Management and Production Engineering Review
Volume 8 • Number 1 • March 2017 • pp. 46–59
DOI: 10.1515/mper-2017-0006

DE G DE GRUYTER OPEN mper

OPTIMIZATION OF SAFETY INSTRUMENTED SYSTEM DESIGN AND MAINTENANCE FREQUENCY FOR OIL AND GAS INDUSTRY PROCESSES

Yury Redutskiy

Molde University College, Faculty of Logistics, Norway

Corresponding author:
Yury Redutskiy
Molde University College
P.O. Box 2110, NO-6402 Molde, Norway
phone: (+47) 71-19-57-94
e-mail: Yury.Redutskiy@HiMolde.no

Received: 11 October 2016
Accepted: 26 January 2017

Abstract

Oil and gas industry processes are associated with significant expenditures and risks. Adequacy of the decisions on safety measures made during early stages of planning the facilities and processes contributes to avoiding technological incidents and corresponding losses. Formulating straightforward requirements for safety instrumented systems that are followed further during the detailed engineering design and operations is proposed, and a mathematical model for safety system design is introduced in a generalized form. The model aims to reflect the divergent perspectives of the main parties involved in oil and gas projects, and, therefore, it is formulated as a multi-objective problem. Application of black box optimization is suggested for solving real-life problem instances. A Markov model is applied to account for device failures, technological incidents, continuous restorations and periodic maintenance for a given process and safety system configuration. This research is relevant to engineering departments and contractors, who specialize in planning and designing the technological solution.

Keywords

emergency shutdown system, Markov models, multiple-criterion optimization, safety instrumented system, systems design, risk management.

Introduction

The technology of oil and gas production and processing is associated with considerable hazards. The mixture of petroleum and impurities is delivered from the reservoir through the wellheads and the gathering infrastructure to the processing facilities, where oil and gas are separated and prepared for further transportation to storage depots, refineries, and export to the end users. These processes are carried out on hazardous industrial facilities, where the occurrence of an incident may lead to significant economic losses, harm to personnel, environmental damage and other negative socio-political consequences. Proper design of processes and industrial instrumentation contributes significantly to the safety of operations on such hazardous facilities.

The international standard IEC 61511 [1] introduces the term *safety instrumented system* (SIS) and defines this concept as a system that consists of *sensors*, *logic solvers* and *final control elements* (Fig. 1a), and implements one or several safety functions, e.g., protection of facility personnel and assets, general public, environment, etc. Several SIS are usually put in place. The systems work as layers or "barriers" aimed at reducing the risk, to which the hazardous facility is exposed [2]. *Distributed control systems* (DCS) run and control the technology and additionally play the role of preliminary safety measures. The next barrier is *emergency shutdown* (ESD) systems, which bring the facility to a full stop in case of a hazard. DCS and ESD aim at preventing the hazardous situations from occurrence. Further measures are put in place to mitigate the consequences of hazards. Such measures include SIS, e.g., *Fire & Gas* (F&G) detection systems, *fire suppression* systems and potentially others, as well as barriers of a different nature, e.g., *emergency response* of the facility personnel and local community. Among the SIS, typical for process industries, such as oil and gas sector, the most significant risk reduction is ensured by ESD systems, which respond to highly critical situations that can quickly escalate to hazards with significant consequences [3]. Thus, it is imperative to ascertain that the safety systems, especially the ESD system, are properly designed in order to perform their functions correctly.

Infrastructures for petroleum production and processing are built while implementing an engineering project, which undergoes particular stages. The project is initiated by an exploration and production (E&P) operator, and it begins with a *conceptual design* stage when general information about the appropriate technology, facilities, and solutions is studied and evaluated. It is a common practice for E&P operators to delegate further work on the engineering design to contractors. The E&P operator formulates the *requirements specification*, a document containing a set of requirements to be fulfilled further by the contractors. The general requirements for different systems, including the safety-related systems, and their functions are developed at this stage. Those requirements are sought to be followed during the *detailed engineering design* stage when a particular technological solution is developed. Later, the facilities are *commissioned*, *tested* and prepared for the *operations*. The engineering contractor provides further service and support according to the warranty.

Statistics[1] demonstrate that dozens of incidents occur in the petroleum sector yearly. In 2003, the British agency Health and Safety Executive conducted a careful analysis of a sample of incidents and their circumstances. The analysis revealed that in almost half of the cases, the cause of hazards was the inadequacy of requirement specification leading to the inadequate safety level of the designed control systems responsible for the safety of operations [4].

The design of SIS for industrial facilities is associated with the choice of certain apparatus among the options available on the market, choice of certain instrumentation architectures, decisions on introducing additional safety measures, and planning the maintenance of facilities and instrumentation systems. During the early phase of planning, general requirements are formulated and later they are followed through during the stage of detailed engineering design and operations. According to HSE [4], insufficient specificity of such requirements to SIS often results in the development of a solution that marginally ensures the required level of safety. Had the detailed analysis been conducted, it would have revealed that far better options could have been chosen from among the alternatives of equipment used by the engineering contractor and the available safety measures often chosen by companies.

