offspring's fitness has to be made. In case when the size of the old population is bigger than the new generated offspring, then the Genetic Algorithm must reinsert the offspring into the original population in order to keep up the size of the initial population. Analogously, in case when the size of the

original population is smaller than the produced offspring or not everyone from offspring belong to each generation, then the algorithm have to apply a reinsertion technique in order to define which individuals must be in the generated population. Then, in the following iteration of the Genetic algorithm, there is usage of new population. Typically, when a maximum amount of generations has been created, or when an acceptable degree of fitness for the population has been achieved, so the Genetic procedures then stopped (Pencheva et al. 2011).

3.6 Representation of the Problem in Matlab

Obtaining the values of $\lambda^{DU}, \lambda^{DD}, \lambda^{S}$ for the subsystems of SIS.

Table 11. The input data, provided into the function:

Parameter in the model	Variable in Matlab	Description
M	M	Number of elements to be in operational condition in MooN architecture
N	N	Total number of element in MooN architecture
ε	alpha	Level of diagnostic coverage for 1 element (value from 0 to 1, percentage)
β	betta	Common-cause failure factor (value from 0 to 1, percentage)
μ	mu	Repair/restoration rate (in 1/hours)
λ^{ST}	lambda_st	Spurious tripping rate for 1 element (in 1/hours)
TI	TI	Test interval, hours

Table 12. The output data, provided by the function:

Parameter in the model	Variable in Matlab	Description
λ^{DU}	la(1)	Failure rate for dangerous undetected failures for the subsystem
λ^{DD}	la(1)	Failure rate for dangerous detected failures for the subsystem
λ^{S}	la(3)	Failure rate for the subsystem's spurious trips

```
function la = structure (M, N, alpha, betta, lambda, mu, lambda_st, TI)

p = 0;
for i = (N-M+1):N
    p = p + nchoosek(N,i).*(1-exp(-lambda.*(1-alpha).*(1-
betta).*TI))^i.*exp(-lambda.*(1-alpha).*(1-betta).*TI.*(N-i));
end
la(1) = - log(1-p)/TI ;

Size=N-M+2;
La_M_temp=zeros(Size, Size);
La_M_temp(1,1) = -N.*alpha.*(1-betta).*lambda;
La_M_temp(1,2) =  N.*alpha.*(1-betta).*lambda;
for i = 2:(Size-1)
    La_M_temp(i,i-1) = mu;
```

```
    La_M_temp(i,i)   = -(N-i+1).*alpha.*(1-betta).*lambda - mu;
    La_M_temp(i,i+1) = (N-i+1).*alpha.*(1-betta).*lambda;
end
M_temp = zeros(Size-1, Size-1);
for i = 1:(Size-1)
    for j = 1:(Size-1)
        M_temp(i,j) = La_M_temp(i,j);
    end
end
Initial_Distrib=zeros(1, Size-1);
Initial_Distrib(1)=1;

[T,Y] = ode45(@(t,y) MooNDD(t,y,M_temp), [0 TI], Initial_Distrib);
for i = 1:(Size-1)
        temp = temp + Y(:,1));
end
    Y(:,Size)=1-temp;

la(2) = - log(1-Y((length(Y(:,Size))),Size))/TI + lambda*betta;

Size=N-M+2;
La_M_temp=zeros(Size, Size);
La_M_temp(1,1) = -N.*alpha.*(1-betta).*lambda_st;
La_M_temp(1,2) =  N.*alpha.*(1-betta).*lambda_st;
for i = 2:(Size-1)
    La_M_temp(i,i-1) = mu;
    La_M_temp(i,i)   = -(N-i+1).*alpha.*(1-betta).*lambda_st - mu;
    La_M_temp(i,i+1) = (N-i+1).*alpha.*(1-betta).*lambda_st;
end

M_temp = zeros(Size-1, Size-1);

for i = 1:(Size-1)
    for j = 1:(Size-1)
        M_temp(i,j) = La_M_temp(i,j);
    end
end
Initial_Distrib=zeros(1, Size-1);
Initial_Distrib(1)=1;

[T,Y] = ode45(@(t,y) MooNDD(t,y,M_temp), [0 TI], Initial_Distrib);
for i = 1:(Size-1)
        temp = temp + Y(:,1));
end
    Y(:,Size)=1-temp;

la(3) = - log(1-Y((length(Y(:,Size))),Size))/TI + lambda_st*betta;
```

Within this function, we may see the implementation of numerical Runge-Kutta method for solving the system of ordinary differential equations (18) and (25). The numerical algorithm is run by the built-in `ode45` function in Matlab.

Obtaining the values of $PFD_{avg}, DT, C_{lifecycle}$ for the subsystems of SIS.

The input data, provided into the function:

Table 13. The input data, provided into the function:

Variable in Matlab	Description
arg(1)	MooN architecture for the transmitters subsystem
arg(2)	MooN architecture for the PLCs subsystem
arg(3)	MooN architecture for the actuators subsystem
arg(4)	Common-cause failure factor for transmitters subsystem
arg(5)	Common-cause failure factor for PLCs subsystem
arg(6)	Common-cause failure factor the actuators subsystem
arg(7)	A choice of test interval
arg(8)	A choice on the model of sensor
arg(9)	A choice on the model of PLC
arg(10)	A choice on the model of actuator

The input data, provided in the table above represents the decision variables for the optimization problem.

In addition to the input date, a set of parameters is present within the function. Those parameters provide the necessary description for the particular problem setting.

Table 14. Modelling Parameters

Parameter in the model	Variable in Matlab	Description
LC	Total_time	Duration of the lifecycle, years
d^t	d	Technological incidents rate, 1/hours

μ^t	mu	Technology restoration rate, 1/hours
$C_{prod.loss}$	Loss_of_production	Loss of production, cost_units per hour
C_{loss}	Cost_of_accident	Cost of the accident, cost_units
$C_{startup}$	C_startup	Cost of a start-up, cost_units
SD	Downtime1	Facility restoration time after a spurious trip, hours
δ	discount	Discount factor, percent
$\%Pr^{tr}$	Percent_spare_parts_sensors	Percentage of spare parts for sensors subsystem
$\%Pr^{ls}$	Percent_spare_parts_PLC	Percentage of spare parts for PLCs subsystem
$\%Pr^{fc}$	Percent_spare_parts_actuators	Percentage of spare parts for actuators subsystem

Table 15. The output data, provided by the function:

