sciendo

ISMSME International Society for Manufacturing, Service and Management Engineering

received: 10 September 2022
accepted: 10 December 2022

pages: 1-21

Employee scheduling and maintenance planning for safety systems at the remotely located oil and gas industrial facilities

Yury Redutskiy Marina Balycheva
Hendrik Dybdahl

ABSTRACT

The safety of operations is vital in any process in the oil and gas sector, especially given that increasingly more hydrocarbon reserves are discovered in non-conventional remote and Arctic locations. Safety systems are designed as a part of a complex IT system for process control. The design of these systems is conducted in the form of an engineering project. This research presents a decision-making framework to facilitate formulating clear and comprehensive recommendations for the requirements specification developed for the safety systems. The contribution of this research to the strategic planning area of IT solutions for hazardous industrial facilities is integrating the problems of designing a safety system, planning its maintenance, and scheduling the employees to conduct the required maintenance. With this joint decision-making, it is possible to explore trade-offs between investments into the systems' complexity and workforce-related expenditures throughout the solution's lifecycle. The reliability modelling is conducted with the help of Markov analysis. The multi-objective decision-making framework is employed to deduce straightforward requirements to the safety system design, maintenance strategy, and workforce organisation. This research is relevant to managing the petroleum sector engineering projects with regard to the design of technological solutions.

KEY WORDS

employee scheduling, engineering project management, maintenance planning in the oil and gas industry, remote and arctic location, requirements specification, safety systems

10.2478/emj-2022-0028

Yury Redutskiy

Molde University College, Norway
ORCID 0000-0002-3385-1712

Corresponding author:
e-mail: yury.redutskiy@himolde.no

Marina Balycheva

National University
of Oil and Gas
ORCID 0000-0003-4713-4295

Hendrik Dybdahl

Molde University College, Norway
ORCID 0000-0001-6391-7842

Introduction

The oil and gas production rates have increased over the past decades (BP, 2022). Increasingly more hydrocarbon reserves are being discovered in non-conventional environments, such as remote areas, deep-water offshore locations, and the Arctic region (Mellemvik et al., 2015). A study conducted by Bird et al. (2008) demonstrates that roughly 22 % of the remaining world's oil and gas reserves are located in the Arctic region, and 84 % are situated offshore.

Redutskiy, Y., Balycheva, M., & Dybdahl, H. (2022). Employee scheduling and maintenance planning for safety systems at the remotely located oil and gas industrial facilities. *Engineering Management in Production and Services, 14*(4), 1-21. doi: 10.2478/emj-2022-0028

These non-conventional environments pose considerable logistic challenges due to the climate in the north and the remoteness of the new production sites from the populated areas and large industrial centres.

Operations conducted on any oil and gas facility are associated with risks and possibilities of incidents. The consequences of an incident affect workers, assets/facilities, and the environment in terms of the ecosystem and the people in the nearby locations. The safety of operations is vital in any process along the oil and gas value chain: production, processing, transportation, refining, and distribution. Any oil and gas facility may be viewed as a hazardous industrial facility, and therefore, much attention has to be paid to its operational safety. To deal with this issue, automated control systems are put in place to monitor process parameters and, if necessary, shut down the operations. Such systems are called safety instrumented systems (SIS). There are usually several SISs deployed for any given technology to implement various safety functions. Some SISs are put in place to prevent hazardous situations, while others aim to mitigate the consequences if an incident happens (Boudreaux, 2010). In the process industry, among the various SISs deployed for a particular solution, emergency shutdown (ESD) systems are considered vital since they ensure the highest risk reduction among the preventive safety measures (Torres-Echeverria, 2009; CCPS, 2010). Therefore, this research focuses on ESD systems; however, the presented ideas and modelling approaches apply to any SIS.

Technological solutions and the necessary safety instrumentation are developed as an engineering project (Fig. 1). A new project is always launched by an exploration and production (E&P) operator. E&P operators are usually rather big companies with steady incoming cash flows, and therefore, they are not afraid to take some risks. Examples of such companies are Equinor, BP, Shell, Chevron, ExxonMobil, Petrobras, etc. The first step in initiating a new industrial facility is conceptual design. During this phase, various technical and technological possibilities are explored for the planned facilities. Further, an engineering contractor company's services are employed to develop and implement the actual engineering solution. At this stage, the requirements specification for the planned facility is developed, discussed, and revised. An important part of formulating the requirements specification is considering the safety regulations imposed by the national authorities. The next step is the detailed engineering design, followed by testing and commissioning. Afterwards, the longest-running phase of the project begins: it is the operations and maintenance phase when the developed solution is put to use for the E&P operator. To run operations and adequately maintain the developed solution in non-conventional remote locations, the E&P operator usually establishes a subsidiary somewhat close to the production site and hires the local workforce.

Three stakeholder categories may be identified as the project goes through the earlier described phases (Redutskiy, 2017). The first is national authorities in charge of the hydrocarbon reserves and performing regulatory functions when it comes to approving the establishment of hazardous facilities and providing general requirements for their safety. The second stakeholder is the E&P operator, investing in the development of the hydrocarbon deposits by building the processing, transportation, and distribution facilities. And finally, the engineering contractors are responsible for developing the technological facilities and IT solutions for process control. Each of these stakeholders has its priorities for the project. The national authorities aim to ensure the appropriate safety level for planned hazardous industrial facilities. Engineering companies strive to minimise lifecycle costs since they usually participate in competitive bidding to be hired for their service. The operating company's priorities include minimisation of lifecycle cost and facility downtime since they strive for uninterrupted operations to gain revenues.

Among the described project phases, special attention should be paid to the requirement specifications. The study (HSE, 2003) examined a sample of incidents in the petroleum sector with respect to the phases of the engineering project implementation in an attempt to determine where the primary causes of the incidents lie. This study concluded that almost half of the examined incidents were due to inadequacies in requirement specification for the safety systems. Too general, vague, or insufficient requirements result in the faulty design of the automated systems indented to ensure the safety of hazardous operations.

To make SIS requirements clear and sufficient, first and foremost, SIS-related safety measures must be examined. For this, one must refer to the international standards on industrial safety: IEC 61508 (1998) and IEC 61511 (2003). These standards demonstrate how specific equipment, architectures, and maintenance choices lead to achieving a specified safety level. The standards IEC 61508 and IEC 61511 are adopted worldwide, and they are the basis for national regulations, e.g., STC Industrial Safety

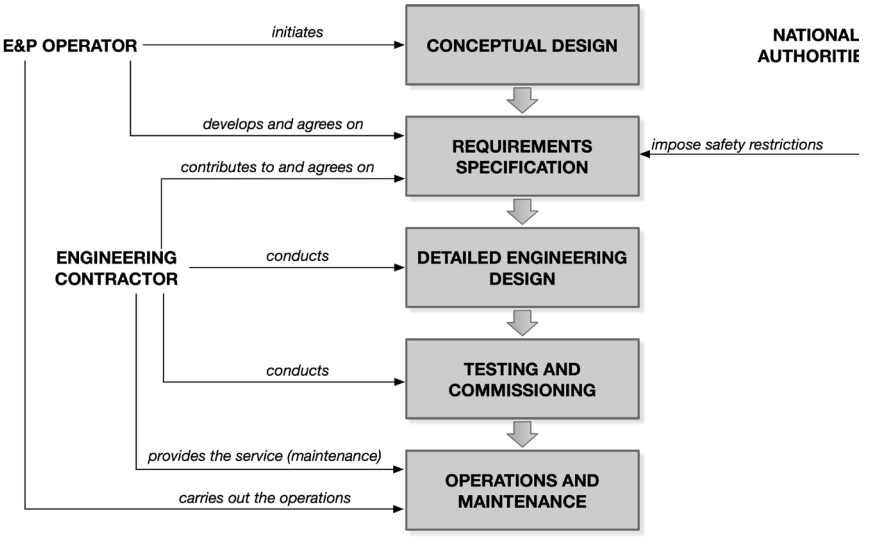

Fig. 1. Stakeholders and phases of the oil and gas engineering projects

Source: elaborated by the authors based on Redutskiy (2017).

(2014) in Russia and NOG-070 (2018) in Norway, which determine the safety level for various hazardous facilities and units to be achieved to operate properly. These requirements for the safety level are still relatively broad. Therefore, the issue of coming up with comprehensive yet straightforward requirement specifications should, perhaps, cover the safety measures inherent in SISs (i.e., instrumentation, architectures, and maintenance strategy) as clearly as possible. That way, these requirements may become a reasonably good starting point for the detailed design of a given SIS.

To ensure the proper function of the developed SIS, the aspect of maintaining the developed solution must be considered together with the issues of the SIS design. To perform adequate maintenance for the modern-day oil and gas industrial facilities faced with the challenges of non-conventional remote environments, it is essential to organise and train the workforce properly. Workforce management in remote areas is fairly costly, and so there is a need for appropriate decision-making when planning the maintenance and scheduling the repairpersons' transportation. The production and engineering companies strive to reduce their expenditures and, therefore, aim for cost-efficient maintenance. There is a need for a detailed plan of when the workers should arrive and how long they should work on each shift.

This research aims to develop a decision-making framework to facilitate the formulation of comprehensive requirement specifications for the safety instrumented systems. The decision-making should simultaneously cover the issues of the SIS design, maintenance, and workforce-related choices relevant to modern-day remotely located industrial facilities.