The objective of this work is to address the problem of optimizing the set of safety measures inherent in SIS for the purpose of formulating straightforward requirements that could be a starting point for the detailed engineering design.

Overview of the research area

Extensive research in modelling and optimizing SIS has already been conducted by many scientists and institutions. Modelling the systems is based primarily on reliability theory. The standards IEC 61508 [5] and 61511 [1] propose methods of safety quantification with the help of simplified equations based on Reliability Block Diagrams (RBD) and Fault Tree Analysis (FTA). The two approaches are rather simple and visual, they work with static methods and mean values. Other researchers [6, 7] use Markov Analysis (MA), a more complex approach that works with dynamic models. A significant contribution to the domain was made by Norwegian researchers who have been developing the PDS method [8]. Several comparative studies were conducted on the issue of applying these methods (RBD, FTA, MA and others). The works [9, 10] conclude that the best two methods are FTA and MA; however, MA provides more flexibility for incorporating many failure modes and analysing their interactions.

The problems of optimizing the SIS design fall into categories of *reliability allocation*, *redundancy allocation*, or simultaneous *reliability and redundancy allocation*. Most of the current research is focused on the latter category. Many models [11, 12] also address the issues of optimizing the proof testing policies. An interested reader can find a detailed overview of reliability modelling techniques and design optimization in the books [13] and [14]. The latter source also provides an insight into algorithmic perspective for the SIS design problems. The author points out that classical discrete optimization methods, such as dynamic programming or implicit enumeration, have rather

[1] Statistical data on incidents in the petroleum industry are provided in the databases of governmental agencies, such as http://www.hse.gov.uk, http://www.atsdr.cdc.gov, http://en.gosnadzor.ru, and other resources.

limited application to real-life instances. It is common for the reliability-redundancy allocation problems that the functions brought to use are defined in the form of tables, or obtained as a result of complex modelling. Because of this, the black box optimization algorithms are often applied. It is worth noting that several researchers suggest multi-objective optimization of the SIS design [15, 16].

In the research mentioned above, the authors study the positive and negative impact of deploying a SIS: the instrumentation reduces the possibility of incidents and hazardous consequences, but at the same time, SIS triggers unwanted disruptions and shutdowns, which lead to production losses. Most research focuses entirely on those two mechanisms of SIS performance, which leads to the lack of representation of technological incidents in the models. Few works [6, 17, 18] attempt to incorporate occurrence of incidents into a Markov model. However, in most cases, the authors stick to aggregated models, where the multiple modes of SIS failure or multiple functions of SIS are represented with generalized states of the model.

In this paper, the problem of SIS design will be addressed within the multi-objective optimization setting. Markov analysis will be applied for modelling the performance of SIS to account for device failures occurrence and repairs, as well as the occurrence of technological incidents and execution of facility maintenance work over the lifecycle of a hazardous facility.

SIS design

Problem setting

The structure of any SIS can be represented by a control loop, as shown in Fig. 1a. Process value transmitters are sensors monitoring process values of the technological parameters. The logic solver is a programmable logic controller (PLC), which receives the signals from the transmitters and, in its turn generates an output control signals according to the programmed algorithm. The signals go to actuators or 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, etc.

In practice, SIS monitors several process parameters, and at the same time process control involves several actions to be performed, e.g. facility shutdown requires some valves to close and others to open, pumps and compressors need to be stopped, etc. This can be represented by Fig. 1c. In terms of the reliability block diagram, this design can be represented as a series structure of several subsystems (Fig. 1d).

When the SIS is designed, particular device models of transmitters, PLCs and actuators are chosen out of a set of functionally analogous alternatives available on the market. Additional measures are introduced to ensure a certain level of safety. One of such measures is redundancy. Each block representing instrumentation on the diagram in Fig. 1a consists of one or more identical devices performing the prescribed function. This is why the blocks are often referred to as subsystems represented by their M-out-of-N ($M$oo$N$) redundancy architectures (Fig. 1b), where N is the total number of identical devices in the subsystem, and M is the number of devices needed to be in operating condition so that the subsystem's intended function could be performed.