Parameter in the model	Variable in Matlab	Description
PFD_{avg}	obj(1)	Average probability of failure on demand
DT	obj(2)	Facility's unavailability
$C_{lifecycle}$	obj(3)	Cost of the lifecycle

```
function obj = prog1(arg)
temp1 = DB_structures(arg(1));
M_sensor = temp1(1);
N_sensor = temp1(2);

temp2 = DB_structures(arg(2));
M_PLC = temp2(1);
N_PLC = temp2(2);

temp3 = DB_structures(arg(3));
M_actuator = temp3(1);
N_actuator = temp3(2);

btemp1 = DB_betta(arg(4));
betta_sensors = btemp1(1);

btemp2 = DB_betta(arg(5));
betta_PLCs = btemp2(1);

btemp3 = DB_betta(arg(6));
```

```
betta_actuators = btemp3(1);

TI = DB_TI(arg(7));
LC_time = Total_time*365*24;

par1 = DB_SENSORS(arg(8));
par2 = DB_PLCS(arg(9));
par3 = DB_ACTUATORS(arg(10));
La_sensors   = structure(M_sensor, N_sensor, par1(1), betta_sensors,
par1(2), par1(3), par1(4), TI);
La_PLCs      = structure(M_sensor, N_sensor, par2(1), betta_PLCs,
par2(2), par2(3), par2(4), TI);
La_actuators = structure(M_sensor, N_sensor, par3(1), betta_actuators,
par3(2), par3(3), par3(4), TI);

La_matrix = zeros (9,9);
La_matrix(1,2) = La_sensors(1);
La_matrix(1,3) = La_PLCs(1);
La_matrix(1,4) = La_actuators(1);
La_matrix(1,5) = La_sensors(2)   + La_sensors(3);
La_matrix(1,6) = La_PLCs(2)      + La_PLCs(3);
La_matrix(1,7) = La_actuators(2) + La_actuators(3);
La_matrix(1,8) = d;
La_matrix(1,1) = -
(d+La_sensors(1)+La_sensors(2)+La_sensors(3)+La_PLCs(1)+La_PLCs(2)+La_PLCs(
3)+La_actuators(1)+La_actuators(2)+La_actuators(3));

La_matrix(2,5) = La_PLCs(3)    + La_actuators(3);
La_matrix(3,6) = La_sensors(3) + La_actuators(3);
La_matrix(4,7) = La_sensors(3) + La_PLCs(3);

La_matrix(2,9) = d;
La_matrix(3,9) = d;
La_matrix(4,9) = d;

La_matrix(2,2) = -(d + La_PLCs(3)    + La_actuators(3));
La_matrix(3,3) = -(d + La_sensors(3) + La_actuators(3));
La_matrix(4,4) = -(d + La_sensors(3) + La_PLCs(3));

La_matrix(5,1) = par1(3);
La_matrix(6,1) = par2(3);
La_matrix(7,1) = par3(3);
La_matrix(5,5) = -par1(3);
La_matrix(6,6) = -par2(3);
La_matrix(7,7) = -par3(3);
La_matrix(8,1) = mu_tech;
La_matrix(8,8) = -mu_tech;

La_m_temp=zeros(8,8);
for i = 1:8
    for j = 1:8
        La_m_temp(i,j) = La_matrix(i,j);
    end
end
Initial_Distrib=zeros(1, 8);
Initial_Distrib(1)=1;

[T,Y] = ode45(@(t,y) ESD_and_Technology(t,y,La_m_temp), [0 TI],
Initial_Distrib);
Y(:,9)=1-Y(:,1)-Y(:,2)-Y(:,3)-Y(:,4)-Y(:,5)-Y(:,6)-Y(:,7)-Y(:,8);

T_unavailability = trapz(T,Y(:,5)) + trapz(T,Y(:,6)) + trapz(T,Y(:,7));
T_down_wfunctioningSIS = trapz(T,Y(:,8));
```

```
Unavailability = 0;
Downtime = 0;
Unavailability = T_down_wfunctioningSIS + trapz(T,Y(:,9)); %OUTPUT
Downtime = T_down_wfunctioningSIS + T_unavailability;

k=ceil(LC_time/TI);
for i=2:k
    Initial_Distrib(1)=Y(length(Y(:,1)),1);
    Initial_Distrib(2)=0;
    Initial_Distrib(3)=0;
    Initial_Distrib(4)=0;
    Initial_Distrib(5)=Y(length(Y(:,5)),5)+Y(length(Y(:,2)),2);
    Initial_Distrib(6)=Y(length(Y(:,6)),6)+Y(length(Y(:,3)),3);
    Initial_Distrib(7)=Y(length(Y(:,7)),7)+Y(length(Y(:,4)),4);
    Initial_Distrib(8)=Y(length(Y(:,8)),8);
    [T,Y] = ode45(@(t,y) ESD_and_Technology(t,y,La_m_temp), [TI*(i-1)
TI*i], Initial_Distrib);
    Y(:,9)=1-Y(:,1)-Y(:,2)-Y(:,3)-Y(:,4)-Y(:,5)-Y(:,6)-Y(:,7)-Y(:,8);

    T_unavailability = trapz(T,Y(:,5)) + trapz(T,Y(:,6)) + trapz(T,Y(:,7));
    T_down_wfunctioningSIS = trapz(T,Y(:,8));
    Unavailability = Unavailability + T_down_wfunctioningSIS +
trapz(T,Y(:,9));
    Downtime = Downtime + T_down_wfunctioningSIS + T_unavailability;
end

PFD_avg = Y(length(Y(:,9)),9);
STR = -log(1-Y(length(Y(:,5)),5)-Y(length(Y(:,6)),6)-
Y(length(Y(:,7)),7))./LC_time;

obj(1) = PFD_avg;
obj(2) = Unavailability;

C_purch_sens = par1(5);
C_design_sens = par1(6);
C_install_sens = par1(7);
C_consumption_s = par1(8);
C_purch_PLC = par2(5);
C_design_PLC = par2(6);
C_install_PLC = par2(7);
C_consumption_p = par2(8);
C_purch_act = par3(5);
C_design_act = par3(6);
C_install_act = par3(7);
C_consumption_a = par3(8);

C_prev_maint_s = par1(9);
C_prev_maint_p = par2(9);
C_prev_maint_a = par3(9);

C_repair_perhour_s = par1(10);
C_repair_perhour_p = par2(10);
C_repair_perhour_a = par3(10);

C_of_test_s = par1(11);
C_of_test_p = par2(11);
C_of_test_a = par3(11);

betta_ps = btemp1(2);
betta_ds = btemp1(3);
betta_is = btemp1(4);
betta_cs = btemp1(5);
```

```
betta_pp = btemp2(2);
betta_dp = btemp2(3);
betta_ip = btemp2(4);
betta_cp = btemp2(5);
betta_pa = btemp3(2);
betta_da = btemp3(3);
betta_ia = btemp3(4);
betta_ca = btemp3(5);

C_procurement = C_startup + (C_purch_sens*betta_ps + C_design_sens*betta_ds
+ C_install_sens*betta_is)*N_sensor + (C_purch_PLC*betta_pp +
C_design_PLC*betta_dp + C_install_PLC*betta_ip)*N_PLC +
(C_purch_act*betta_pa + C_design_act*betta_da +
C_install_act*betta_ia)*N_actuator;
Cost_operations = (C_consumption_s.*betta_cs+C_prev_maint_s).*N_sensor +
(C_consumption_p.*betta_cp+C_prev_maint_p).*N_PLC +
(C_consumption_a.*betta_ca+C_prev_maint_a).*N_actuator +
(12./TI).*(N_sensor.*C_of_test_s + N_PLC.*C_of_test_p +
N_actuator.*C_of_test_a);
Cost_risk = (C_repair_perhour_s + C_repair_perhour_p + C_repair_perhour_a +
Loss_of_production).*Downtime1.*STR + Percent_spare_parts_sensors.*N_sensor
+ Percent_spare_parts_PLC.*N_PLC +
Percent_spare_parts_actuators.*N_actuator.*STR +
Cost_of_accident.*d.*PFD_avg;

Cost_LC = C_procurement + pvfix(discount/Total_time, Total_time,
(Cost_operations + Cost_risk), 0, 0);
obj(3) = Cost_LC;
```

In addition to the functions, the algorithm refers to several database files, containing all the necessary information regarding the possible subsystem structure, nomenclature of elements, reliability characteristics of each element, as well as the cost associated with the choice of a particular hardware component.

3.7 Adaptaion of the Model to Complex SIS Structures

In this work we have so far considered the model for only one control loop of SIS. Usually, SIS consist of several loops, each of those can be modelled and optimized in the manner described above. However, if we're speaking about ESD systems, the view of the loop can be different.

The purpose of ESD system is to shutdown the technology, which usually implies several actions to be performed. This means that we would get a more complicated view of actuators subsystem architecture. If in case of an incident we need to, for instance, close Valve Group 1 and Valve Groups 2, and each of the valve groups could have the MooN architecture, then in terms of reliability (or, with the help of reliability blog diagram) those two systems will be connected in a series.

The same deduction is applicable for the sensors subsystem. If we have several parameters, for which the critical ranges are defined, and in case one of the parameters enters this range then the full shutdown of the facility is to be implemented. Each particular parameter has a set of sensors that can be organized into a MooN architecture. And the subsystems for each parameter would be connected in a series in terms of reliability.

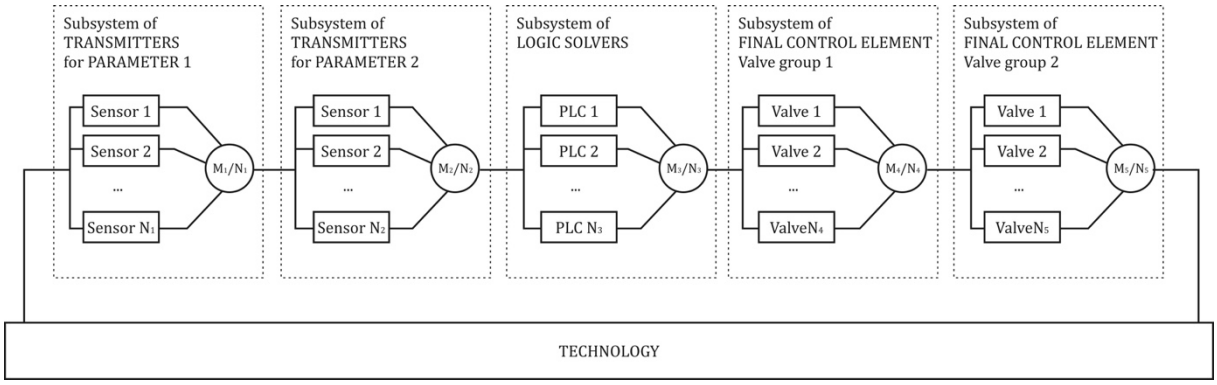

Figure 26. Modified reliability block diagram for the complex ESD system structures

This increases the number of states for the Markov model. The example is given below.

Table 16. Modified table of the Markov process states.