1. Overview of the research area

The research concerning industrial safety systems is mainly based on the reliability theory and the approaches to modelling the failures in an SIS. The international standards IEC 61508 (1998) and IEC 61511 (2003) present a comprehensive overview of the basic ideas and modelling approaches relevant to SIS design and maintenance. Among several widely used modelling techniques, the standards focus primarily on simplified equations (SE), reliability block diagrams (RBD), and fault tree analysis (FTA). Despite the wide application of the mentioned techniques, they primarily focus on various mechanisms of instrumentation failures and do not allow including such important aspects as device repairs and technological incidents. Due to these limitations of the SE, RBD, and FTA methods, some researchers choose to employ more complex and dynamic modelling approaches, such as Markov analysis (MA), which allows including device failures and repairs as well as technological incidents and restorations into one modelling framework. Examples of MA application may be found in the literature (Bukowski, 2006; Jin et al., 2011; Redutskiy, 2017; Srivastav et al., 2020). A reader interested in the details and comparison of

various modelling and design approaches relevant to safety instrumented systems is encouraged to refer to a review by Gabriel et al. (2018) or the book by Kuo and Zuo (2003).

In addition to the viewpoint of safety and reliability modelling of the SIS performance, this paper addresses choosing the appropriate maintenance strategy together with the workforce organisation to conduct the required maintenance. The problems related to workforce organisation and employee scheduling have been covered extensively over the past few decades for various applications, such as home nurse visitations, technician service scheduling, etc. However, strategic planning of the safety solution for remotely located industrial facilities and planning the employee shift work has not yet gained the proper attention in the literature. The research (Castillo-Salazar, 2016) provides an extensive overview of employee scheduling models and details relevant to real-life applications. Among these problem settings, the authors distinguish a class of problems named "workforce scheduling and routing problems". The problems in this category address the requirement for personnel to perform a given service at a given location. An important feature of this problem category is that the demand has to be satisfied precisely, unlike in many other real-life settings (e.g., tech-support call centres where the demand for personnel is considered stochastic). This particular approach to modelling the demand for servicepersons or service crews is relevant to the oil and gas industry since the maintenance requirements are usually provided in the form of a timeframe within which the maintenance must be completed so that the operations would proceed safely. The issues of hazards and industrial safety prompt the demand for the required maintenance to be met exactly. This approach to fulfilling the demand requirement is usually modelled based on the set-covering employee scheduling problem formulation proposed by (Dantzig, 1954). An overview of some issues pertaining to these problem contexts may be found in research (Soriano et al., 2020). Among the pool of research specific to the non-conventional and remote locations in the petroleum sector, several research papers may be noted (Hermeto, Ferreira, & Bahiense, 2014; Bastos, Fleck, & Martinelli, 2020; Vieira et al., 2021; De La Vega et al., 2022).

The overwhelming majority of the literature on workforce scheduling for maintenance and maintenance as a safety aspect is quite strongly divided into these two respective streams. The first (Hermeto, Ferreira, & Bahiense, 2014; Bastos, Fleck, & Martinelli, 2020; Vieira et al., 2021; De La Vega et al., 2022) focuses primarily on the tactical or operational details of employee scheduling and transport utilisation, primarily helicopters. The second focuses on the engineering details of safety, i.e., the safety system design (which corresponds to the strategic planning level). Thus, maintenance is considered merely a rather abstract concept or a very rough estimation of one operational-level detail. Notably, several research papers within this stream (Torres-Echeverria, 2009; Torres-Echeverria, Martorell & Thompson, 2012; Zhao, Si & Cai, 2019) employ multi-objective optimisation based on meta-heuristic algorithms. These papers engage in very detailed studying of the algorithm modalities and result in the produced Pareto optimal set with respect to the conflicting or non-conflicting relationship between various objectives. The results, however, could be used to draw certain real-life practical conclusions, which is one of the gaps this research aims to address.

The research (Helber & Henken, 2010) stresses the importance of addressing the issues that directly impact personnel requirements and workforce-related decisions. For the problem addressed in this research, the design and maintenance strategy choices for the planned SIS are the factors directly influencing the demand for the employees required to conduct the system maintenance. Given the specifics of maintaining a remotely located industrial facility, workforce-related costs play an especially significant role. Therefore, balancing these design and maintenance scheduling aspects should provide valuable insight into decision-making from the strategic planning viewpoint.

Upon conducting an extensive literature search, the authors of this paper have not found any academic articles that would address the two mentioned research gaps other than those produced by the research group (Redutskiy, 2018; Redutskiy et al., 2021) whose work is continued here.

This paper aims to develop a decision-making framework that would integrate the problems of designing the SIS, planning its maintenance, and scheduling the employees to conduct the required maintenance. With this joint decision-making, it is possible to explore the trade-offs between the investments into the complexity of the SIS (and thereby, its reliability) and the workforce-related expenditures, such as training costs, salaries, travel costs, bonuses for longer shifts and so on throughout the entire solution's lifecycle. The reliability modelling is conducted

with the help of Markov analysis. The integer programming model is developed to solve the employee scheduling problem. Finally, the lifecycle cost covering the mentioned aspects of the SIS is evaluated. To apply the model for deducing comprehensive requirements for the SIS design, maintenance strategy, and workforce organisation, a multi-objective optimisation is employed to produce several solutions, that is, a Pareto-front, to further examine their features and draw the appropriate conclusions.

2. Problem setting

The international standards IEC 61508 and IEC 61511 introduce the term safety instrumented system (SIS), defining them through their structure. An SIS consists of the same essential parts as any other automated system. The structure's (Fig. 2a) essential parts are explained further:

- process value transmitters, or sensors, are put in place to identify the state of the technology by measuring necessary process parameters;
- logic solvers, or programmable logic controllers (PLC), are industrial computers programmed to implement specific algorithms. The PLC's input modules gather the measurement information from the sensors, and the output modules deliver the control signal to the next subsystem;
- final control elements, or actuators, are put in place to affect the processes by, for example, making valves open or close, making pump drives work at a particular load or turning some electrical equipment on or off by the use of switches.

When designing any real-life SIS for a given technology, an important point is the choice of devices — sensors, controllers, and actuators — for the automated safety system. All device types are presented on the market by several analogous alternatives from various brands of automation instrumentation: Rockwell, Emerson, General Electric, Honeywell, Siemens, and others. Even though different brand devices may physically implement the same action, the reliability characteristics of these analogous alternatives from different instrumentation vendors vary considerably. Therefore, the choice of instrumentation, that is, particular device models for the subsystems of the developed safety solution, is an important issue of the SIS design.

Another important point with respect to SIS design is that in reality, each of the blocks in Fig. 2a — process value transmitters, logic solvers, and final control elements — may have more than one device implementing the same function at the same time, which is quite common for SISs. This design approach is called redundancy. The aim of using more than one component for the subsystems is to improve the subsystem's overall reliability: while some devices fail, others may continue performing their designated function. Redundancy of a subsystem is usually expressed through its M-out-of-N (MooN) architecture (Fig. 2b). In this notation, N stands for the total number of components in the architecture, and M represents the number of devices in the architecture that must operate, so that the whole architecture would perform properly.

A problem concerning redundancy is that, in some cases, multiple devices within a subsystem may fail because of the same cause or stress. It may be an accidental power cut to these identical devices or physical damage to a certain technological unit. This phenomenon is referred to as common-cause failure (CCF). To reduce the possible influence of CCF, additional device separation may be introduced within the MooN architecture. In Fig. 2b, it is marked by dashed lines between components.

The SIS structure depicted in Fig. 2a is a simplification aimed at reflecting the key blocks of an SIS. Real-life automated systems monitor many process parameters simultaneously and deliver their values to the PLC. Each of these sensor subsystems is responsible for identifying its potential incident. Therefore, instead of just one block of process value transmitters, in real-life solutions, there are several sensor subsystems, as demonstrated in Fig. 2c. There are also several actuators controlled by the PLC. It means that in case an incident is identified (and therefore, there is a demand for the safety systems to perform their function, e.g., technology shutdown), multiple actions are taken: some equipment must be turned off, pumps must be stopped, some valves must close, while others must open, and so on.

From the viewpoint of reliability modelling (reliability block diagrams), the structure in Fig. 2c implies a sequential connection of the blocks representing the SIS subsystems (Fig. 2d). The idea of the sequentially connected functional blocks is that all of the SIS subsystems have to be operating properly for the SIS to be able to perform its function.

To summarise, the issues of designing an SIS include the following:

- device model choice for the sensors, controllers, and actuators;

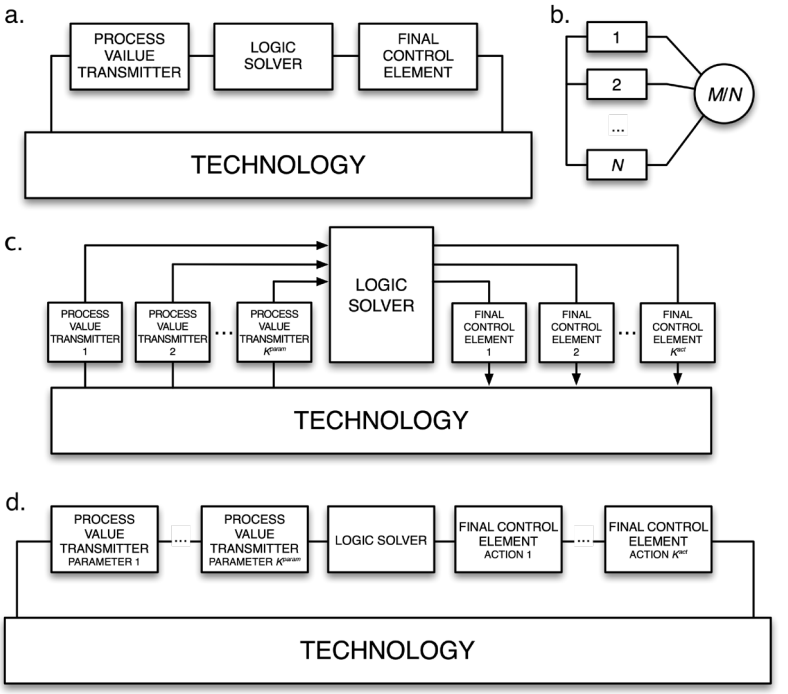

Fig. 2. SIS structure: a. Automated control loop. b. *MooN* redundancy architecture. c. Structure of a realistic SIS. d. Sequential structure of the SIS blocks is due to the reliability block-diagram principles

Source: elaborated by the authors based on IEC 61508 (1998) and IEC 61511 (2003).