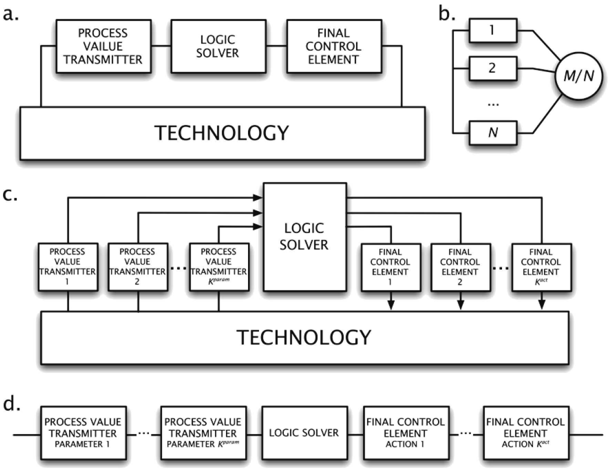
a.
PROCESS VAILUE TRANSMITTER
LOGIC SOLVER
FINAL CONTROL ELEMENT
TECHNOLOGY
b.
1
2
...
N
M/N
c.
PROCESS VALUE TRANSMITTER 1
PROCESS VALUE TRANSMITTER 2
PROCESS VALUE TRANSMITTER K^param
LOGIC SOLVER
FINAL CONTROL ELEMENT 1
FINAL CONTROL ELEMENT 2
FINAL CONTROL ELEMENT K^act
TECHNOLOGY
d.
PROCESS VALUE TRANSMITTER PARAMETER 1
PROCESS VALUE TRANSMITTER PARAMETER K^param
LOGIC SOLVER
FINAL CONTROL ELEMENT ACTION 1
FINAL CONTROL ELEMENT ACTION K^act

Fig. 1. a) Structure of one control loop of SIS, based on [1]; b) subsystem of SIS, based on [1]; c) structure of real-life SIS; d) reliability block diagram of a real-life SIS.

Another measure considered during the SIS design is the introduction of additional electrical and physical separation of the devices in each subsystem. This is done to mitigate the phenomenon of common-cause failure (CCF) when all the components of a subsystem (Fig. 1b) fail simultaneously.

Instrumentation maintenance is another important aspect of planning SIS. The maintenance of equipment is executed in two forms: continuously during the process, and periodically in the form of proof tests. When a detected failure of a device takes place, the device is repaired or replaced within a predefined time limit. For the purpose of fixing all the undetected failures, proof tests are conducted with an interval *TI*. These tests are associated with costs of labour and tools as well as losses due to facility downtime for the duration of the tests. Expensive and highly reliable instrumentation with elaborate redundancy structures usually requires infrequent proof testing, and, conversely, cheaper devices and simpler redundancies need to be examined and maintained often. Thus, both design and maintenance planning are associated with expenditures in the long run, and so a trade-off between the costs and losses needs to be explored.

Thereby, the problem of SIS design and maintenance frequency optimization should include the following decision variables:

- particular device models of transmitters, logic solvers, and final control elements from the databases of alternatives,
- redundancy scheme ($M$oo$N$) for each subsystem;
- additional separation of electric circuits for mitigating common-cause failures;
- test interval, corresponding to the periodic maintenance frequency.

To formulate the optimization problem, the objectives and priorities of parties involved in oil and gas sector projects should be accounted for. The role of international standards IEC 61508 [5] and 61511 [1] is evident for hazardous facilities requiring certain safety measures. The standards propose economic consideration of introducing any safety measure called the ALARP principle of risk-reduction. The acronym is used to formalize driving the target level of risk to a certain solution to be "as low as reasonably practicable", i.e. a safety measure should only be introduced if the benefits of employing the measure prove to be greater than the cost of the risk reduction measure. In addition to this suggestion of economically substantiated design, the standards provide the framework for quantification of requirements to the system's safety integrity level (SIL). For the safety systems operating in "low-demand mode"[2], such as the ESD system, the standards provide the following requirements (Table 1):

- risk-reduction requirements are provided in the form of value range for average probability of failure on demand (PFD$_{\text{avg}}$, i.e. the probability of SIS failure when there is actual demand for its function),
- fault tolerance requirements, which are presented as a combination of two parameters: fault tolerance (FT, the number of components in a $M$oo$N$ subsystem that are allowed to fail) and safe failure fraction (SFF, the percentage of all safe and detected failures for a subsystem).

The international standards are adopted in most countries and affirmed as governmental regulations specifying the necessary SIL for the processes in particular branches of industries[3]. Since the petroleum industry deals with hydrocarbons and other flammable and toxic substances, the facilities performing the primary functions require safety systems ensuring SIL 3.

Another perspective necessary to consider for petroleum industry projects is the perspective of E&P operators, companies investing in the development of new industrial facilities and infrastructures and their operation. The E&P operator's goal is profit in the long run, and thus the company is concerned about two things: first, capital expenditures for building the facilities and setting up the process safety systems, and second, revenues from the operations during the lifecycle of their projects, which means that they strive for smooth production operations, or in other words, they wish to minimize facility downtime.

The contractors who develop the engineering solutions including the necessary safety systems have their own angle in the engineering design context. Since the contractors are participating in bidding competitions to be hired for their services, their goal is cheap solutions.

Table 1
Requirements for safety integrity level, suggested by IEC 61508 [5] and 61511 [1].

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

[2] The system "where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof test frequency", IEC61508 [5].

[3] Examples of governmental regulations on SIL in the petroleum industry: in Norwegian legislation [19], in Russian legislation [20].