	EMERGENCY SHUTDOWN SYSTEM					Technology
	Transmitters Parameter 1	Transmitters Parameter 2	Logic Solvers	Valves Line 1	Valves Line 1	
1	*working*	*working*	*working*	*working*	*working*	*working*
2	*failed (DU)*	*working*	*working*	*working*	*working*	*working*
3	*working*	*failed (DU)*	*working*	*working*	*working*	*working*
4	*working*	*working*	*failed (DU)*	*working*	*working*	*working*
5	*working*	*working*	*working*	*failed (DU)*	*working*	*working*
6	*working*	*working*	*working*	*working*	*failed (DU)*	*working*
7	*under maintenance*	*working*	*working*	*working*	*working*	*stopped*
8	*working*	*under maintenance*	*working*	*working*	*working*	*stopped*
9	*working*	*working*	*under maintenance*	*working*	*working*	*stopped*
10	*working*	*working*	*working*	*under maintenance*	*working*	*stopped*
11	*working*	*working*	*working*	*working*	*under maintenance*	*stopped*
12	*working*	*working*	*working*	*working*	*working*	*stopped (due to incident)*
13	*failure*					*incident*

4 COMPUTATIONAL EXAMPLE

4.1 Description of a Case

We will consider application of the SIS design methodology proposed in Chapter 3 on the example of heating facility project. The data was provided by Rosneft, one of the largest vertically integrated companies in Russia.

Line heater is a technological unit often used in oil and gas production and treatment infrastructure. Its purpose is to heat oil emulsions, highly viscous oil for easier transportation via pipelines. Basically, the unit is a furnace, where the energy of burning the fuel gas is used for heating the flow through the line.

The following documents were analyzed:

- Technical and commercial proposal
- Request for project proposal
- The automation system project documentation

According to GOST R 51330.17-99 Electrical apparatus for explosive atmospheres (adaptation of IEC 60079-18-92), for the line heater the Apparatus Group of the hazardous, explosive atmosphere is *IIA* (which indicates that the facility belongs to the most dangerous class processes).

The parameters which were identified as potentially dangerous, are provided in the table below.

Table 17. Identification of critical range for technological parameters.

#	Parameter / Process Value	Critical Range	Frequency of occurrence, 1/year
1	Temperature of the arc	Threshold HH = 850 °C	0,03
2	Flame detected on main burner	*No flame* detected	0,08

In case any of the events, described in Table 17 takes place, the following actions are to be taken:

- open the valve for discharging the fuel gas to flare;
- closing valves on the input and output lines.

4.2 Project Documentation Analysis

The information about the project had been provided by Russian oil and gas company Rosneft in the form of project documentation. The documentation consists of the several stages, which were analyzed for the purpose of highlighting the requirements to the safety systems.

The analysed documentation corresponds to the following system implementation work phases (see table below).

Table 18. Scope of system implementation work done in the framework of the project, corresponding to the requirements of GOST 34.601-90 "Computer-Aided Systems. Implementation Milestones".

Milestones	Work Phases	Contractor
1. Requirements definition	1.1. Facility survey and grounding of PCS necessity	Design developer
	1.2. Definition of user requirements to PCS	Design developer
	1.3. Development of completed work report and requisition for PCS development (top level specifications)	Design developer
2. PCS development	2.1. Facility study	Design developer
	2.2. Due research engineering	Design developer
	2.3. Development of PCS concept options, meeting user's requirements	Design developer
	2.4. Preparation of completed work report	Design developer
3. Requirements Specification	Development and approval of Requirements Specification for PCS implementation	Design developer & Operator company
4. Engineering design	4.1. Development of concepts for the system and its parts	Design developer
	4.2. Design development for PCS and its parts	Design developer
	4.3. Development and issue of documents for PCS components supply and (or) Requirements Specification for their design	Design developer
	4.4. Development of task orders for automated facility interfacing parts design engineering	Design developer
5. Detailed design	5.1. Development of detailed design for the system and its parts	Engineering company (System

		integrator)
	5.2. Software development or adaptation	System integrator
6. Commissioning	6.1. Automated facility preparation for PCS commissioning	System integrator
	6.2. Personnel training	System integrator
	6.3. PCS packaging with supplied components (software and hardware, software and hardware systems, information tools).	System integrator
	6.4. Civil & installation works	System integrator
	6.5. Pre-commissioning	System integrator
	6.6. Pre-testing	System integrator
	6.7. Pilot operation	System integrator
	6.8. Acceptance tests	System integrator
7. PCS support	7.1. Works according to warranty	System integrator
	7.2. Post-warranty service	System integrator

Below, there's an excerpt from the actual *Requirement specification* document developed by Rosneft during the "Request for project proposal" phase.

Requirements for emergency shutdown system

Emergency shutdown system (ESD) must control process critical parameters and stop process system in case of parameter deviations from set points and on operator's manual intervention.

Emergency shutdown system (ESD) shall be equipped with continuous control and alert facilities. The system shall allow restart of the system or unit only after shutdown cause removal and failure alarm reset or positive locking.

ESD system shall be based on dedicated primary instruments and actuators. Emergency message and event sequence recorders shall be provided.

Gas detectors shall be installed at process sites and production facilities.

Failure of ESD system detectors shall not cause any automatic actions for process equipment.

ESD alarm signals shall be transmitted to individual ESD WKS. Operator WKS is a human-machine interface element for tripping functions, and these functions shall provide the following at a minimum:

- *review mnemonic diagrams (video frames) with warning signal output;*
- *detailed mnemonic diagrams (video frames) with warning signal output, details of failure recovery and suppression;*
- *control of blocking and suppression for inputs and outputs;*
- *confirmation and reset of warning signals.*

Process operational system facilities shall be provided for cutoff devices for periodic inspection of control circuit integrity, and instrumentation monitoring system (IMS) shall be provided with functional testing subsystem for cutoff devices with partial stroke. In this case protective function always has priority over test function and, if necessary, gives the closing signal.

Analog input monitoring shall be provided for signal verification. In case of external signal shutdown or overrun the warning signal shall be sent to operator.

Plant restart shall be possible only after manual reset (acknowledgment).

Configuration of ESD system shall be provided for process transfer to safe condition in case of equipment failure.

ESD system shall also include the following components and facilities at a minimum:

- *ESD visualization system being a part of operator workstation software;*
- *data acquisition and control generation devices (ESD PLC with input/output modules) located in system cabinets;*
- *industrial communication modules;*
- *marshalling cabinets;*

Event sequence recording system (recorder) (ESR) shall be provided for reception and recording the sequence of events generated by ESD system and in some cases by DCS system with assignment of the event date and time as well as sequence recording on intrinsic magnetic rigid disks for further printing and analysis.

The presented passage from the documentation reveals that the requirements to the design implementation of the safety systems are insufficient and not specific enough. Therefore, further the attempt of providing such requirements will be made by applying the modelling framework described in the previous chapter. It is proposed that

the configuration of ESD system that will be obtained further can be used as a starting point for the phase “Detailed design”.

4.3 Data for the Optimization Run

The equipment alternatives are given in the following tables: Table 19 through Table 22.

Table 19. Database of temperature sensors.

Alternatives	1	2	3	4	5
Model	Metran-281-Exia	TPU 0304	Yokogawa YTA310	Rosemount 3144P	ABB TPS300
Dangerous failure rate 1/hour	$2 \cdot 10^{-5}$	$2{,}86 \cdot 10^{-5}$	$5 \cdot 10^{-6}$	$9 \cdot 10^{-7}$	$7{,}14 \cdot 10^{-7}$
Spurious trip rate, 1/hour	$1 \cdot 10^{-5}$	$1 \cdot 10^{-5}$	$4{,}6 \cdot 10^{-6}$	$4{,}6 \cdot 10^{-7}$	$4{,}8 \cdot 10^{-7}$
Diagnostic coverage, %	60%	60%	89%	80%	90%
Purchase cost, RUB	8000	5000	15000	20000	30000
Design cost, RUB	600	300	300	250	270
Installation cost, RUB	300	350	300	250	250
Consumption cost per year, RUB	400	150	350	300	200
Maintenance cost per year, RUB	4000	3000	2500	2500	2700
Repair cost per hour, RUB	50	50	40	40	40
Test cost, RUB	100	90	100	80	100

Table 20. Database of flame detectors.

Alternatives	1	2
Model	Parus-002 UF-1	SNP-OE-1
Dangerous failure rate 1/hour	$1 \cdot 10^{-5}$	$1{,}67 \cdot 10^{-5}$
Spurious trip rate, 1/hour	$1 \cdot 10^{-5}$	$1 \cdot 10^{-5}$
Diagnostic coverage, %	75%	80%

Purchase cost, RUB	12000	8000
Design cost, RUB	500	400
Installation cost, RUB	500	500
Consumption cost per year, RUB	200	250
Maintenance cost per year, RUB	2000	2000
Repair cost per hour, RUB	40	50
Test cost, RUB	80	50

For the sensors subsystem, the percentage of spare parts is fixed as 20%.