- redundancy architecture choices, i.e., MooN architectures for each subsystem;
- the decision of whether to use additional device separation or not.

The problem of the SIS design should benefit from considering planning the maintenance of the SIS within the same decision-making framework. Both design and maintenance are associated with considerable expenditures and, at the same time, influence the reliability of the developed safety system. The maintenance of the safety systems is usually conducted in two forms. First, continuous maintenance is performed while the technology is running. The purpose of continuous maintenance is to address the identified failures. And second, there are also maintenance tests (or proof tests), which are conducted periodically. Such tests aim to address the failures that go undetected while the process runs.

Simultaneous consideration of the design and maintenance decisions helps explore the reliability and economic trade-offs between the decision alternatives. Highly reliable devices or architectures with significant redundancy will likely require rare maintenance. However, such solutions may turn out to be expensive. Simpler solutions with cheaper devices, on the other hand, are likely to require frequent maintenance. The more effort is associated with the instrumentation maintenance, the bigger some cost components are. For example, labour costs play a significant role in the solution's lifecycle if the operations in remote locations are considered, if only due to considerable travel costs associated with the maintenance personnel shift work. Also, such cost components as expenditures for spare parts and various maintenance tools can become quite high for a system with insufficient reliability. Yet another aspect of SIS performance evaluation is estimated losses due to the technology downtime associated with instrumentation overhauls.

So far, only the issue of maintenance frequency (which is usually expressed in the form of test interval TI) has been brought up. Besides TI, a part of planning the maintenance strategy is to organise testing in a certain manner. Fig. 3 shows three approaches to proof testing or maintenance policies. They are parallel, sequential, and staggered maintenance policies. Parallel testing implies that all the SIS instrumentation gets tested and repaired simultaneously. The sequential policy means that within each subsystem, the components get tested one after another. Of course, parallel testing requires considerably more staff to be present for the testing rather than sequential testing. On the other hand, the testing itself takes less time (hence, less facility downtime) if parallel

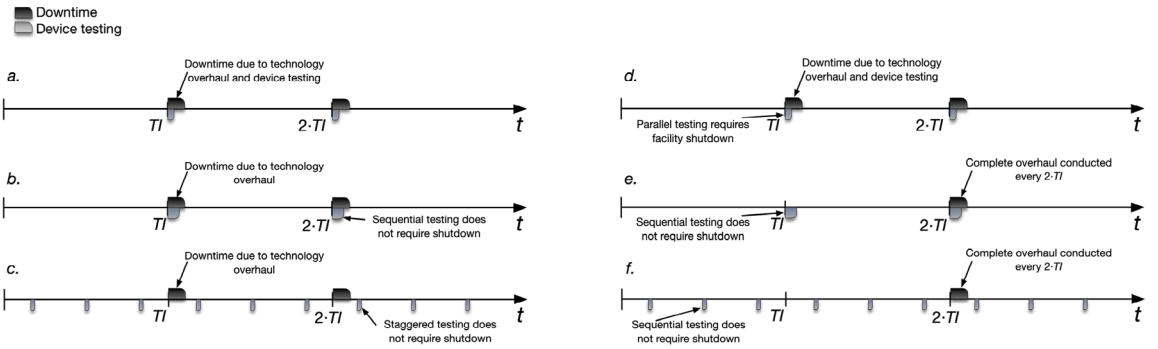

Fig. 3. Examples of proof testing policies. a, d: parallel proof testing policy; b, e: sequential proof testing policy; c, f: staggered proof testing policy for one subsystem with the tests uniformly distributed within *TI*. a, b, c: technology overhaul period equals *TI*; d, e, f: technology overhaul period equals 2·*TI*

Source: elaborated by the authors based on Torres-Echeverria (2009).

testing is chosen. Yet another approach to proof testing is the staggered policy when the subsystem's components are tested at separate points in time within the test interval. It should be mentioned that there are many more approaches to proof testing than the three described here. The international standards, however, usually recommend testing the entire SIS within the predefined timeframe. This is why, in this research, the decision-making is limited to the instrumentation testing approaches demonstrated in Fig. 3.

As Fig. 3 demonstrates, in addition to maintaining the SIS instrumentation, the technological facilities should also be maintained at certain points. The model presented further considers the period between two consecutive technological overhauls to be equal to the value of TI or a multiple of TI.

This paper continues previous research (Redutskiy, 2017; Redutskiy, 2018; Redutskiy et al., 2021). Here, Markov analysis is applied to evaluate the safety system's performance in terms of reliability. This particular type of reliability analysis is chosen due to its versatility, that is, the capability to incorporate the occurrence of events of various nature, such as device failures and repairs, as well as technological incidents and restorations. These stochastic events are assumed to be exponentially distributed, that is, they occur with a constant frequency or rate, as demonstrated in expression (1). The assumption of the exponential distribution of failures and incidents is proven valid for systems that include many electric and electronic devices (Goble, 2010). When it comes to the validity of the exponential distribution for repairs and restorations, Bukowski (2006) showed that such an assumption might turn out to be optimistic, which is hardly suitable for long-term SIS and maintenance planning. As mentioned, the research (Redutskiy, 2017) is continued here. That paper proposes a simple approach to the distribution of repairs and restorations into a pessimistic assumption by utilising the maximum limits set for the repair times instead of the average repair times.

$$P^{event}(t) = 1 - e^{-\lambda \cdot t}, t \geq 0 \qquad (1)$$

Fig. 4 shows the classification of failures assumed for this research. All safe failures are considered to be detected failures, which is a reasonable assumption for an SIS such as an emergency shutdown (ESD) system. If a safe failure occurs, the ESD must shut down the technology.

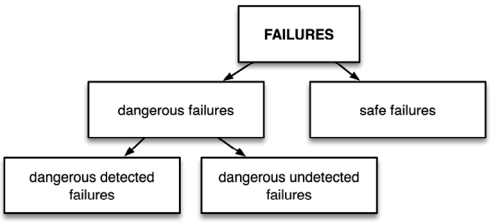

Fig. 4. Classification of the failure modes assumed for this research

Source: adapted from Redutskiy (2017).

To quantify the safety of a certain SIS solution, the most important reliability indicator is the average probability of failure on demand (PFDavg). The requirements for PFDavg in the regulations are normally set in the form of a safety integrity level (SIL). According to regulations set by national authorities (e.g., STC Industrial Safety, 2014; NOG-070, 2018), the SIL requirement SIL 3 is the main process within the oil and gas production, processing, transportation, and refining technology. Another safety indicator considered in this research is the expected facility downtime (DT). It reflects the operating company's

perspective since the operator's goal is profit in the long run; therefore, they strive for the smooth operation of their technology.

As stated earlier, the maintenance of the SIS solutions is crucial to their performance. The maintenance is performed by engineers specialising in automated systems; therefore, the problem of organising the workforce to implement the required maintenance strategies becomes relevant for the modern-day facilities located in remote, Arctic and offshore areas far from cities and large industrial centres. In many cases, a subsidiary is established by the operating company somewhat close to the production site, and the local engineers are trained at this facility on the SIS and facility maintenance.

Still, when the engineers have to be transported to the remotely located facility and back, it may involve several transportation modes and legs. To address the workforce organisation issues, this research applies a modification of the set-covering formulation of employee scheduling first proposed by Dantzig (1954). The model determines how many workers should take a trip of a particular duration starting at a particular time. Employee scheduling utilises the approach of "hard demand constraints", meaning that the demand must be met exactly. This is often the case for oil and gas industrial facilities since the maintenance must be completed within a predefined timeframe. These timeframe requirements are used in the model together with the SIS design to calculate the weekly demand of workers required to be present at the facility during each week of the planning horizon.

The employee scheduling model in this research accounts for certain shift work specifics relevant to the petroleum sector. The model addresses compensation to the workers if their shifts are longer than the "standard" shift. It has become customary in the industry for companies to award workers who spend more time on their shifts with larger yearly or quarterly bonuses. The model also accounts for the daily work schedule, which depends on the size of the maintenance crew. There are two different options for the daily work schedules; these are 8-hour and 12-hour schedules. In the first option, three workers in the maintenance crew are required to ensure con-

Tab. 1. SIL requirements

SIL	Risk reduction requirement		Fault tolerance requirement[B] for logic solvers			Fault tolerance requirement[B] for sensors and actuators
	PFD_{AVG}	RRF[A]	with SFF<60%	with 60% ≤ SFF < 90%	with SFF ≥ 90%	
1	$[10^{-2}, 10^{-1})$	$(10, 10^2]$	1	0	0	0
2	$[10^{-3}, 10^{-2})$	$(10^2, 10^3]$	2	1	0	1
3	$[10^{-4}, 10^{-3})$	$(10^3, 10^4]$	3	2	1	2
4	$[10^{-5}, 10^{-4})$	$(10^4, 10^5]$	special requirements			special requirements

a. Risk reduction factor. b. Refer to IEC 61508 (1998) for an explanation of fault tolerance requirement and safe failure fraction (SFF

Source: IEC 61508 (1998) and IEC 61511 (2003).