Keeping in mind these priorities of the parties involved in oil and gas projects, the following objectives will further be considered in this work:

- average probability of failure on demand represents the mechanisms of failures and incidents occurrence,
- mean downtime of the technological facility presents the expected value of the technological facility being in the shutdown state; instrumentation failures and spurious trips contribute to the downtime, and so do the technological incidents,
- lifecycle cost of a facility functioning with an ESD system.

The generalized mathematical representation of the optimization problem is presented below. The necessary notations are provided in Table 2. The objective functions are given in (1).

$$\begin{gathered}\min \mathrm{PFD}_{\mathrm{avg}}\left(X^{\mathrm{inst}}, X^{\mathrm{red}}, X^{\mathrm{sep}}, TI\right), \\ \min \mathrm{DT}\left(X^{\mathrm{inst}}, X^{\mathrm{red}}, X^{\mathrm{sep}}, TI\right) \\ \min \mathrm{C}_{\mathrm{lifecycle}}\left(X^{\mathrm{inst}}, X^{\mathrm{red}}, X^{\mathrm{sep}}, TI\right).\end{gathered} \tag{1}$$

Table 2
Notations for the SIS design optimization problem.

Notation	Description
	Indices and sets
q	index of subsystems, $q = 1$ corresponds to process value transmitters, $q = 2$ corresponds to logic solvers, $q = 3$ corresponds to final control elements
l	index of device models
r	index of redundancy schemes
S_q^{inst}	set of device model alternatives for instrumentation subsystem q
S_q^{red}	set of redundancy alternatives for instrumentation subsystem q
	Decision variables
x_{lq}^{inst}	binary decision variable: equals 1, if device model l is chosen for subsystem q; 0, otherwise
x_{rq}^{red}	binary decision variable: equals 1, if redundancy option r is chosen for subsystem q; 0, otherwise
x_q^{sep}	binary decision variable: equals 1, if additional electrical/physical separation is introduced for subsystem q; 0, otherwise
TI	integer decision variable: time between two consecutive proof tests, [month]
	Functions
$\mathrm{PFD}_{\mathrm{avg}}$	average probability of failure on demand
DT	facility downtime
$\mathrm{C}_{\mathrm{lifecycle}}$	lifecycle cost of the solution
SIL^{RR}	risk reduction requirement for achieving a certain safety integrity level defined in Table 1
SIL^{FT}	fault tolerance requirement for achieving a certain safety integrity level defined in Table 1

Here, the first three arguments in the parenthesis are matrices and a vector of corresponding design binaries, as explained in (2).

$$\begin{gathered}X^{\mathrm{inst}} = \left\{x_{lq}^{\mathrm{inst}}\right\}, \qquad X^{\mathrm{red}} = \left\{x_{rq}^{\mathrm{red}}\right\}, \\ X^{\mathrm{sep}} = \left\{x_q^{\mathrm{sep}}\right\}.\end{gathered} \tag{2}$$

The optimization problem solutions are stipulated to achieve the necessary target SIL*, prescribed by governmental regulations on safety. The requirements stated in Table 1 can be rewritten in the form of constraints (3) and (4).

$$\mathrm{SIL}^{RR}\left(X^{\mathrm{inst}}, X^{\mathrm{red}}, X^{\mathrm{sep}}, TI\right) = \mathrm{SIL}^{*}, \tag{3}$$

$$\mathrm{SIL}^{FT}\left(X^{\mathrm{inst}}, X^{\mathrm{red}}, X^{\mathrm{sep}}, TI\right) = \mathrm{SIL}^{*}. \tag{4}$$

Logical constraints need to be imposed on the binary design decision variables: for a particular subsystem, only one device model should be chosen (5), as well as only one redundancy option (6).

$$\sum_{l \in S_q^{\mathrm{inst}}} x_{lq}^{\mathrm{inst}} = 1, \qquad \forall q, \tag{5}$$

$$\sum_{r \in S_q^{\mathrm{red}}} x_{rq}^{\mathrm{red}} = 1, \qquad \forall q. \tag{6}$$

Thus, expressions (1) and (3)–(6) represent the multi-objective optimization problem of the ESD system design and its maintenance frequency.

Modelling assumptions

The occurrence of device failures, incidents and repairs is considered to be stochastic and modelled in the framework of reliability theory. Equation (7) demonstrates the exponential distribution for the probability of failure occurrence, which corresponds to constant failure rate. This is a valid assumption for complex systems with electronic components [10]

$$p(t) = 1 - e^{-\lambda \cdot t}. \tag{7}$$

Further, the notations provided in Table 3 will be applied to indicate different failure modes for modelling devices and instrumentation subsystems.

From the most general perspective, the failures can be divided into random and systematic [8]. The former ones are caused by the components degradation with time and are unforeseen, whereas the latter can be easily connected to mistakes in design and implementation, and thus mitigated.

The random failures of the ESD can be either dangerous failures or safe failures. IEC 61508 [5] gives the following definition of dangerous failures: they are failures that put SIS “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 threaten the SIS's capabilities to perform when needed. The occurrence of such failures (spurious trips) is represented by the SIS taking action without any actual demand.