Table 21. Database of programmable logic controllers.

Alternatives	1	2	3
Model	Rockwell ControlLogix 5555	Emerson DeltaV SLS1508	ABB 800xA
Dangerous failure rate 1/hour	$9{,}11 \cdot 10^{-7}$	$1{,}25 \cdot 10^{-6}$	$5{,}96 \cdot 10^{-6}$
Spurious trip rate, 1/hour	$8{,}33 \cdot 10^{-7}$	$1{,}09 \cdot 10^{-6}$	$5{,}5 \cdot 10^{-6}$
Diagnostic coverage, %	90%	98%	97%
Purchase cost, RUB	450000	250000	150000
Design cost, RUB	20000	15000	12000
Installation cost, RUB	10000	5000	10000
Consumption cost per year, RUB	10000	10000	10000
Maintenance cost per year, RUB	40000	30000	40000
Repair cost per hour, RUB	100	300	100
Test cost, RUB	2000	2000	2000

For the sensors subsystem, the percentage of spare parts is fixed as 30%.

Table 22. Database of valves.

Alternatives	1	2
Model	Roost 3-km series	Fisher GX
Dangerous failure rate 1/hour	$6{,}67 \cdot 10^{-5}$	$4 \cdot 10^{-5}$
Spurious trip rate, 1/hour	$3{,}33 \cdot 10^{-5}$	$3{,}33 \cdot 10^{-5}$
Diagnostic coverage, %	10%	20%
Purchase cost, RUB	16000	30000
Design cost, RUB	13000	18000
Installation cost, RUB	10000	5000
Consumption cost per year, RUB	10000	10000
Maintenance cost per year, RUB	10000	10000
Repair cost per hour, RUB	800	800
Test cost, RUB	1000	1000

For the final control elements subsystem, the percentage of spare parts is fixed at 20%.

The following constraints are applied with regards to the feasible architectures:

- feasible architectures for the transmitter subsystem: 1oo1, 1oo2, 1oo3, 1oo4, 2oo2 and 2oo3.
- feasible architectures for the logic solver subsystem: 1oo1, 1oo2, 1oo3, 1oo4 and 2oo3.
- Feasible architectures for the final control elements: 1oo1, 1oo2, 1oo3, 1oo4, 2oo2, 2oo3.

The following constraints are applied with regards to the common-cause failure factor:

- The value for β-factor is 0,035 for the standard solution with regards to the electrical separation of the circuits of the devices.

- The value for β-factor is 0,02 if the additional measures of the electrical separation are applied.

The values of cost modifiers, corresponding to the decision making on the electrical separation are estimated in the table below:

Table 23. Cost modifiers corresponding to β-factor.

Cost modifier	Standard alternative	Additional electrical separation
Purchase cost modifier β_{purch}	1,15	1,35
Design cost modifier β_{des}	1,05	1,1
Installation/commissioning cost modifier β_{inst}	1,1	1,25
Consumption cost modifier β_{cons}	1,2	1,35

The repair rate (or restoration rate) is pessimistically estimated as 0,125 hour^{-1} because of the requirements of repair within 8 hours since the failure is detected by the diagnostics. This value is pessimistic, because, according to chief project engineers department statement, most of the failed tools are fixed within 2 hours from the moment when a failure is detected.

With regards to the duration of the test interval (*TI*), it can vary from 1 month to 24 months with 1 month step.

The duration of the *Lifecycle* is 12 years.

The down time of the technology after the spurious tripping is 48 hours.

The losses due to the shutdown are 2500 RUB per hour.

The expected loss due to one hazardous event occurrence is estimates as 10 000 000 RUB.

4.4 Results of the Optimization Run

The problem of choosing the SIS specification was run in Matlab with the use of `gamultiobj` solver within the Optimization toolbox. The following settings for multi-objective genetic algorithm were applied:

- population: 200 individuals, initial population created with the uniform distribution.
- number of generations: 300,
- selection function: tournament (built-in function),
- generational gap: 0,8 (or 80%),
- crossover fraction 0.8, single-point crossover,
- mutation function: Gaussian.

The problem was solved in the unconstrained formulation, i.e. only the three objective function values (probability of failure on demand, downtime and lifecycle cost) were sought to be minimized, and the upper and lower bounds on choosing the alternatives from the databases of equipment were provided.

The resulting Pareto-front is demonstrated along with the initial population on the figures blow. Figure 27 demonstates the 3-dimentional plot of all the values of the objective function for all obtained solutions. The Pareto-frintier is given in black "*x*" marks. In total we received 24 solutions in the Pareto-frontier. Figure 28 demonstrated the relations between the values of each pair of objectives for the solutions in the Pareto-frontier.

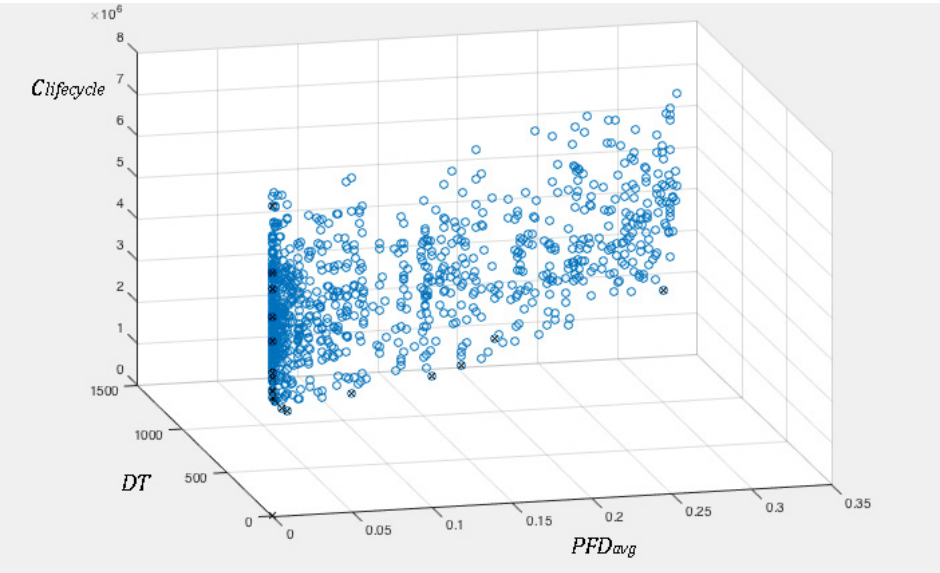

Figure 27. Results of optimization run.

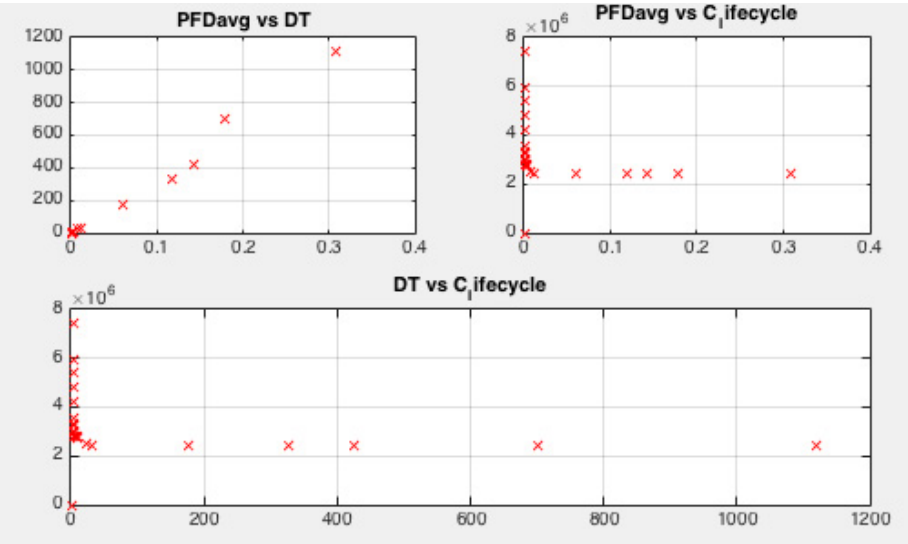

Figure 28. Pairwise comparison of the values of objectives.

4.5 Discussion of the Results

From the results in Figure 28 we can conclude that PFD_{avg} and the unavailability time are generally not conflicting objectives. This is clear because the failure of the equipment contributes greatly into the value of the unavailability time.