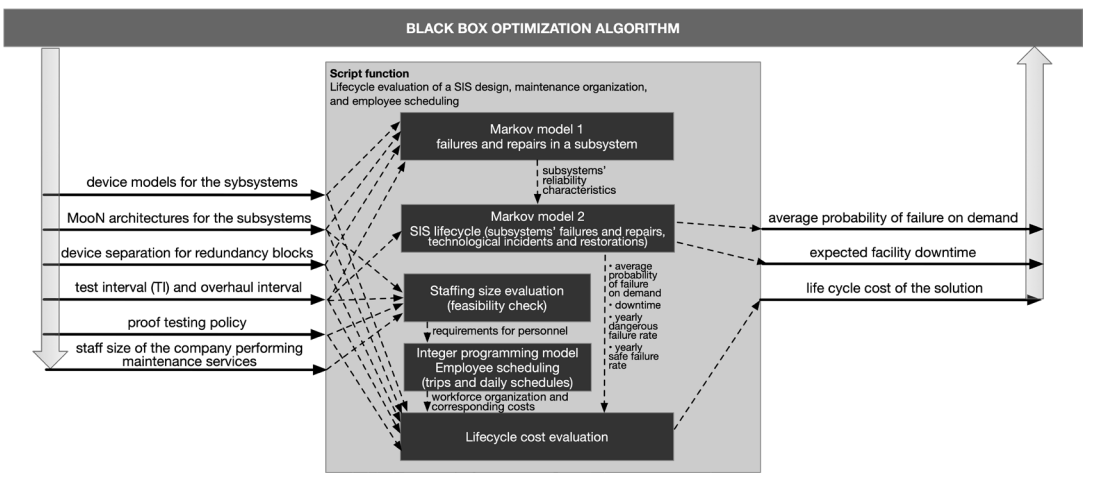

Fig. 5. Multi-objective decision-making framework

Source: based on Redutskiy (2018).

tinuous 24-hour service. In the latter option, only two workers are needed to ensure the service level. In addition, the model accounts for the establishment of a workforce of a given size, providing salaries and limiting the amount of time spent on trips to the remotely located facilities.

Another distinctive characteristic of the employee scheduling approach used in this research is that the developed model accounts for individual employees' yearly travel schedules instead of merely determining the collective number of crews required to take a certain trip. Accounting for each employee helps to determine the engineering staff size precisely to properly limit the time each worker spends at the remote facility and to ensure the availability of vacations for each employee.

The decision-making framework developed in this research consists of different blocks addressing various aspects of planning an SIS in the long-term perspective. The modelling blocks, the decision variables, and the objective functions for the optimisation problem are reflected in Fig. 5.

Decision variables:

- particular device models for each subsystem of the SIS;
- redundancy architecture (MooN) for each subsystem;
- the decision of whether to use additional electric separation for each subsystem or not;
- test interval (TI) for periodic proof testing and overhaul interval as a multiple of TI;
- proof testing policy (parallel, sequential, or staggered) for each subsystem;
- staff size of the engineering company performing the maintenance.
- Since there are different stakeholders with diverging viewpoints, which need to be considered when designing and planning SIS maintenance, the following objectives are used for decision-making:
- SIS's average probability of failure on demand;
- expected facility downtime;
- the lifecycle cost of an SIS operating for a particular hazardous technology.

2.1. Modelling assumptions

The lifecycle viewpoint suggested in the earlier research (Redutskiy, 2017; Redutskiy, 2018) is used for the strategic planning of the automated safety solutions employed for hazardous oil and gas industry technologies. This research, however, includes a more detailed view of the maintenance policies by incorporating the details of parallel, sequential, and staggered proof testing policies into the modelling and decision-making framework.

The assumptions made for further modelling are as follows:

- The instrumentation failures are assumed to be random, and the classification shown in Fig. 4 is assumed for these failures. Systematic failures are excluded from consideration as these failures must be resolved before the operations begin.
- The notations DD, DU, and ST are used in the models to distinguish dangerous detected, dangerous undetected failures, and spurious trips (or safe failures), according to the classification in Fig. 4.
- Instrumentation failures and repairs, as well as technological incidents and restorations, are considered to be exponentially distributed.
- Whenever a device failure is revealed during the course of operations, the failure is resolved within a predefined timeframe.
- All devices are tested within the period called test interval (TI). These proof tests are considered perfect, i.e., it is assumed that the undetected failures are resolved after a proof test.
- A major overhaul is conducted with a period which is a multiple of TI.
- The requirement for the number of servicepersons to be available at the facility at any time is computed with respect to the chosen architectures of the SIS subsystems and the chosen proof-testing policies.
- All possible trip starting times and the trip durations of one, two, four, and six weeks are considered along with their associated costs.
- A set-covering employee scheduling model is used to determine the number of maintenance crews required to go on particular trips and work following particular daily schedules. The model formulation is extended to include the consideration of the engineering staff size and the schedules of each employee to make sure that each employee does not spend more than six months every year away at the remote location and also that each employee is getting an uninterrupted 4-week vacation.
- A multi-objective decision-making framework is used. The three objective functions chosen for the optimisation aim to represent the viewpoints of the major stakeholders in the projects of SIS development and operation.

2.2. Modelling assumptions

The model presented in this subsection is largely based on the paper by Redutskiy (2017). However, considerable elaborations have been made to account for various complex proof-testing approaches.

The device failures and repairs within a MooN architecture are modelled over the period of TI. As Fig. 6 demonstrates, the Markov model for the failures and repairs includes (N – M + 2) states. State 1 stands for all N components operating properly. State 2 corresponds to one failure within the architecture. Each further state represents one more device failure. The failure of the entire redundancy architecture is represented by the last absorbing state, which corresponds to (N – M + 1) failures. Independent failures are depicted by sequential left-to-right transitions on the graph, while common cause failures are depicted by the direct transition to the absorbing state. Repairs relevant to DD and ST failures are depicted by right-to-left transitions.

Markov model equations are used for the three modelled failure types: equations (2) – (6) are expressed for DU failures in a redundancy architecture, and equations (7) for DD and ST failures.

For the DU failures, ordinary differential equations (ODE) (2) describe the probability of the subsystem being in a particular Markov model state. The non-zero transition rates are provided in (3). The stochastic process starts in state 1 when t = 0. Further course of the stochastic process is described by the switching Markov model with the time horizon

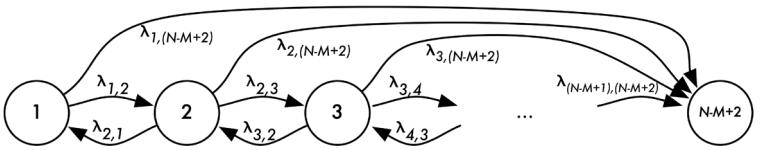

Fig. 6. Markov process of failures and repairs in a subsystem with a MooN architecture

Source: based on Redutskiy (2017).

Tab. 2. Notations used for the subsystem modelling

Notation	Description
Indices and Parameters	
i, j	indices of the Markov model states
k	index for the devices, $k \in \{1..N\}$
N	total number of components in a MooN redundancy architecture
M	necessary number of operating devices in a MooN architecture
TI	test interval, [h]
T^{test}	time required for testing and repairing one component in the architecture, [h]
λ	dangerous failure rate for one component, [h^{-1}]
λ^S	spurious trip rate for one component, [h^{-1}]
μ	repair rate, [h^{-1}]
ε	diagnostic coverage, fraction
β	common cause failure factor, fraction
$\lambda_{i,j}^{DU}$	transition rates for the model of dangerous undetected failures, [h^{-1}]
$\lambda_{i,j}^{DD}$	transition rates for the model of dangerous detected failures, [h^{-1}]
$\lambda_{i,j}^{ST}$	transition rates for the model of spurious trips, [h^{-1}]
Variables	
t	time, [h]
$p_j^{DU}(t)$	probability of (j – 1) dangerous undetected failures
$p_j^{DD}(t)$	probability of (j – 1) dangerous detected failures
$p_j^{ST}(t)$	probability of (j – 1) spurious trips in a subsystem
p_i^k	initial probability of the model's i^{th} state after testing k devices (for sequential or staggered policies)
Outputs of the Model	
λ^{DU}	dangerous undetected failure rate for a subsystem, [h^{-1}]
λ^{DD}	dangerous undetected failure rate for a subsystem, [h^{-1}]
λ^{ST}	spurious tripping rate for a subsystem, [h^{-1}]

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

$$\begin{gathered} \lambda_{i,i}^{DU} = -\lambda \cdot (1-\epsilon) \cdot [(N-i+1) \cdot (1-\beta) + \beta] \\ \lambda_{i,i+1}^{DU} = \lambda \cdot (1-\epsilon) \cdot (N-i+1) \cdot (1-\beta) \\ \lambda_{i,N-M+2}^{DU} = \lambda \cdot (1-\epsilon) \cdot \beta, \ i \in \{1, \dots, (N-M+2)\} \end{gathered} \tag{3}$$

$$p_1^{DU}(0) = 1, \ p_i^{DU}(0) = 0, i \in \{2, \dots, (N-M+2)\} \tag{4}$$

$$\begin{gathered} \pi_1^1 = 1, \ \pi_i^1 = 0, i \in \{2, \dots, (N-M+2)\}. \\ \pi_1^k = p_1^{DU}\big((k-1) \cdot T^{test}\big) + \frac{1}{N} \cdot p_2^{DU}\big((k-1) \cdot T^{test}\big), \dots, \\ \pi_{N-M+1}^k = \frac{1}{N} \cdot p_{N-M+1}^{DU}\big((k-1) \cdot T^{test}\big) + \frac{N-M+1}{N} \cdot p_{N-M+2}^{DU}\big((k-1) \cdot T^{test}\big), \\ \pi_{N-M+2}^k = 0, \ k \in \{2, \dots, N\}. \end{gathered} \tag{5}$$

$$\begin{gathered} \pi_1^1 = 1, \ \pi_i^1 = 0, i \in \{2, \dots, (N-M+2)\}. \\ \pi_1^k = p_1^{DU}\left(\frac{(k-1) \cdot TI}{2 \cdot N}\right) + \frac{1}{N} \cdot p_2^{DU}\left(\frac{(k-1) \cdot TI}{2 \cdot N}\right), \dots, \\ \pi_{N-M+1}^k = \frac{1}{N} \cdot p_{N-M+1}^{DU}\left(\frac{(k-1) \cdot TI}{2 \cdot N}\right) + \frac{N-M+1}{N} \cdot p_{N-M+2}^{DU}\left(\frac{(k-1) \cdot TI}{2 \cdot N}\right), \\ \pi_{N-M+2}^k = 0, \ k \in \{2, \dots, N\} \end{gathered} \tag{6}$$