Table 3
Common notations used for failure classification, used in numerous sources, e.g., in [10, 16].

Notation	Description
Superscript notations	
DF	dangerous failure
DD	dangerous detected failure
DU	dangerous undetected failure
RF	random hardware failure
ST	spurious trips
Applicability of the notations	
λ	failure rate
p	probability of failure

Repairs of the devices and technology restorations will also be modelled as exponentially distributed events with the constant failure rate. In the paper [6], the author concludes that the assumption of constant repair rate produced as the reciprocal of the average device repair time is an optimistic one. In this work, the models will be fit out for more pessimistic results by producing the repair rates as reciprocals of the maximum allowed repair time.

Markov models of failure and incident occurrence will be further described. The approach to modelling is largely based on the ideas presented in [17] and [18], meanwhile the necessary adaptations are made for the purpose of further calculation of costs and other specifics considered in this work. The model of lifecycle cost follows the logic of [10] and its adaptation in [16], with additional modifications for the necessity of this research.

Further considerations concern mathematical modelling of failure and incident occurrence as well as restoration processes taking place. A summary of the assumptions made is provided below:

- only random hardware failures are considered;
- failure classification presented in Table 3 is used; with this approach, we assume that all safe failures are detected because a spurious trip leads to the shutdown of the technology;
- technology is shut down for an overhaul in case a detected failure (DD or ST) occurs;
- the occurrence of failures, incidents, repairs, and restorations is described by the exponential distribution;
- periodically conducted proof tests are considered perfect, i.e. all undetectably failed devices are restored.

Failures and repairs in a subsystem

The dangerous and safe failures of components of any subsystem are modelled for the time interval between two consecutive proof tests: [0, TI]. Markov processes describing the independent failures in a subsystem with $M$oo$N$ architecture include $(N-M+2)$ states (Fig. 2). State 1 represents the operating state for all N components. State 2 corresponds to the failure of one component. Each further state represents the failure of one more component. The entire subsystem fails to perform the prescribed instrumented function when $(N-M+1)$ components fail, which corresponds to the last state on the graph. Independent failures are depicted by left-to-right transitions on the graph. Common cause failures are depicted by the direct transition from any state to the last state on the graph. Repairs are depicted by right-to-left transitions. The last state is the absorbing state: if the process moves to this state, the facility is shut down, and a major overhaul is to be performed.

Table 4
Notations used for the subsystem modelling.

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

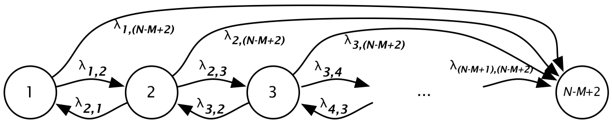

Fig. 2. Markov process of failures and repairs in a subsystem with $MooN$ architecture.

Markov model equations are presented further separately for the three modelled failure modes: (8)–(11) for DU failures, (12)–(15) for DD failures and (16)–(19) for ST.

Markov model of dangerous undetected failures in a subsystem:

$$\begin{gathered}\frac{dp_j^{\mathrm{DU}}(t)}{dt} = \sum_{i=1}^{N-M+2} p_i^{\mathrm{DU}}(t)\cdot\lambda_{i,j}^{\mathrm{DU}}, \\ j \in \{1,\ldots,(N-M+2)\},\end{gathered} \tag{8}$$

$$\begin{gathered}\lambda_{i,i}^{\mathrm{DU}} = -\lambda\cdot(1-\varepsilon)\cdot[(N-i+1)\cdot(1-\beta)+\beta], \\ \lambda_{i,(i+1)}^{\mathrm{DU}} = (N-i+1)\cdot(1-\varepsilon)\cdot(1-\beta)\cdot\lambda, \\ \lambda_{i,(N-M+2)}^{\mathrm{DU}} = (1-\varepsilon)\cdot\beta\cdot\lambda, \\ i\in\{1,\ldots,(N-M+2)\},\end{gathered} \tag{9}$$

$$\begin{gathered}p_1^{\mathrm{DU}}(0)=1, \qquad p_i^{\mathrm{DU}}(0)=0, \\ i\in\{2,\ldots,(N-M+2)\},\end{gathered} \tag{10}$$

$$\lambda^{\mathrm{DU}} = -\frac{\log\left(1-p_{N-M+2}^{\mathrm{DU}}(\mathrm{TI})\right)}{\mathrm{TI}}. \tag{11}$$