PFD_{avg} and $C_{lifecycle}$ are conflicting oblectives with regards to Pareto-optimal front. This can also be observed from consideration of the cost of hazards occurrence, i.e. the cost of a catastrophic event, which is a considerably large number.

System's downtime and its lifecycle cost also demonstrate conflictive relation. The relation is similar to the PFD_{avg} and $C_{lifecycle}$ relation, because failures are the domninant factor in the unavailability consideration.

As a drawback of the applied methodology we can observe Figure 27 and Figure 28 that the distribution of the solution in the Pareto-frontier is non-uniform. This is obviously the issue of the heuristic algorithm applied in this work. There are methods of improving the quality of this distribution. For example, in (Torres-Echeverria and Thompson 2007) the authors propose to run the solver 10 times, and provide the optimal solution from each run into the following run as a new initial population. The authours claim that this provides more diversity and results in a better Pareto-front.

Now we should make a decision on choosing the architecture for the ESD system. We have obtained 23 solutions; however we need to achieve a certain level of

safety integrity. In accordance with the requirements, stated for ESD in Table 6, we need to achieve SIL III and the PFD_{avg} at the level of $1{,}7 \cdot 10^{-4}$. This is derived from:

$$PFD_{avg} = \frac{F_{tolerable}}{d^t}, \quad (59)$$

Here, $F_{tolerable} = 1 \cdot 10^{-6}$ is our target frequency of the hazardous events occurrence.

If we apply this constraint for the safety integrity level to our results, i.e. we choose among our 23 solutions only those which have $PFD_{avg} \leq 1{,}7 \cdot 10^{-4}$, we would end up with only 10 solutions. Additional considertations can be applied to choose the best alternative among the remaining 10. For example, we can address the value of estimated losses due to potential incidents and the total downtime. If we apply such a kind of thinking, we would obtain one solution, for which the specification is provided further:

Transmitters subsystem: 1oo4.

PLC subsystem: 1oo2.

Actuators subsystem: 1oo1.

Temerature sensor: Yokogawa YTA310.

Flame detector: Parus-002 UF-1

PLC: Emerson DeltaV SLS1508.

Valves: Fisher GX.

Test interval: 2 months.

Additional electrical separation is applied to the transmitters subsystem, and not applied to the PLCs and valves subsystems.

For such a specification, the values of the objective functions are as follows:

$PFD_{avg} = 4{,}0108 \cdot 10^{-6}$,

$DT = 192\ hours$ over the 12 years lifecycle, and

$C_{lifecycle} = 3\ 571\ 978\ RUB$ over the 12 years lifecycle.

4.6 ESD System Design for the Required Value of Risk Reduction Factor

In this section we will address the methodology that was applied in order to obtain the specification for the ESD system design by the engineering organization, which implemented the considered project.

For the ESD system design in accordance with IEC 61508 the following steps are applied:

1. The frequency of occurrence of critical incidents for each critical parameter in the absence of the ESD are determined. Note that in the absence of layers of protection the frequency of incidents is equal to the frequency of accidents.

2. The acceptable frequency of incidents for each critical area is determined.

3. The required value of the risk reduction factor (RRF), for each critical area, to ensure an acceptable frequency accidents and accordingly to ensure the third class of risk. For the chosen value of the risk reduction factor is also possible to determine the required value of safety integrity level (SIL), according to the tables provided in IEC 61508.

4. The specification for ESD that provides the desired RRF level for each critical area.

It should be noted that as a result of identifying the ESD, to achieve the required RRF (and therefore acceptable frequency), turns out some many variants of the ESD system are acceptable options and there is no clear guidance on which a decision-maker should choose. In this perspective it is generally common to choose the variant of ESD, which provides the acceptable frequency of accidents at a minimal cost. The example of the conducted analysis is provided below.

Table 24. The required values of RRF.

№	Hazards	Occurrece frequency [1/year]	Acceptable frequency [1/year]	Required RRF
1	Temperature of the arc	0,03	0.001	30
2	The presence of the flame on the 1st basic burner	0.08	0.001	80

To ensure the required values RRF and respectively the desired frequency of accidents it is necessary to carry out the desing of ESD. For this the same alternatives as provided in the data in section 4.2 are used, however, those options of the ESD design that provide the required RRF, were considered. Following this same problem setting, the engineering organization came up with this specification as an alternative that was implemented in practice:

Transmitters subsystem: 1oo1.

PLC subsystem: 1oo1.

Actuators subsystem: 1oo2.

Temerature sensor: Rosemount 3144P

Flame detector: Parus-002 UF-1

PLC: Rockwell Allen-Bradley ContolLogix 5555.

Valves: Fisher GX.

Test interval: 3 months.

Additional electrical separation is not applied.

For such a specification, the values of the objective functions are as follows:

$PFD_{avg} = 1{,}6376 \cdot 10^{-4}$,

$DT = 315\ hours$ over the 12 years lifecycle, and

$C_{lifecycle} = 3\ 933\ 558\ RUB$ over the 12 years lifecycle.

Below the comparison of the obtained solution with 10 solutions from the obtained Pareto-front (including the requirement for the SIL) is demonstrated. Figure 29 depicts the 10 solution from the Pareto-front with red "x" marks, and the specification obtained in this section with blue "o" mark.

The solution, intended to provide the necessary level of risk-reduction, does indeed satisfy the requirement for average probability of failure on demand (62). However, we can observe from Figure 29 that this solution is strictly dominated by 5 other solution from Pareto-front. And with regards to the expected downtime, the last obtained solution is much worse than the solution from the Pareto-front.

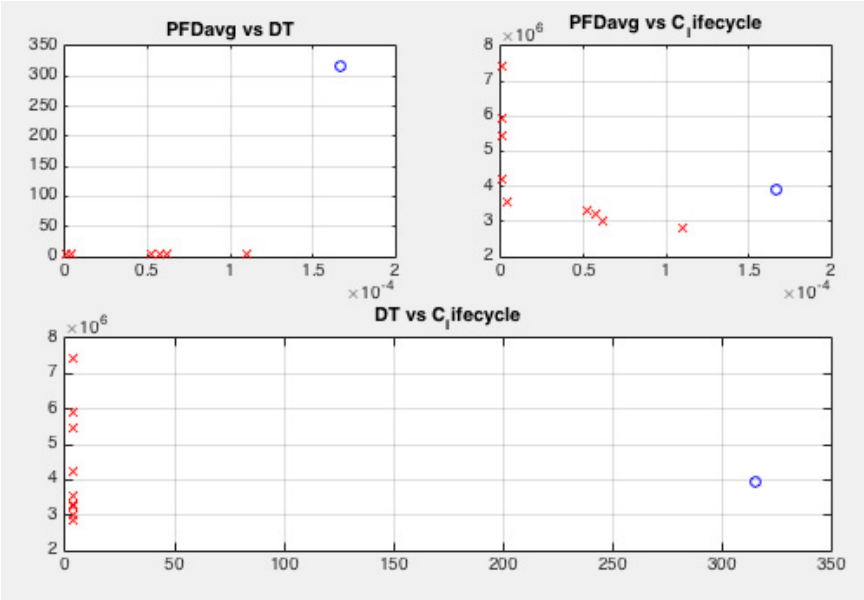

Figure 29. Comparison of solutions.

5 CONCLUSIONS AND SUGGESTIONS FOR FURTHER RESEARCH

Consideration of dfferent kinds of uncertainty is a very importand aspect of any planning work. Its importance become even more significant, when we're addressing the operations implemented in highly-haardous environments.

Oil and gas industry is crucial for modern society. The operations of petroleum production are associated with significant dangers, and thus the consideration of hazards and their consequences should not be ignored.

Most aspects of safety are considered during the planning stage of any particular froject. The very first measures that are planned to be implemented are the barriers that help preveting the potentially hazardous situations. In this work we have addressed the issues of planning the safety system for the petroleum production infrastructure. In petroleum industry, the automated control systems play a significant role in preventing the hazards from occurring. The basic level is represented by the districbuted control system. The most important safety measure is the emergency shutdown system, which provides the largest risk reduction by safely shutting down the process of technology. There are international standards adapted in many countries for those systems. The standards name the systems "Safety Instumented Systems".

Modelling and designing the particular architecture of SIS is an exhausting process, which requires a lot of knowledge of the process itself, of the hardware tools, its reliability characteristics, and the safety indicators that provide the comprehensive description of the system behaviour.

This work is focused on the application of SIS to the infrastructure planning in Russian engineering practice. We have observed on the examples from Russian researchers and from Russian engineering companies that the methods and techniques applied to SIS design fall behind the achievement of state-of-the-art research.