$$\begin{gathered} \frac{dp_j^{DD}(t)}{dt} = \sum_{i=1}^{N-M+2} p_i^{DD}(t) \cdot \lambda_{i,j}^{DD} \quad j \in \{1, \dots, (N-M+2)\} \\ \frac{dp_j^{ST}(t)}{dt} = \sum_{i=1}^{N-M+2} p_i^{ST}(t) \cdot \lambda_{i,j}^{ST} \quad j \in \{1, \dots, (N-M+2)\} \end{gathered} \tag{7}$$

$$\begin{gathered} \lambda^{DU} = -\frac{\log\left(1-p_{N-M+2}^{DU}(TI)\right)}{TI}, \ \lambda^{DD} = -\frac{\log\left(1-p_{N-M+2}^{DD}(TI)\right)}{TI}, \\ \lambda^{ST} = -\frac{\log\left(1-p_{N-M+2}^{ST}(TI)\right)}{TI} \end{gathered} \tag{8}$$

depicted in Fig. 3. The initial probabilities for the intervals of this time horizon are defined in (4), (5), and (6) for the parallel, sequential, and staggered tests respectively.

The choice of the proof testing policy has an impact on how the Markov model for the DU failures is run, as shown in equations (2) – (6). This is due to the fact that the point of proof testing is to deal specifically with the DU failures in a system. The Markov model for the DD and ST failure modes is virtually unaffected by the proof testing policy choice. Refer to the paper by Redutskiy (2017) for the full mathematical formulation of the DD and ST failures in a MooN architecture.

By producing the solutions to the ODEs (2) and (7), the failure rate values for the entire MooN architecture are obtained in (8). These values are further used in the lifecycle model of the SIS as the aggregated reliability characteristics of the subsystems.

2.3. Lifecycle modelling from the safety perspective

The lifecycle model presented next is mostly adopted from the paper by Redutskiy (2017). For the SIS subsystem, the following possible states are considered:

- performing properly,
- under the overhaul after the dangerous detected failure of the entire subsystem,
- under overhaul after a spurious trip,
- in the dangerous undetected failure mode.

For the technology, the following states are considered:

- up and running, and no incidents have occurred,
- shutdown due to a detected incident,
- shutdown due to repairs in the SIS,
- running while an incident has occurred without a proper response from the SIS (failure-on-demand state).

Given these possibilities for the SIS states and the technological unit, the entire process may be described by the states listed in Table 3 and the transitions depicted in Fig. 7. This description is, however, relevant only to safety systems that comprise exactly one sensor subsystem, one controller subsystem, and exactly one actuator subsystem. To account for realistic SIS structures (as depicted in Fig. 2d), this general model has to be adjusted.

States 1 and 2 and the last absorbing state will always be present in the model of the stochastic process. The groups of states 3–5, 6–8, and 9–11, which currently comprise three states each (corresponding to the three subsystems), will have to be expanded to the necessary number of subsystems in a real-life SIS.

The lifecycle is split into K periods, which correspond to the defined test interval and the frequency of technological overhauls. It is reflected in expression (9). Fig. 8 demonstrates an example of the time horizon. The choice of the overhaul period (OP) is related to the choice of the testing policy. If a parallel testing policy is chosen for any subsystem, then the technology has to be shut down every TI. For the case of sequential and staggered testing policies chosen for the entire SIS, the choice of OP is independent of TI. After the proof testing is finished, there is a predefined start-up time which is required to get the technology running again. It is reflected in (9).

The ODEs for the lifecycle model are provided in (10). The solution of these ODEs is used to evaluate the two safety indicators: the average probability of

Tab. 3. Markov model for the lifecycle

State	Sensors	PLCs	Actuators	Technology	Comment
1	up	up	up	running	normal course of the process
2	up	up	up	shutdown	safety function performed
3	O/S	up	up	shutdown	overhaul after a spurious trip
4	up	O/S	up	shutdown	
5	up	up	O/S	shutdown	
6	O/D	up	up	shutdown	overhaul after a dangerous detected failure
7	up	O/D	up	shutdown	
8	up	up	O/D	shutdown	
9	failure	up	up	running	undetected failure has occurred
10	up	failure	up	running	
11	up	up	failure	running	
12	SIS is down, incident has occurred				failure on demand state

Source: Redutskiy (2017).

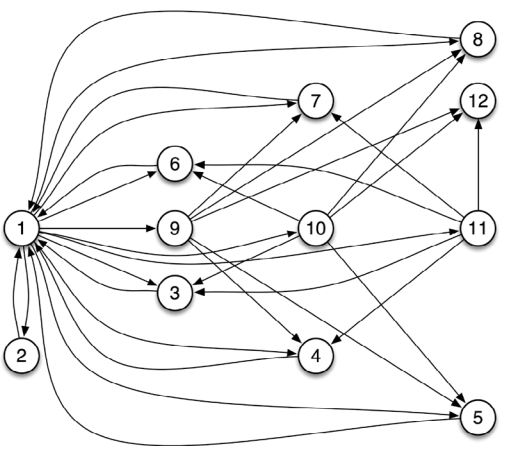

Fig. 7. Markov model of the lifecycle

Source: based on Redutskiy (2017).

Tab. 4. Notations used for the subsystem modelling

Notation	Description
Indices and Parameters	
i, j	indices of the Markov model states
q	index of the subsystems
K	total number of periods the lifecycle is split into
TI	test interval, [h]
OP	overhaul period, which has to be a multiple of *TI*, [h]
LC_h	duration of the lifecycle, [h]
T^{SU}	start-up time for the technology after the shutdown, [h]
$\lambda_{i,j}$	transition rate from state *i* to state *j*, [h^{-1}]
Variables	
$p_j(t)$	probability of the process being in the j^{th} state
Outputs of the Model	
PFD_{avg}	average probability of failure on demand
DT	expected downtime of the process, [h]

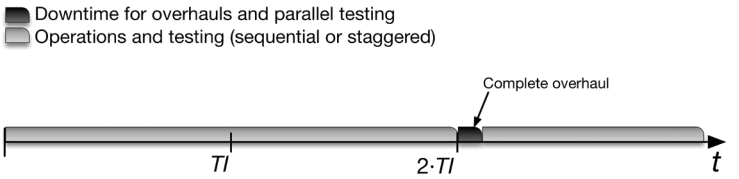

Fig. 8. An example of the time horizon for the lifecycle model where the overhaul period equals 2·*TI*

$$K = \left\lceil \frac{LC_h}{TI} \right\rceil.$$
$$t \in [0, OP] \cup [OP + T^{SU}; 2 \cdot OP] \cup \ldots \cup [(K-1) \cdot OP + T^{SU}; K \cdot OP] \tag{9}$$

$$\frac{dp_j(t)}{dt} = \sum_{i=1}^{12} p_i(t) \cdot \lambda_{i,j} \quad j \in \{1, \ldots, 12\},$$
$$p_1(0) = 1, p_2(0) = 0, \ldots p_{12}(0) = 0. \tag{10}$$

$$PFD_{avg} = \frac{1}{LC_h} \cdot \int_0^{LC_h} PFD(t)dt = \frac{1}{TI} \cdot \int_0^{OP} p_{12}(t)dt + \sum_{k=2}^{K} \frac{1}{OP - T^{SU}} \cdot \int_{(k-1)\cdot OP + T^{SU}}^{k \cdot OP} p_{12}(t)dt,$$
$$DT = \sum_{j=2}^{2} \left[\int_0^{TI} p_j(t)dt + \sum_{k=2}^{K} \int_{(k-1)\cdot TI + T^{OD}}^{k \cdot TI} p_{12}(t)dt \right] \tag{11}$$

failure on demand and the expected facility downtime are expressed in (11).

2.4. Employee scheduling model

The blocks of the decision-making framework (Fig. 5) that are relevant to workforce organisation are, first of all, the computation of the weekly demand for the employees during a period of one year, and second, the employee scheduling problem. The latter is based on the set-covering model proposed by Dantzig (1954). As already mentioned, the requirements for facility maintenance are strict in the oil and gas industry; therefore, the demand for maintenance personnel must be met precisely. Table 5 contains the notations necessary to describe this modelling block.