Markov model of dangerous detected failures in a subsystem:

$$\begin{gathered}\frac{dp_j^{\mathrm{DD}}(t)}{dt} = \sum_{i=1}^{N-M+2} p_i^{\mathrm{DD}}(t)\cdot\lambda_{i,j}^{\mathrm{DD}}, \\ j \in \{1,\ldots,(N-M+2)\},\end{gathered} \tag{12}$$

$$\begin{gathered}\lambda_{1,1}^{\mathrm{DD}} = -\varepsilon\cdot\lambda\cdot[N\cdot(1-\beta)-\beta], \\ \lambda_{1,2}^{\mathrm{DD}} = N\cdot\varepsilon\cdot(1-\beta)\cdot\lambda, \\ \lambda_{1,(N-M+2)}^{\mathrm{DD}} = \varepsilon\cdot\beta\cdot\lambda, \\ \lambda_{i,(i-1)}^{\mathrm{DD}} = (i-1)\cdot\mu, \\ \lambda_{i,i}^{\mathrm{DD}} = -\varepsilon\cdot\lambda\cdot[(N-i+1)\cdot(1-\beta)+\beta] \\ -(i-1)\cdot\mu, \\ \lambda_{i,(i+1)}^{\mathrm{DD}} = (N-i+1)\cdot\varepsilon\cdot(1-\beta)\cdot\lambda, \\ \lambda_{i,(N-M+2)}^{\mathrm{DD}} = \varepsilon\cdot\beta\cdot\lambda, \\ i\in\{2,\ldots,(N-M+2)\},\end{gathered} \tag{13}$$

$$\begin{gathered}p_1^{\mathrm{DD}}(0)=1, \qquad p_i^{\mathrm{DD}}(0)=0, \\ i\in\{2,\ldots,(N-M+2)\},\end{gathered} \tag{14}$$

$$\lambda^{\mathrm{DD}} = -\frac{\log\left(1-p_{N-M+2}^{\mathrm{DD}}(\mathrm{TI})\right)}{\mathrm{TI}}. \tag{15}$$

Markov model of spurious trips in a subsystem:

$$\begin{gathered}\frac{dp_j^{\mathrm{ST}}(t)}{dt} = \sum_{i=1}^{N-M+2} p_i^{\mathrm{ST}}(t)\cdot\lambda_{i,j}^{\mathrm{ST}}, \\ j \in \{1,\ldots,(N-M+2)\},\end{gathered} \tag{16}$$

$$\begin{gathered}\lambda_{1,1}^{\mathrm{ST}} = -\lambda^S\cdot[N\cdot(1-\beta)-\beta], \\ \lambda_{1,2}^{\mathrm{ST}} = N\cdot(1-\beta)\cdot\lambda^S, \\ \lambda_{1,(N-M+2)}^{\mathrm{ST}} = \beta\cdot\lambda, \\ \lambda_{i,(i-1)}^{\mathrm{ST}} = (i-1)\cdot\mu, \\ \lambda_{i,i}^{\mathrm{ST}} = -\lambda^S\cdot[(N-i+1)\cdot(1-\beta)+\beta] \\ -(i-1)\cdot\mu, \\ \lambda_{i,(i+1)}^{\mathrm{ST}} = (N-i+1)\cdot(1-\beta)\cdot\lambda^S, \\ \lambda_{i,(N-M+2)}^{\mathrm{ST}} = \beta\cdot\lambda^S, \\ i\in\{2,\ldots,(N-M+2)\},\end{gathered} \tag{17}$$

$$\begin{gathered}p_1^{\mathrm{ST}}(0)=1, \qquad p_i^{\mathrm{ST}}(0)=0, \\ i\in\{2,\ldots,(N-M+2)\},\end{gathered} \tag{18}$$

$$\lambda^{\mathrm{ST}} = -\frac{\log\left(1-p_{N-M+2}^{\mathrm{ST}}(\mathrm{TI})\right)}{\mathrm{TI}}. \tag{19}$$

The provided equations are relevant for every subsystem of the considered safety system. The subsystem index q is omitted from the notations for the sake of simplicity.

For any failure mode, the probability of the subsystem being in a particular Markov model state is described by a set of ordinary differential equations (8), (12) and (16), known as Kolmogorov forward equations.

For the transitions depicted on the graph in Fig. 2, the non-zero transition rates are given in (9), (13) and (17) for the three failure modes, respectively. All the rest transition rates are zeroes. The starting point of the stochastic process is state 1, which corresponds to the initial distribution of probabilities in (10), (14) and (18).

The probability of the DU, DD and ST failures for the modelled subsystem is the probability of the stochastic process being in the state $(N-M+2)$. Given the exponential distribution of failures, the corresponding failure rates are obtained in the expressions (11), (15) and (19) for the three failure modes, respectively.

Lifecycle modelling from the safety perspective

For each subsystem of the ESD system, the following possible states are considered:

- the subsystem is performing its function,

- the subsystem is under overhaul due to a DD failure,
- the subsystem is under overhaul due to an ST,
- the subsystem is in the DU failure mode.

For the technology, the following states are considered:

- technology is running on the facility,
- technology is in the shutdown state,
- the technological incident has occurred.

The occurrence of failures in the three subsystems and technological incidents is described in Table 5. The transitions between the states are represented by the graph in Fig. 3.

Table 5
Markov model for the lifecycle.