Designing the specification of SIS is a very important decision, implemented by the engineering organization when they plan the infrastructures for oil and gas production. In order to obtain the good alternatives for the SIS specification we have applied the multicriteria optimization which included both reliability and economic evaluation approaches. Introducing a SIS and with consideration of the processes' safety

integrity proves to be economically efficient, because it helps reduce the total cost of the lifecycle. The Pareto-optimal set has far better trade-offs (e.g. must lower costs) that the initial solutions.

It was seen that the optimization algorithm in the given problem setting gives preference to components with better reliability specifications in spite of their higher acquisition cost. Reduction of common cause failure is also important and at the same time costly decision. It has been noted that the proposed problem setting guides the algorithm to choose the lower value for the factor for architectures with a high level of redundancy.

As a suggestion for further research the author proposes elaborating the models by incorporating the diverse redundancy into the model. In this work, we have considered different schemes of redundancy, however for each alternative we have considered one and the same model of the tool. The reliability characteristics of the safety system could be improved by introducing the different models of a similar kind of the equipment into the redundant solutions.

Another suggestion for further developments in the field of modelling of SIS functioning with a particular process by introducing different alternatives for testing policies and the approaches to parallel/sequential/staggered testing schemes. Such modelling could be used to determine the number of employees and their schedules. This is a very important direction of work, because many oil and gas production site in Russia are located in underpopulated regions, and the transportation of staff to the working places (the facilities) and back is highly inconvenient and costly. At the same time, given that employees live far from their workplace, they work 3 to 6 months shifts. In this particular setting, it is important to estimate the number of workers and working crews that should be available for conducting the testing procedures, ensuring the correct work of the facility.

LIST OF REFERENCES

[1] ABB (Asea Brown Boveri Ltd.), *"Best Practices For Avoiding Common Cause Failure And Preventing Cyber Security Attacks In Safety Systems",* 2012. Available online. https://library.e.abb.com/public/3e234b767729aaa0c1257aa60064b129/3BUS095673_en_Whitepaper_-_The__Rocky_Relationship_between_Safety_and_Security.pdf

[2] Andrews, J.D. and Clifton A. Ericson. 2000. *Fault tree and Markov analysis applied to various design complexities.* Conference Papers and Contributions (Aeronautical and Automotive Engineering). System Safety Society. URI: https://dspace.lboro.ac.uk/2134/3656. In Proc of 18th International System Safety Conference. Texas, USA, 2000.

[3] Angeline P. J. 1996. *Genetic programming's continued evolution.* Chapter 1 in K.E. Kinnear, Jr. and P.J. Angeline (Eds.), Advances in Genetic Programming 2. Cambridge, MA: MIT Press, p. 1 -20. 1996.

[4] Arendt, L. S., and D. K. Lorenzo. 2000. *"Evaluating process safety in the chemical industry."* A User's Guide to Quantitative Risk Analysis, CCPS. 2000.

[5] Aronofsky, J. S. and A. C. Williams. 1962. *"The Use of Linear Programming and Mathematical Models in Under-Ground Oil Production."* Management Science 8 (4):394-407.

[6] Arroyo, J. E. C. 2003. *"Heurísticas e Metaheurísticas para Otimização Combinatória Multi- objetivo (in portuguese)"*, PhD Thesis, UNICAMP, SP - Brazil.

[7] Baker, A., P. Croucher and A. Rushton. 2006. *The handbook of logistics and distribution management.* London and Philadelphia: Kogan Page.

[8] Berkeley, D., P. C. Humphreys, and R. D. Thomas. 1991. *"Project risk action management. "* Construction Management and Economics 9*, № 1 (1991): 3-17.*

[9] Bohannon, John M. 1970. *"A linear programming model for optimum development of multi-reservoir pipeline systems."* Journal of Petroleum Technology 22 (11):1,429-1,436.

[10] Bradley, H.B. 1987. *Petroleum engineering handbook.* United States: Society of Petroleum Engineers, Richardson, TX. http://www.osti.gov/scitech/biblio/5929149

[11] Bukowski, J. 2001. *Modeling and analyzing the effects of periodic inspection on the performance of safety-critical systems.* IEEE Transactions on Reliability, 50:321–329.

[12] Bukowski, J. 2006a. *Incorporating process demand into models for assessment of safety system performance.* In Proceedings of RAMS'06 Symposium, Alexandria, VI, USA.

[13] Bukowski, J. 2006b. *Using Markov models to compute PFDave when repair times are not exponentially distributed.* In Proceedings of the annual reliability and maintainability symposium, Newport Beach, CA, USA.

[14] Bukowski, J. V. and Lele, A. 1997. *Case for architecture-specific common cause failure rates and how they affect system performance.* In Proceedings of the Annual Reliability and Maintainability Symposium, pages 153–158.

[15] CCPS. 2007. *Safe and Reliable Instrumented Protective Systems.* Center for Chemical Process Safety.Wiley Interscience. New Jersey, USA.

[16] Chebouba, A, Farouk Yalaoui, A Smati, Lionel Amodeo, K Younsi, and A Tairi. 2009. *"Optimization of natural gas pipeline transportation using ant colony optimization."* Computers & Operations Research 36 (6):1916-1923.

[17] Cramer, E. and U. Kamps*. Sequential k-out-of-n Systems.* Department of Mathematics, University of Oldenburg, D-26111 Oldenburg, Germany. https://www.researchgate.net/publication/239546267_Sequential_k-out-of-n_Systems_Summary_and_References

[18] Deb, K. 2001. Multiobjective optimization using evolutionary algorithms. John Wiley and Sons LTD. Chichester, UK, 2001.

[19] Deb, K. 2008. Multiobjective optimization using evolutionary algorithms, John Wiley & Son.

[20] Dey, P. K. 2001. *"A risk-based model for inspection and maintenance of cross-country petroleum pipeline."* Journal of Quality in Maintenance Engineering 7 (1):25-41.

[21] DIN V 19250. *Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen.* Berlin, 1994.

[22] DIN/VDE 0801. *Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben.* Berlin, 1990.

[23] Dugan, J., S. Bavuso and M. Boyd. 1992. *Dynamic fault tree models for fault tolerant computer systems.* IEEE Transactions on Reliability 1992;41(3):363-377.

[24] Dziubinski, M., M. Fratczaka, and A. S. Markowski. "Aspects of risk analysis associated with major failures of fuel pipelines." Journal of Loss Prevention in the Process Industries 19 (2006): 399–408.

[25] Fedorov, Y. N. 2008. *Engineer Manual PCS. Design and development: teaching practical manual.* Moscow: INFA – Engineering, (in Russian language).

[26] Frair, L. C. 1973. *"Economic Optimization of Offshore Oilfield Development."* PhD Dissertation., University of Oklahoma, Tulsa, OK.

[27] GAO, Pipeline Safety. 2012. *Collecting Data and Sharing Information on Federally Unregulated Gathering Pipelines Could Help Enhance Safety.* GAO-12-388. Washington, DC: US Government Accountability Office (22 Mar 2012). Accessed 13 Jun 2012. Available: http://www. gao. gov/products/GAO-12-388

[28] Goble, W. M. and Brombacher, A. C. 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):145–148.

[29] Goble, W.M. 1998*. Control Systems Safety Evaluation & Reliability.* 1998. The Instrumentation, Systems and Automation Society. Research Triangle Park, NC, U.S.

[30] Goble, W.M., Bukowski J., Brombacher A.C. 1998. *How diagnostic coverage improves safety in programmable electronic systems.* ISA Transactions, 1998, 36(4), 345-350.

[31] Goble, W.M., Cheddie H. 2005. *Safety Instrumented Systems Verification.* The Instrumentation, Systems and Automation Society. Research Triangle Park, NC, US.

[32] Goldberg, David. 1989. *Genetic Algorithms in Optimization, Search and Machine Learning, Addison Wesley.* Founder & President, Big Beacon & Professor Emeritus, UIUC

[33] GOST 27.002-89 *"Reliability in engineering. Terms and definitions".* Minsk: Publishing Standards, 1990, (in Russian language).

[34] GOST 27.301-95 *"Reliability in engineering. Calculation of reliability. The main provisions".* Minsk: Publishing Standards, 1996, (in Russian language).

[35] GOST 27.310-95 *"Reliability in engineering. Analysis of types, consequences and criticality of failures. The main provisions"*. Minsk: Publishing Standards, 1997, (in Russian language).

[36] GOST R 51901-2002 *Reliability managment. Risk analysis of technical systems.* - Moscow: Gosstandart Of Russia, 2002, (in Russian language).

[37] Grefenstette, J. 1993. *GENESIS*, Navy Center for Applied Research in Artificial Intelligence, Navy research Lab., Wash. D.C. 20375-5000.

[38] Gruhn P., Cheddie H. 1998. *Safety Shutdown Systems: Design, Analysis and Justification.* The Instrumentation, Systems and Automation Society. Research Triangle Park, NC, US.