The maintenance personnel requirements are determined for the two kinds of maintenance considered in this research: continuous and periodic. The number of workers required at the facility for conducting continuous maintenance is calculated based on the maximum allowable amount of time for resolving the detected device failures, which are demonstrated in (12). Personnel requirements for the

Tab. 5. Notations for the employee scheduling model

Notation	Description
Indices and Sets	
w	index of weeks in a one-year period: w ∈ {1..52}
q	index for subsystems of the SIS: transmitters, controllers, and final elements
r	index for redundancy alternatives
l	index for trips
s	index for daily schedule alternatives: 8-hour daily work or 12-hour daily schedule
f	index for maintenance workers w ∈ {1..N^{staff}}
p	index for proof testing policies: p={1,2,3} corresponding to parallel, sequential, and staggered policies
S_q^{red}	set of redundancy architecture alternatives for subsystem q
S^{trip}	set of trips (all possible trips' start times and durations of one, two, four, or six weeks)
$S^{4w.trip}$	set of all possible 4-week trips
S^{sched}	set of alternative daily work schedules (work-rest schedule during each day)
Parameters	
$N_{r,q}$	the total number of devices in subsystem q given the redundancy option r
T_q^{repair}	repair time of the devices in subsystem q
$T^{repair.max}$	the upper bound on the repair time for the entire SIS for continuous maintenance (8 hours)
$\sigma_{l,w}$	a binary parameter indicating whether week w is covered by the trip option l or not
S_s^{crew}	crew size associated with any particular daily work schedule alternative s
β_s^{sched}	employees pay rate cost modifier given the chosen daily schedule alternative s
$x_{q,p}^{TP}$	binary indicator: equals 1 if testing policy p is chosen for subsystem q
$d_w^{continuous}$	weekly demand for the employees for continuous maintenance
$d_w^{periodic}$	weekly demand for the employees for periodic parallel or sequential proof tests
$d_w^{staggered}$	weekly demand for the employees for periodic staggered proof tests for subsystem q
d_w^{emp}	total demand for the workers whose presence is required at the facility during week w
$C^{WF.est}$	initial investments associated with establishing a local workforce
$C^{WF.oper}$	yearly operational expenditures associated with the local workforce
C^{start}	subsidiary start-up cost
C^{train}	cost of training one maintenance engineer
C^{comp}	yearly expenditures associated with running the local subsidiary
C^{wage}	average salary of one maintenance engineer
d_l^{trip}	cost of one worker's trip to the remote location and back, depending on the trip duration
N^{staff}	total number of employees on the maintenance staff
Decision Variables	
$x_{f,l,s}^{emp}$	binary variable: equals 1, if employee f is taking trip l to travel to the facility and work according to daily schedule s
$y_{l,s}^{travel}$	integer variable: number of service crews taking trip l to travel to the facility and work according to daily schedule s

parallel or sequential proof tests are determined given each subsystem's architecture and the maintenance policy choice (13).

When it comes to determining the number of people required for the staggered tests, it has to be determined separately for each subsystem because of the different subsystems' architectures and, therefore, different planning periods for the staggered proof-testing approach (14). Finally, expression (15) sums up all the demand for the required number of employees. This array is further used in the employee scheduling model.

The employee scheduling block of the modelling framework proposed in this research considers the lifecycle cost as one of the objectives for decision-making. As a part of the lifecycle cost, expression (16) demonstrates the initial investments into the workforce organisation, i.e., starting up a local subsidiary and training the locally hired workforce. Further, expression (17) describes the yearly costs associated with running the company, paying salaries to the employees, and organising the schedules of employees travelling to the remotely-located industrial facilities.

$$d_w^{continuous} = \left\lceil \sum_q \left(\sum_{r \epsilon S_q^{red}} N_{r,q} \cdot x_{r,q}^{red} - \sum_{r \epsilon S_q^{red}} M_{r,q} \cdot x_{r,q}^{red} \right) \cdot \frac{T_q^{repair}}{T^{repair.max}} \right\rceil, \quad w = \{1, \dots, 52\} \setminus \left\{ \frac{TI}{7 \cdot 24}; \frac{2 \cdot TI}{7 \cdot 24}; \frac{3 \cdot TI}{7 \cdot 24}; \dots; 52 \right\} \tag{12}$$

$$d_w^{periodic} = \sum_q \left(x_{q,1}^{TP} \cdot \sum_{r \epsilon S_q^{red}} N_{r,q} \cdot x_{r,q}^{red} + x_{q,2}^{TP} \cdot 1 \right), \quad w = \left\{ \frac{TI}{7 \cdot 24}; \frac{2 \cdot TI}{7 \cdot 24}; \frac{3 \cdot TI}{7 \cdot 24}; \dots; 52 \right\}. \tag{13}$$

$$d_{w,q}^{staggeredTP} = x_{q,3}^{TP} \cdot 1, \quad w = \left\{ \frac{TI}{7 \cdot 24 \cdot \sum_{r \epsilon S_q^{red}} N_{r,q} \cdot x_{r,q}^{red}} \cdot \frac{1}{2}; \frac{TI}{7 \cdot 24 \cdot \sum_{r \epsilon S_q^{red}} N_{r,q} \cdot x_{r,q}^{red}} \cdot \frac{3}{2}; \dots; 52 \right\}, \forall q. \tag{14}$$

$$d_w^{emp} = d_w^{continuous} + d_w^{periodic} + \sum_q d_{w,q}^{staggeredTP}, \ \forall w \tag{15}$$

$$C^{WF.est} = C^{start} + C^{train} \cdot N^{staff} \tag{16}$$

$$C^{WF.oper} = C^{comp} + 12 \cdot C^{wage} \cdot N^{staff} + \sum_{l \in S^{trips}} \sum_{s \in S^{sched}} C_l^{trip} \cdot \beta_s^{sched} \cdot S_s^{crew} \cdot y_{l,s}^{travel} \tag{17}$$

$$\sum_{l \in S^{trips}} \sum_{s \in S^{sched}} \sigma_{l,w} \cdot y_{l,s}^{travel} \geq d_w^{emp}, \ \forall w \in \{1, \dots, 52\} \tag{18}$$

$$\sum_{f=1}^{N^{staff}} x_{f,l,s}^{emp} = S_s^{crew} \cdot y_{l,s}^{travel}, \ \forall l \in S^{trips}, \forall s \in S^{sched} \tag{19}$$

$$\sum_{s \in S^{sched}} \sigma_{l,w} \cdot x_{f,l,s}^{emp} \leq 1, \ \forall l \in S^{trips}, \forall f \in \{1, \dots, N^{staff}\}, \forall w \in \{1, \dots, 52\} \tag{20}$$

$$\sum_{l \in S^{trips}} \sigma_{l,w} \cdot x_{f,l,s}^{emp} \leq 1, \ \forall s \in S^{sched}, \forall f \in \{1, \dots, N^{staff}\}, \forall w \in \{1, \dots, 52\} \tag{21}$$

$$\sum_{l \in S^{trips}} \sum_{s \in S^{sched}} \sum_{w=1}^{52} \sigma_{l,w} \cdot x_{f,l,s}^{emp} \leq \frac{52}{2}, \ \forall f \in \{1, \dots, N^{staff}\} \tag{22}$$

$$\sum_{l \in S^{4w.trips}} \left(1 - x_{f,l,s}^{emp}\right) \geq 1, \ \forall s \in S^{sched}, \forall f \in \{1, \dots, N^{staff}\} \tag{23}$$

Further, the constraints for the employee scheduling model are defined. First of all, constraint (18) based on Dantzig's problem formulation ensures that the demand for the employees is covered throughout the entire planning horizon, which in our case is every week of any given year. Constraint (19) connects the integer variable from the set-covering constraint (18) with the binary variable of each employee's personal schedule. Constraints (20) and (21) ensure that each employee is assigned to no more than one trip and one daily schedule. Constraint (22) declares that each employee should not spend more than six months out of a year on trips to remote locations. And finally, constraint (23) declares that each employee has to have a four-week uninterrupted vacation.

2.5. Lifecycle modelling from the economic perspective

As suggested in IEC 61508, the economic perspective on risk reduction needs to be addressed. At the same time, lifecycle cost minimisation is one of the three priorities of the decision-making framework (Fig. 5). The present value of the total cost is evaluated for the designed solution in (24).

This evaluation includes three main components: procurement, operation and risk costs. The reader can address (Torres-Echeverria, 2009; Goble, 2010; Redutskiy, 2017) for the details of this model.

To integrate the employee scheduling model into this decision-making framework, the expenditures

$$C^{lifecycle} = C^{procurement} + \sum_{\tau=1}^{LC}\left(C_{\tau}^{operations} + C_{\tau}^{risk}\right) \cdot \frac{1}{(1+\delta)^{\tau-1}} \quad (24)$$

calculated in (16) and (17) become the components of the procurement and operating costs, respectively.

3. Computational experiment

3.1. Experiment setting and the optimisation algorithm

The suggested framework is applied to a case provided by a petroleum company operating a remotely-located facility: an oil terminal with a storage tank. The storage facility is used as temporary storage for crude and substandard oil and for several days in case the throughput at the oil processing facility is exceeded or if there is an emergency at the facility. Table 6 shows possible critical situations and the required shutdown measures.

Following the logic in Fig. 2c–d, the ESD system for this project has to comprise six subsystems to function as described in Table 6. Therefore, the developed Markov model for this solution's lifecycle comprises 21 states.

Table 6 also shows the instrumentation alternatives considered by the engineering contractor for this project. The table provides relevant characteristics of the devices, their costs, reasonable redundancy options, as well as some additional parameters for this engineering solution.

Given this study's focus on maintenance organisation, the data regarding typical trips, schedules, and compensations have been collected. Table 6 shows the

Tab. 6. Modelling parameters and equipment database

Critical process parameters				Shutdown actions		
#	Parameter	Event	Frequency, [y^{-1}]	#	Final control element	Action
1	Liquid level in the tank	Level ≥ HH	0.075	1	Safety Valve 1 on the fill line	close
2	Fire in the storage tank	Fire detected	0.03	2	Safety Valve 2 on the output line	close
				3	Pump delivering crude hydrocarbons to the tank	shutdown