#	PVT	LS	FCE	Tech	Comments
1	up	up	up	up	normal course of the process
2	up	up	up	down	safety function performed
3	O/S	up	up	down	overhaul after a spurious trip
4	up	O/S	up	down	
5	up	up	O/S	down	
6	O/D	up	up	down	overhaul after a dangerous detected failure
7	up	O/D	up	down	
8	up	up	O/D	down	
9	failure	up	up	up	undetected failure has occurred
10	up	failure	up	up	
11	up	up	failure	up	
12	ESD is down, the incident has occurred				failure on demand state

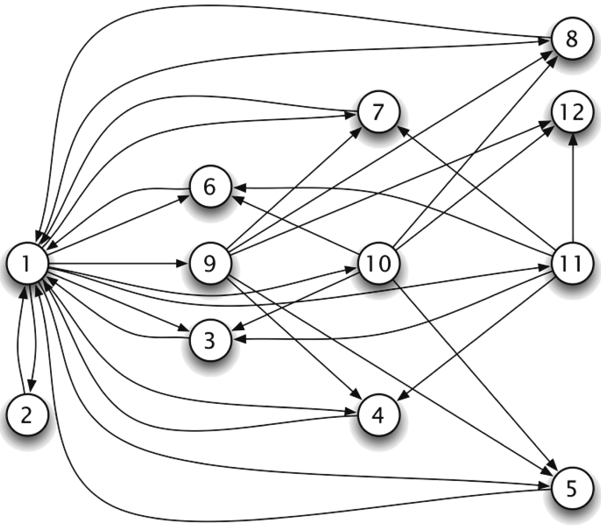

Fig. 3. Markov process of failures, incidents, and restorations over the system lifecycle.

Incidents, failures, and repairs are modelled during the entire lifecycle of the technological unit with the deployed safety system. The lifecycle is divided into K (Fig. 4) periods (20).

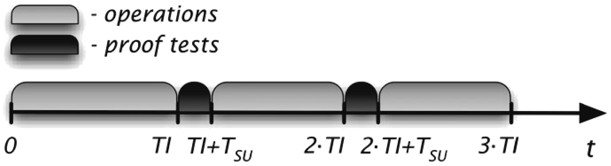

Fig. 4. Time horizon for lifecycle modelling.

Table 6
Notations used for lifecycle modelling from the safety perspective.

Notation	Description
Indices, parameters, and functions	
i, j	indices of states for Markov model
q	index of ESD subsystems
k	index of time periods between the proof tests
t	time, [h]
$p_j(t)$	the probability of the process being in the j-th state
$\lambda_{i,j}$	transition rate from state i to state j, [h^{-1}]
Output of the model	
$\mathrm{PFD_{avg}}$	average probability of failure on demand
DT	mean down time of the process, hours
t	time, [h]
LC_h	duration of the lifecycle, [h]
r	incidents occurrence rate, [h^{-1}]
μ^t	restoration rate for the technology, [h^{-1}]
μ	repair rate for one component, [h^{-1}]
λ_q^{DU}	DU failure rate for the q-th subsystem, [h^{-1}]
λ_q^{DD}	DD failure rate for the q-th subsystem, [h^{-1}]
λ_q^{ST}	ST rate for the q-th subsystem, [h^{-1}]
π_j^k	initial condition for the k-th time period

$$K = \left\lceil \frac{\mathrm{LC}_h}{\mathrm{TI}} \right\rceil, \tag{20}$$

$$\begin{gathered} t \in [0;\mathrm{TI}] \cup [\mathrm{TI} + T_{SU}; 2 \cdot \mathrm{TI}] \\ \cup [2 \cdot \mathrm{TI} + T_{SU}; 3 \cdot \mathrm{TI}] \cup \ldots \\ \cup [(K-1) \cdot \mathrm{TI} + T_{SU}; K \cdot \mathrm{TI}], \end{gathered} \tag{21}$$

$$\begin{gathered} \frac{dp_j\,(t)}{dt} = \sum_{i=1}^{12} p_j\,(t) \cdot \lambda_{i,j}, \\ j \in \{1,\ldots,12\}, \end{gathered} \tag{22}$$