[39] Gupta, Vijay, and Ignacio E Grossmann. 2014. *"Multistage stochastic programming approach for offshore oilfield infrastructure planning under production sharing agreements and endogenous uncertainties."* Journal of Petroleum Science and Engineering 124:180-197.

[40] Hauge, S. and Onshus, T. 2010. *Reliability Data for Safety Instrumented Systems.* SINTEF, Trondheim.

[41] Hauge, S., Hokstad P., Langseth H., Oien K. 2006a. *Reliability Prediction Method for Safety Instrumented Systems.* PDS Data Handbook 2006 edition. SINTEF, Norway.

[42] Hauge, S., Lundteigen, M. A., Hokstad, P., and Håbrekke, S. 2010b. *Reliability Prediction Method for Safety Instrumented Systems.* SINTEF, Trondheim.

[43] Haugland, Dag, Åsa Hallefjord, and Harald Asheim. 1988. *"Models for petroleum field exploitation."* European Journal of Operational Research 37 (1):58-72.

[44] Henselwood, Fred, and Gerry Phillips. 2006. *"A matrix-based risk assessment approach for addressing linear hazards such as pipelines."* Journal of Loss Prevention in the Process Industries 19 (2006): 433-441.

[45] Honeywell International Inc. 2002. *"Safety Instrumented Systems (SIS), Safety Integrity Levels (SIL), IEC61508, and Honeywell Field Instruments".* Industrial Measurement and Control. Accessed 02.05.2016. https://www.honeywellprocess.com/library/support/Public/Documents/Safety%20Instrumented%20Systems%20(SIS),%20Safety%20Integrity%20Levels%20(SIL),%20IEC61508,%20and%20Honeywell%20Field%20Instruments.pdf

[46] HSE, Books. 2003. *Out of Control.* Edited by Second edition. Vol. pages 44 - 45.

[47] HSE, Heatlth and Safety Executive. 2001. *Consultations and discussions* ending during 2001.

[48] IEC. 1998-2005. *IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.* Parts 1-7. International Electrotechnical Commission, Switzerland.

[49] IEC. 2003. *IEC 61511 Functional Safety – Safety Instrumented Systems for the Process Industry Sector.* Parts 1-3. International Electrotechnical Commission, Switzerland.

[50] International Association of Oil & Gas Producers, 2010. *"Major Accidents"* Report No. 434 – 17 March 2010, http://www.ogp.org.uk/pubs/434-17.pdf - accessed 10 March 2016.

[51] International Society of Automation (ISA). 1999. *Standards and Technical Documents.* A Hybrid Autonomous Control System - ISA TECH 1999.

[52] ISA-S84.01.1996. *Application of safety instrumented systems for the process industries.* Instrument Society of America, Research Triangle Park, 1996.

[53] Kabirian, Alireza, and Mohammad Reza Hemmati. 2007. *"A strategic planning model for natural gas transmission networks."* Energy policy 35 (11):5656-5670.

[54] Kanigolla, Anupama. 2014. *Genetic Algorithm.* Department of Computer Science & Engineering Saveetha School of Engineering, Chennai, India. IJSRD - International Journal for Scientific Research & Development| Vol. 2, Issue 05, 2014 | ISSN (online): 2321-0613

[55] Krasheninnikov, M.S., Koshurina, A.A., Kuleshov, A.P., Shapkin, V.A., 2011. *"Equipment for the evacuation of people in a environmental disasters",* NSTU name R.E. Alekseeva, http://www.nntu.ru/sites/default/files/file/conf/ecotechno/2011/ecotechno2011tez.pdf - accessed 10 March 2016. (in Russian language)

[56] Konak, A., Coit, D.W. and Smith, A.E. 2006. *Multi-objective optimization using genetic algorithms: A tutorial.* Reliability Engineering and SystemSafety 2006;91(9):992-1007.

[57] Kuo Way, Zuo Ming J. 2003. *Optimal reliability modeling. Principles and applications.* John Wiley & Sons. New York, USA, ISBN 047127545X

[58] Langeron, Y., Barros, A., Grall, A., and Berenguer, C. 2008. *Combination of safety integrity levels (SILs): A study of IEC61508 merging rules.* Journal of Loss Prevention in the Process Industries, 21:437 449.

[59] Lee, AS, and J. S. Aronofsky. 1958. *"A linear programming model for scheduling crude oil production."* Journal of Petroleum Technology 10 (07):51-54.

[60] Lewis, E.E. 1996 Introduction to reliability engineering. 2nd ed. John Wiley & Sons. New York, USA.

[61] Lukas, Samuel, Arnold Aribowo and Milyandreana Muchri. 2012. *Solving Timetable Problem by Genetic Algorithm and Heuristic Search Case Study.* Universitas Pelita Harapan Timetable, Real-World Applications of Genetic Algorithms, Dr. Olympia Roeva (Ed.), ISBN: 978-953-51-0146-8, InTech, Available from: http://www.intechopen.com/books/real-world-applications-of-genetic-

algorithms/solving-timetable-problem-by- genetic-algorithm-and-heuristic-search-case-study-universitas-pelita-ha

[62] Macdonald, Dave. 2004. *Practical Industrial Safety, Risk Assessment, and Shutdown Systems.* Elsevier Science & Technology Books. January 2004.

[63] Macini, P. and Mesini, E. 2008. *PETROLEUM ENGINEERING – UPSTREAM - The petroleum upstream industry: hydrocarbons exploration and production.* Department of Civil, Environmental and Materials Engineering, University of Bologna, 40131 Italy. http://www.eolss.net/sample-chapters/c08/e6-193.pdf

[64] Marseguerra M., E. Zio and S. Martorell. 2006. *Basics of genetic algorithms optimization for RAMS applications.* Reliability Engineering and SystemSafety 2006;91(9):977-991.

[65] Misumi, Y. and Y. Sato. 1999. *Estimation of average hazardou-eventfrequency for allocation of satety-integrity levels.* Reliability Engineering and System Safety, 66:135–144.

[66] Montanez, George D. 2013. *Information Transmission Through Genetic Algorithm Fitness Maps.* Machine Learning Department, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA. 2013 IEEE Congress on Evolutionary Computation, June 20-23, Cancún, México.

[67] On Safe Lines Quality, 2006. QHSE Software. Health and Safety, and Environmental meandering advice. Accessed 28.04.2016 https://www.onsafelines.com/qhse/qhse-support/index.htm?context=50

[68] Pencheva, Tania, Krassimir Atanassov and Anthony Shannon. 2011. *Generalized nets model of offspring reinsertion in genetic algorithms.* Annual of "Informatics" Section Union of Scientists in Bulgaria Volume 4, 2011, 29-35.

[69] PHMSA, Pipeline and Hazardous Materials Safety Administration. 2016. "Pipeline Safety", Research & Development. Accessed 25.03.2016 http://phmsa.dot.gov/pipeline/research-development

[70] Pitombeira-Neto, A. S. 2011. *"Modelo híbrido de otimização multiobjetivo para formação de células de manufatura (in portuguese)"*, PhD Thesis, USP-São Carlos, SP – Brazil.

[71] Purshouse, R.C. 2003. *On the evolutionary optimisation of many objectives.* PhD Thesis. The University of Sheffield. Sheffield, UK.

[72] Restrepo, Carlos E., Jeffrey S. Simonoff, and Rae Zimmerman. 2009. *"Causes, cost consequences, and risk implications of accidents in US hazardous liquid pipeline infrastructure."* International Journal of Critical Infrastructure Protection 2 (1):38-50. doi: 10.1016/j.ijcip.2008.09.001.

[73] Rouvroye, J. L. and A. C. Brombacher. 1999. *New quantitative safety standards: different techniques, different results.* Reliability Engineering and System Safety, 66:121–125.

[74] Ruan, Yingjun, Qingrong Liu, Weiguo Zhou, Bill Batty, Weijun Gao, Jianxin Ren, and Toshiyuki Watanabe. 2009. *"A procedure to design the mainline system in natural gas networks."* Applied Mathematical Modelling 33 (7):3040-3051.

[75] Schlumberger. 2016. *Oilfield Glossary.* Accessed 10.05.2016. http://www.glossary.oilfield.slb.com/Terms/u/upstream.aspx

[76] Schneeweiss W.G. 2001*. Tutorial: Petri nets as a graphical description mediumfor many reliability scenarios.* IEEE Transaction on reliability 2001;50(2):159-164.

[77] Shershukova, K. P. 2013a. *Definition of safety performance distributed control system as a layer of protection of technological facilities //* Problems of automation of technological processes of production, transportation and processing of oil and gas production: Materials of all-Russian scientific and practical Internet-conference - Ufa: Publisher UGNTU, p.62-66, (in Russian language).