Instrumentation alternatives																
	Level transmitter					Fire detector			PLC			Safety valve			Pump drive	
Alternative	LT1	LT2	LT3	LT4	LT5	FD1	FD2	FD3	PLC1	PLC2	PLC3	SV1	SV2	SV3	PD1	PD2
Vendor	V1	V1	V2	V3	V3	V4	V4	V5	V6	V1	V3	V7	V1	V8	V3	V1
Failure rate, ×10^{-6} [h^{-1}]																
Dangerous failures	2	0.58	20	3	7.1	20	6	1.2	0.9	1.3	5.9	67	40	90	27	17
Spurious trips	1	4	15	1.2	3	10	4	2.28	0.8	1.1	5.5	33	33	30	13	9
Diagnostic coverage [%]	67	40	67	70	50	0	35	40	90	98	97	20	30	10	20	30
Costs																
Purchase [CU[a]]	1400	1750	850	1100	1250	40	57.5	85	22500	12500	7500	1300	1750	1400	750	1250
Design [CU]	5	5	6	5	8.5	5	5	5	2000	1000	600	650	900	900	100	100
Consumption [CU/y]	1.5	0.5	1	0.5	3	0.5	0.5	0.5	500	500	400	250	200	100	50	75
Repair [CU/event]	5	2.5	2	2.5	6	2	2	2	5	5	5	45	40	25	50	40
Test [CU/event]	5	4	5	6	8	3	3	3	1000	1000	750	500	500	500	75	100
Redundancy alternatives	1oo1, 1oo2, 1oo3, 1oo4, 2oo2, 2oo3					2oo2, 2oo3, 2oo4, 2oo5, 2oo6, 2oo7, 2oo8			1oo1, 1oo2, 1oo3, 1oo4, 2oo3			1oo1, 1oo2, 1oo3, 1oo4			1oo1, 1oo2, 1oo3	

Other parameters	Trips and daily schedules with associated costs			
CCF factor for standard circuits: β=0.035. CCF factor for electrical separation: β=0.02. Repair rate for the subsystems: μ=0.125 h^{-1}. Facility restoration rate: μ^t=0.0625 h^{-1}. Cost of hazard: 5 000 000 CU Lifecycle: 15 y. TI is chosen from a set of values from 12 to 52 weeks. [a] Here, fictional currency units (CU) are used to mask the real purchase costs for the devices so that particular instrumentation vendors would not be identifiable.	#	Work/rest	# of workers for continuous service	Pay rate, CU/day
	1	8h/16h	3	125
	2	12h/12h	2	250
	Daily work schedule alternatives			
	#	Duration	Pay rate cost modifier	
	1	1-week trip	1	
	2	2-week trip	1.25	
	3	4-week trip	1.5	
	4	6-week trip	2	

trip alternatives with the corresponding costs, given how the case company rewards the workers for longer trips and working hours.

A script function has been developed in MATLAB to realise the decision-making framework (Fig. 5), and MATLAB's multi-objective genetic algorithm (a variant of NSGA-II, solver gamultiobj) has been used to run the black-box optimisation. For the details of this meta-heuristic algorithm, Mathworks refers the users to Deb (2001). The example at hand includes 142 decision variables, of which 140 are binaries, and the remaining two are integers. The following settings for the solver are applied: population size: 300; initial population created with the uniform distribution applying a customised function suggested by Mathworks; selection function: tournament; generational gap: 0.8 (or 80 %); crossover and mutation functions: customised functions suggested by Mathworks.

3.2. Results and discussion

Among the solutions produced as the result of the solver run, those fulfilling the SIL3 requirement are demonstrated in Table 7 and further analysed.

- The decision-making framework chooses field devices (sensors and actuators) with better reliability characteristics despite their higher costs. It is observed by comparing the chosen instrumentation to the database of the available alternatives.
- Electric separation is preferred over the baseline solution. For most subsystems in most solutions, the additional electric separation is chosen to mitigate the CCF effect despite the associated additional costs. This shows that the expected long-term production losses due to the downtime caused by CCFs are considered more costly by the decision-making framework than the investments into this safety measure.
- Electric separation is always chosen for the subsystems of PLCs and fire detectors. For the PLCs, preventing common-cause failures is critical. For the fire detector, the additional cost related to electrical separation is quite small.
- For the level sensors, device models LT4 and LT5 are chosen. Both device models are produced by the same manufacturer (V3). Based on this result, it may be suggested that when level sensors are selected, one requirement may be that they are produced by this manufacturer (V3). From the solutions, one may observe that higher redundancy architecture 1oo4 is most often chosen for LT5, while architecture 1oo3 is preferred for LT4.
- The highest redundancy among the alternatives (2oo8) is chosen for the subsystem of fire detectors. These high redundancies may be attributed to the cheap cost of fire detectors in comparison to the other devices in the SIS.
- For the subsystem of PLCs, device model PLC2 (manufacturer V1) is always chosen with the architecture 1oo3. From the instrumentation database, this controller model appears to be a trade-off between reliability and cost: reliability characteristics for PLC2 are almost as good as the best among all the alternatives, while its price is reasonable.
- For the actuator subsystems, the valve SV2 and pump drive PD2 are chosen, both produced by the same manufacturer, V1. Architecture 1oo3 is chosen most often. However, some actuator subsystems are assigned 1oo2 redundancy. Choosing the appropriate architecture for actuators should perhaps be considered in greater detail during the detailed design phase.
- For three solutions, a test interval of 12 weeks is chosen, while the overhaul period is 24 weeks (almost six months). For the remaining four solutions, a TI of 16 weeks is chosen, while the OP is 48 weeks (almost a year). For the former three solutions, one may observe that the expected downtime is no less than 142 hours, while for the remaining four solutions, the value of downtime is estimated as no more than 100 hours. When the overhaul is conducted, the system needs to shut down, which is the reason why the downtime is significantly higher for the three solutions with an OP of 24 weeks. For the company strongly focusing on reducing facility downtime, such solutions may appear suboptimal.
- Given the values of PFDavg presented in Table 7, one may observe that all the solutions achieved the required SIL3. The table also reflects the cost associated with these solutions. The lifecycle cost of the solutions is estimated at around 32 million currency units (CU). However, there is still a difference between the solution costs within the range of approximately 30-34 million units. Such a difference in costs is a matter for the stakeholders to consider while the requirements are formulated and the stakeholder's concerns are addressed.
- From the cost structure presented in Table 7, one may observe that workforce-related costs constitute at least 40 % of the overall lifecycle cost. This

fact, again, shows the importance of proper workforce planning.

- As it is possible to observe from Table 7, the costs associated with the risk is small compared to the other cost. This is achieved by the considerably strict requirements applied to the safety systems design in this research. The relatively small risk costs show that considerable risk reduction has been successfully achieved for the planned solution.
- Besides the workforce costs, another considerable component of the operational expenditures is the production losses due to the facility downtime. This cost component accounts for 25–30 % of the cost of operations.
- For the majority of solutions and for most subsystems, the sequential testing policy has been chosen, as displayed in Table 7. This result may be attributed, first of all, to the fact that sequential proof testing does not require an operational shutdown. Parallel testing requires the process shutdown, so the parallel testing policy is never chosen to avoid more downtime. Another reason why the sequential testing policy is generally preferred (even over the staggered policy, which also does not require operations shutdown) is that this decision-making problem combines maintenance planning with its implementation through employee scheduling. Because of it, the optimisation algorithm tries to organise the maintenance in such a way that during the course of operations, there is a rather stable demand for the number of employees to be constantly present at the facility (which in this case is either 3 or 4 crews for various solutions), and only for the periods of major overhauls, more workers are required (in this example, six crews).
- A closer look at the employee scheduling results reveals that for the normal course of operations, generally, four-week trips with an 8-hour daily working schedule (i.e., crew size of three workers) are preferred. For the weeks when the overhauls are conducted, one-week trips with a 12-hour daily schedule (crew size of two) are preferred.
- A comparison of the produced results with earlier results presented in the paper by Redutskiy et al. (2021) reveals that it was possible to achieve an approx. 15 % reduction in workforce-related costs through a more detailed consideration of the employee scheduling aspects. The solutions presented in Table 7 demonstrate that with this approach, the algorithm is inclined to choose somewhat more elaborate architectures, which

Tab. 7. Optimisation results

Choices of instrumentation and maintenance									
#	Level sensor	Fire detector	PLC	Safety valve 1	Safety valve 2	Pump drive	TI, w	Overhaul period, w	Staff size
1	1oo4 / e / LT5 sequential	2oo8 / e / FD3 sequential	1oo3 / e / PLC2 sequential	1oo3 / e / SV2 sequential	1oo2 / e / SV2 staggered	1oo3 / e / PD2 sequential	12	24	19
2	1oo4 / b / LT4 sequential	2oo8 / e / FD3 sequential	1oo3 / e / PLC2 sequential	1oo2 / e / SV2 sequential	1oo3 / e / SV2 sequential	1oo3 / e / PD2 sequential	12	24	19
3	1oo3 / e / LT4 sequential	2oo6 / e / FD3 sequential	1oo3 / e / PLC2 sequential	1oo3 / b / SV3 staggered	1oo2 / e / SV2 sequential	1oo2 / e / PD2 sequential	16	48	19
4	1oo4 / e / LT5 sequential	2oo8 / e / FD3 sequential	1oo3 / e / PLC2 sequential	1oo3 / e / SV2 sequential	1oo3 / e / SV2 staggered	1oo3 / e / PD2 staggered	16	48	20
5	1oo3 / e / LT4 sequential	2oo6 / e / FD3 sequential	1oo3 / e / PLC2 sequential	1oo3 / e / SV3 sequential	1oo3 / e / SV2 sequential	1oo3 / e / PD2 sequential	16	48	20
6	1oo4 / e / LT5 sequential	2oo8 / e / FD3 sequential	1oo3 / e / PLC2 sequential	1oo3 / e / SV2 sequential	1oo2 / e / SV2 sequential	1oo2 / e / PD2 sequential	16	48	21
7	1oo4 / e / LT5 sequential	2oo6 / e / FD3 sequential	1oo3 / e / PLC2 sequential	1oo2 / e / SV2 staggered	1oo3 / e / SV2 staggered	1oo3 / e / PD2 staggered	12	24	23

Reliability characteristics and cost structure for the Pareto-front solutions							
#	PDF_{AVG}	DT, h	Lifecycle cost, CU	Procurement cost, CU	Cost of operations, CU	Workforce-related costs, CU	Risk costs, CU
1	$2.6208 \cdot 10^{-05}$	142	32 362 339	11 721 650	20 636 203	13 113 790	4 486
2	$2.7351 \cdot 10^{-05}$	143	32 339 055	11 701 730	20 632 643	13 113 790	4 682
3	$3.7958 \cdot 10^{-05}$	98	29 775 209	11 219 360	18 549 351	13 636 924	6 498
4	$3.0243 \cdot 10^{-05}$	97	34 219 297	11 795 778	22 418 341	16 391 556	5 177
5	$3.7958 \cdot 10^{-05}$	98	29 775 209	11 219 360	18 549 351	13 636 924	6 498
6	$2.9056 \cdot 10^{-05}$	96	34 252 125	11 824 353	22 422 799	16 391 556	4 974
7	$2.6208 \cdot 10^{-05}$	142	32 362 339	11 721 650	20 636 203	13 113 790	4 486

results in approx. 15 % higher procurement costs; however, when it comes to the total cost of the solution's lifecycle, a reduction of approx. 3–8 % is observed compared to earlier research which has not accounted for many workforce organisation details.

Conclusions

The paper focuses on the design and maintenance of an ESD system and organising the workforce to maintain this system at a remotely-located hazardous industrial facility. This research shows the benefits of combining the aspects of design, maintenance, and workforce planning into one decision-making framework.

This research has demonstrated the possibility of incorporating complex maintenance policies into a Markov model, an aspect that has not been explored well in the literature. It allowed the optimisation algorithm to choose between the proof tests, which require temporarily shutting down the operations and the policies that can be implemented while the facility is continuously running. In the oil and gas sector, the losses associated with production downtime are significant; therefore, the latter options of testing policies are chosen.

This research has elaborated the employee scheduling model by considering the travel schedule for every employee on the staff, allowing for the introduction of such aspects as the maximum time an employee spends at a remote location annually, as well as ensuring the mandatory continuous vacation period. This allows for a more precise evaluation of the staff size in comparison to standard set-covering formulation when the number of crews taking a certain trip is determined, and the maintenance is planned through the collective notion of the effort of the entire staff.

In addition, this research has focused on each individual employee's travel schedule. This measure allows getting a more accurate size of the crew and limiting the amount of time spent on the remote location to ensure a continuous annual vacation availability for each employee.

The main area for applying the analysis and results produced in this research is developing comprehensive requirements for the safety systems, which should lay the groundwork for the detailed engineering design. Therefore, the obtained results and deduced recommendations correspond to the strategic planning level of an engineering project. From the analysis of the results produced by the developed decision-making framework, the following recommendations have been concluded:

- advisable device models and/or instrumentation manufacturers for particular subsystems.
- advisable redundancies and separation decisions for the SIS subsystems
- advisable maintenance strategy: proof testing frequency and maintenance policy.

In real-life engineering practice, the requirements for safety systems can be vague: in most cases, the documentation merely states that the developed solution has to achieve SIL3. The obtained results may help to shape straightforward recommendations that can be utilised in the requirement specification document.

The main limitation of this research is that the conclusions obtained from the modelling and optimisation results are suitable only for each particular problem context to which they apply. In other words, it is not possible to use the same conclusions for every engineering project or for planning any kind of facility. For example, although PLCs and actuators supplied by vendor V1 were preferred in this case, these device models will not necessarily be chosen for another project case. Nevertheless, the developed approach has proven that at least some conclusions can be drawn for every particular project. Therefore, an insight into strategic SIS planning may be gained.

This research focuses on planning only one SIS among the several automated systems deployed at any real-life hazardous industrial facility. One obvious direction for future research is to extend the decision-making to several SISs and plan the workforce requirements and schedules for the entire facility and for all the automated systems at the facility. Another direction for future research is to apply employee scheduling on the tactical or operative level of decision-making by incorporating more details from the practical perspective of workforce organisation.

Acknowledgements

The authors gratefully acknowledge the support for their research received from the Norwegian Agency for International Cooperation and Quality Enhancement in Higher Education (Diku) as a part of the project "Logistical and environmental management of natural resources, development, and trans-

portation in the Arctic area (Arctic Logistics)", UTF-2016-long-term/10023.

Literature

Bastos, Y. B., Fleck, J. L., & Martinelli, R. (2020). A stochastic programming approach for offshore flight scheduling. *IFAC-PapersOnLine*, *53*(4), 478-484.

Bird, K. J., Charpentier, R. R., Gautier, D. L., Houseknecht, D. W., Klett, T. R., Pitman, J. K., Moore, T. E., Schenk, Ch. J., Tennyson, M. E., & Wandrey, C. R. (2008). *Circum-Arctic resource appraisal: Estimates of undiscovered oil and gas north of the Arctic Circle*. Fact Sheet, No. 2008-3049. US Geological Survey.

Boudreaux, M. (2010). Safety Lifecycle Seminar. *Emerson Global Users Exchange - Annual Technical Conference*, 27 September - 1 October, 2010. San Antonio, Texas, the USA.

British Petroleum (BP). (2022). *BP Statistical Review of World Energy*. London, UK.

Bukowski, J. V. (2006). Using Markov models to compute probability of failed dangerous when repair times are not exponentially distributed. *Annual Reliability and Maintainability Symposium (RAMS'06)*, IEEE, 273-277.

Castillo-Salazar, J. A., Landa-Silva, D., & Qu, R. (2016). Workforce scheduling and routing problems: literature survey and computational study. *Annals of Operations Research*, *239*(1), 39-67.

Centre for Chemical Process Safety (CCPS). (2010). *Guidelines for Safe Process Operations and Maintenance*. John Wiley & Sons.

Dantzig, G. B. (1954). Letter to the editor – A comment on Edie's Traffic delays at toll booths. *Journal of the Operations Research Society of America*, *2*(3), 339-341.

De La Vega, J., Santana, M., Pureza, V., Morabito, R., Bastos, Y., & Ribas, P. C. (2022). Model - based solution approach for a short-term flight rescheduling problem in aerial passenger transportation to maritime units. *International Transactions in Operational Research*, *29*(6), 3400-3434.

Deb, K. (2001). *Multi-Objective Optimization using Evolutionary Algorithms*. John Wiley & Sons.

Gabriel, A., Ozansoy, C., & Shi, J. (2018). Developments in SIL determination and calculation. *Reliability Engineering & System Safety*, *177*, 148-161.

Goble, W. M. (2010). *Control Systems Safety Evaluation and Reliability*, 3rd ed. Research Triangle Park: ISA.

Health and Safety Executive (HSE). (2003). *Out of Control*, 2nd ed. HSE Books, UK.

Helber, S., & Henken, K. (2010). Profit-oriented shift scheduling of inbound contact centers with skills-based routing, impatient customers, and retrials. *OR Spectrum*, *32*(1), 109-134.

Hermeto, N. D. S. S., Ferreira Filho, V. J. M., & Bahiense, L. (2014). Logistics network planning for offshore air transport of oil rig crews. *Computers & Industrial Engineering*, *75*, 41-54.

International Electrotechnical Commission (IEC) 61508. (1998/2010). *Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems*. IEC, Geneva, Switzerland.

International Electrotechnical Commission (IEC) 61511. (2003/2016). *Functional Safety – Safety Instrumented Systems for the Process Industry*. IEC, Geneva, Switzerland.

Jin, H., Lundteigen, M. A., Rausand, M. (2011). Reliability performance of safety instrumented systems: A common approach for both low-and high-demand mode of operation. *Reliability Engineering & System Safety*, *96*(3), 365-373.

Kuo, W., & Zuo, M. J. (2003). *Optimal reliability modeling. Principles and applications*.

Mellemvik, F., Bambulyak, A., Gudmestad, O., Overland, I., & Zolotukhin, A. (2015). *International Arctic Petroleum Cooperation*. New York: Routlege.

Redutskiy, Y. (2017). Optimization of safety instrumented system design and maintenance frequency for oil and gas industry processes. *Management and Production Engineering Review*, *8*(1), 46-59.

Redutskiy, Y. (2018). Pilot study on the application of employee scheduling for the problem of safety instrumented system design and maintenance planning for remotely located oil and gas facilities. *Engineering Management in Production and Services*, *10*(4), 55-64.

Redutskiy, Y., Camitz-Leidland, C. M., Vysochyna, A., Anderson, K. T., & Balycheva, M. (2021). Safety systems for the oil and gas industrial facilities: Design, maintenance policy choice, and crew scheduling. *Reliability Engineering & System Safety*, *210*, 107545.

Soriano, J., Jalao, E. R., & Martinez, I. A. (2020). Integrated employee scheduling with known employee demand, including breaks, overtime, and employee preferences. *Journal of Industrial Engineering and Management*, *13*(3), 451-63.

Srivastav, H., Barros, A., & Lundteigen, M. A. (2020). Modelling framework for performance analysis of SIS subject to degradation due to proof tests. *Reliability Engineering & System Safety*, *195*, 106702.

STC Industrial Safety (Closed Joint-Stock Company Scientific technical center of industrial safety problems research). (2014). *Federal law "On industrial safety of hazardous production facilities"* STC Industrial safety CJSC, Moscow, Russia.

The Norwegian Oil and Gas Association. (2018). *070 – Application of IEC61508 and IEC61511 in the Norwegian Petroleum Industry*, Norwegian Oil and Gas, Sandnes, Norway.

Torres-Echeverria, A. C. (2009). *Modelling and optimization of Safety Instrumented Systems based on dependability and cost measures*. PhD thesis, The University of Sheffield, Sheffield, the UK.

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

Vieira, T., De La Vega, J., Tavares, R., Munari, P., Morabito, R., Bastos, Y., & Ribas, P. C. (2021). Exact and heuristic approaches to reschedule helicopter flights for personnel transportation in the oil industry. *Trans-*

portation Research Part E: Logistics and Transportation Review, *151*, 102322.

Zhao, J., Si, S., & Cai, Z. (2019). A multi-objective reliability optimization for reconfigurable systems considering components degradation. *Reliability Engineering & System Safety*, *183*, 104-115.