[78] Shershukova, K.P. 2013b. *Risk reduction coefficient calculation of a distributed control system* // Scientific and technical journal "Automation, telemechanics and communication in the oil industry", №8: 33-38, (in Russian language).

[79] Shershukova, K.P. 2013c (dissertation). *Modelling Safety System Integrated into process control system of gas condensate processing.* Candidate of technical sciences dissertation, 2013. Federal State Budgetary Educational Institution of Higher Education. Thesis in The automation and control of technological processes and production, (industry) (technical Sciences). Moscow: Gubkin Russian State University of Oil and Gas (National Research University).

[80] Sullivan, J. 1982. *"A computer model for planning the development of an offshore gas field."* Journal of Petroleum Technology 34 (07):1,555-1,564.

[81] Teluk, A.S. and Shershukova, K.P. 2011. *The definition of an acceptable level of safety integrity and assurance of means of the instrument of security systems* // Mining information-analytical bulletin (Scientific and technical journal), №9: 54-59, (in Russian language).

[82] Teluk, A.S. and Shershukova, K.P. 2012a. *The model of distributed control system as a layer of protection technological facilities* // Scientific and technical journal "Automation, telemechanics and communication in the oil industry", №7: 21-25, (in Russian language).

[83] Teluk, A.S. and Shershukova, K.P. 2012b. *Risk assessment of hazardous production facilities for the design of automatic safety systems* // Mining information-analytical bulletin (Scientific and technical journal), №6: 82-89, (in Russian language).

[84] Teluk, A.S. and Shershukova, K.P. 2012c. *Evaluation of safety indicators of automated control systems as a layer of protection of technological processes in the gas industry* // Materials of the ninth all-Russian conference of young scientists, experts and students "New technologies in gas industry (gas, oil, energy), p.32-33, (in Russian language).

[85] Teluk, A.S. and Shershukova, K.P. 2012d. *The system of indicators to evaluate the functioning of the emergency protection* // Proceedings of the Russian state University of oil and gas named after I. M. Gubkin. Collection of scientific articles on problems of oil and gas issues, №3: 173-184, (in Russian language).

[86] Teluk, A.S. and Shershukova, K.P. 2012e. *The synthesis of emergency protection systems (in accordance with GOST R IEC 61508)* // Proceedings of the international youth conference in the framework of the Festival of Science. The Ministry of Education and Science of the Russian Federation, Voronezh Institute of High Technologies, Voronezh State Technical University. Voronezh: Publishing and printing center "Science Book", p. 118-121, (in Russian language).

[87] The Federal Law *"On Industrial Safety of Hazardous Production Facilities"* [M.: Closed Joint-Stock Company "Scientific technical center of industrial safety problems research", 2014. — p. 48.

[88] Torres-Echeverria, A. C. and H. A. Thompson. 2007. *Multi-objective genetic algorithm for optimization of system safety and reliability based on IEC 61508 requirements: a practical approach.* Article: Proceedings of the Institution of Mechanical Engineers, Part O, Journal of Risk and Reliability, 221(3):193-205, January 2007.

[89] Torres-Echeverria, Alejandro Carlos. 2009. "*Modelling and Optimization of Safety Instrumented Systems Based on Dependability and Cost Measures."* PhD thesis. The University of Sheffield. Department of Automatic Control and Systems Engineering.

[90] YOKOGAWA. 2016. *"Safety Instrumented System A Critical Barrier",* Research & Development. Presented by: Sujith Panikkar, CFSE. Accessed 11.04.2016. http://www.yokogawa.com/rd/?nid=megadlist

[91] Zhang, T., W. Long, and Y. Sato. 2003. *Availability of systems with self-diagnostic components applying Markov model to IEC 61508-6.* Reliability Engineering and System Safety, 80(2):133 – 141.

[92] Zhi, He. 1995. *"Risk management for overseas construction projects."* International Journal of Project Management (Elsevier Science Ltd), № 4 (1995): 231-237.

APPENDIX A. QUANTIFICATION OF RISKS. RISK CLASS ASCERTAINMENT WITH EVENT TREE METHOD

We will determine a class of risk of the technological process. It is required to carry out the following actions:

Step 1. Consider the technological units within the facility, for which we're conducting the analysis, separately. Generally, a technological process can have several technological units.

Step 2. Determine frequency F of i^{th} dangerous event in the case of a technological parameter of the unit, we're addressing, moves to the critical area. Frequency F can be found by various methods which are applied depending on the initial data which is available at a designer of safety systems. One of such methods is a quantitative method which is based on building a tree of events, see figure below.

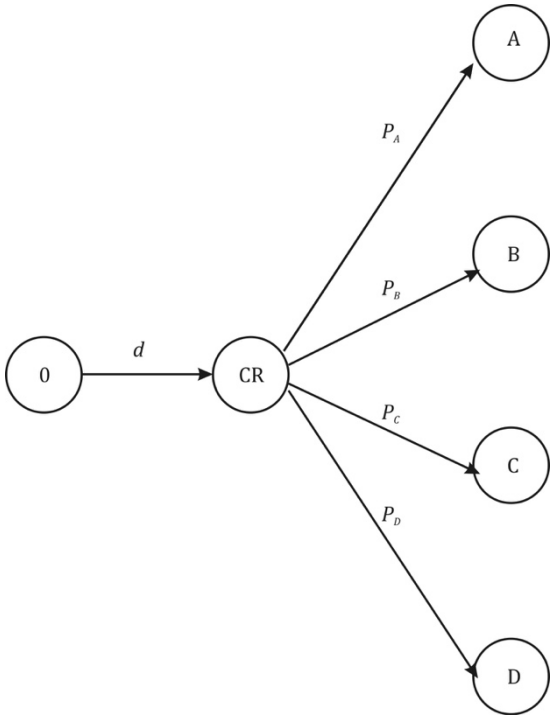

Figure 30. Event tree. Example adopted from Shershukova (2013c)

In the tree of events the following designations are used:

0 – state of the technology, when values of technological parameters are within their nominal range;

CR – state of the technology, when values of technological parameters have moved to their critical range;

A, B, C, D – state of the technology, when the corresponding groups of dangerous consequences take place;

d – incident rate, characterizing the transition from 0 into CR;

P_i - probability of i^{th} consequence.

From the analysis of the tree of events given on the figure above, it follows that required frequency is defined by a ratio:

$$F_i = d \cdot P_i, \quad i = A, B, C, D. \qquad (60)$$

If numeric values d and P_i aren't known, then for calculation of F_i one can be done with a combined method of an assessment.

Step 2.1 The frequency of moving to the critical range is given by its lower d_{LB} and upper bounds d_{UB}.

Table 25. Estimation of frequency of a parameter moving to its critical values range. Example adopted from Shershukova (2013c)

	Qualitative characteristic	Ranges of frequencies [1/hour]
1	Low	$10^{-6} < d < 10^{-5}$
2	Medium	$10^{-5} < d < 10^{-4}$
3	High	$10^{-4} < d < 10^{-3}$

Step 2.2 The probability of dangerous consequences are estimated with the following scale. The table is made for each group i of the consequences.

Table 26. Point assessment of dangerous consequence probability.

Example adopted from Shershukova (2013c)

	Qualitative characteristic	B_i (points)
1	Impossible	0
2	Low	3
3	Medium	6
4	High	9

Then the probability P_i of the i^{th} consequence is estimated as:

$$P_i = \frac{B_i}{\sum_i B_i}, \quad i = A, B, C, D. \tag{61}$$

And further the range to which F_i belongs is determined:

$$F_i \in [d_{LB} \cdot P_i \quad d_{UB} \cdot P_i], \quad i = A, B, C, D. \tag{62}$$

Step 3. Frequency of dangerous consequences from the each group A,B,C,D is defined for all critical parameters for all the units of the facility, and then the total frequency is obtained as a summation of frequencies for each parameter.

Step 4. The class of risk of a technological process is determined by a couple (i, F_i).

Table 27. Risk assessment. List of critical parameters. Example adopted from Shershukova (2013c)

N	Critical Parameter
1	Combustion exhaust gas temperature
2	No flame on the main burner.

For every critical parameter the combined method is applied

Table 28. Summary of risk assessment. Example adopted from Shershukova (2013c)

N	Group of consequences	Frequency of occurrence d	Probability of a consequence		Frequency F_i	
			B_i points	Probability P_i	F_{LBi}	F_{UBi}
1	Marginal	0,03	6	0,67	0,01	0,1
	Critical		3	0,33	0,001	0,01
2	Critical	0,08	9	1	0,01	0,1

The summation of the values of F_i for all the parameters, would result in a pair:

(i=C, F=0,11), i.e. dangerous events with critical consequences occur with the average frequency 0,11 [1/year]. This would give us the class *I* of risk.