$$\begin{aligned}
&\lambda_{1,1} = -\left(\sum_q \lambda_q^{\mathrm{DU}} + \sum_q \lambda_q^{\mathrm{DD}} + \sum_q \lambda_q^{\mathrm{ST}} + r\right),\\
&\lambda_{1,2} = r, \qquad \lambda_{1,3} = \lambda_1^{\mathrm{ST}},\\
&\lambda_{1,4} = \lambda_2^{\mathrm{ST}}, \qquad \lambda_{1,5} = \lambda_3^{\mathrm{ST}},\\
&\lambda_{1,6} = \lambda_1^{\mathrm{DD}}, \qquad \lambda_{1,7} = \lambda_2^{\mathrm{DD}},\\
&\lambda_{1,8} = \lambda_3^{\mathrm{DD}}, \qquad \lambda_{1,9} = \lambda_1^{\mathrm{DU}},\\
&\lambda_{1,10} = \lambda_2^{\mathrm{DU}}, \qquad \lambda_{1,11} = \lambda_3^{\mathrm{DU}},\\
&\lambda_{2,1} = \mu^t, \qquad \lambda_{2,2} = -\mu^t,\\
&\lambda_{3,1} = \mu, \qquad \lambda_{3,3} = -\mu,\\
&\lambda_{4,1} = \mu, \qquad \lambda_{4,4} = -\mu,\\
&\lambda_{5,1} = \mu, \qquad \lambda_{5,5} = -\mu,\\
&\lambda_{6,1} = \mu, \qquad \lambda_{6,6} = -\mu,\\
&\lambda_{7,1} = \mu, \qquad \lambda_{7,7} = -\mu,\\
&\lambda_{8,1} = \mu, \qquad \lambda_{8,8} = -\mu,\\
&\lambda_{9,4} = \lambda_2^{\mathrm{ST}}, \qquad \lambda_{9,5} = \lambda_3^{\mathrm{ST}},\\
&\lambda_{9,7} = \lambda_2^{\mathrm{DD}}, \qquad \lambda_{9,8} = \lambda_3^{\mathrm{DD}},\\
&\lambda_{9,9} = -\left(\lambda_2^{\mathrm{ST}} + \lambda_3^{\mathrm{ST}} + \lambda_2^{\mathrm{DD}} + \lambda_3^{\mathrm{DD}} + r\right),\\
&\lambda_{9,12} = r, \qquad \lambda_{10,3} = \lambda_1^{\mathrm{ST}},\\
&\lambda_{10,5} = \lambda_3^{\mathrm{ST}}, \qquad \lambda_{10,6} = \lambda_1^{\mathrm{DD}},\\
&\lambda_{10,8} = \lambda_3^{\mathrm{DD}},\\
&\lambda_{10,10} = -\left(\lambda_1^{\mathrm{ST}} + \lambda_3^{\mathrm{ST}} + \lambda_1^{\mathrm{DD}} + \lambda_3^{\mathrm{DD}} + r\right),\\
&\lambda_{10,12} = r, \qquad \lambda_{11,3} = \lambda_1^{\mathrm{ST}},\\
&\lambda_{11,4} = \lambda_2^{\mathrm{ST}}, \qquad \lambda_{11,6} = \lambda_1^{\mathrm{DD}},\\
&\lambda_{11,7} = \lambda_2^{\mathrm{DD}},\\
&\lambda_{11,11} = -\left(\lambda_1^{\mathrm{ST}} + \lambda_2^{\mathrm{ST}} + \lambda_1^{\mathrm{DD}} + \lambda_2^{\mathrm{DD}} + r\right),\\
&\lambda_{11,12} = r,
\end{aligned} \tag{23}$$

$$\pi_1^1 = 1, \qquad \pi_2^1 = 0, \quad \ldots \quad \pi_{12}^1 = 0, \tag{24}$$

$$\begin{aligned}
&\pi_1^k = p_1\left((k-1)\cdot \mathrm{TI}\right) + p_9\left((k-1)\cdot \mathrm{TI}\right)\\
&+p_{10}\left((k-1)\cdot \mathrm{TI}\right) + p_{11}\left((k-1)\cdot \mathrm{TI}\right)\\
&+p_{12}\left((k-1)\cdot \mathrm{TI}\right),\\
&\pi_j^k = p_j\left((k-1)\cdot \mathrm{TI}\right),\\
&j \in \{2,\ldots,8\}, \qquad \pi_j^k = 0,\\
&j \in \{9,\ldots,12\}, \qquad k \in \{2,\ldots,K\},
\end{aligned} \tag{25}$$

$$\mathrm{PFD_{avg}} = \frac{1}{LC_h}\cdot\int\limits_0^{LC_h} \mathrm{PFD}\,(t)\,dt = \frac{1}{\mathrm{TI}}\cdot\int\limits_0^{\mathrm{TI}} p_{12}\,(t)\,dt + \sum_{k=2}^{K}\frac{1}{(\mathrm{TI}-T_{\mathrm{SU}})}\cdot\int\limits_{(k-1)\cdot\mathrm{TI}+T_{\mathrm{SU}}}^{k\cdot\mathrm{TI}} p_{12}\,(t)\,dt, \tag{26}$$

$$\mathrm{DT} = \sum_{j=2}^{8}\left[\int\limits_0^{\mathrm{TI}} p_j\,(t)\,dt + \sum_{k=2}^{K}\int\limits_{(k-1)\cdot\mathrm{TI}+T_{SU}}^{k\cdot\mathrm{TI}} p_j\,(t)\,dt\right]. \tag{27}$$

During each k-th time period of the modelling time horizon (21), the behaviour of the given configuration of SIS and the technology is described by ordinary differential equations (22) for the probabilities of the Markov process being in each state j. The non-zero transition rates (23) correspond to the transitions depicted in Fig. 3 as well as rates of remaining in the current state.

The initial distribution of probabilities is defined at the beginning of every time interval k (21). At the very beginning of the lifecycle (i.e. $k = 1$), the process is in the state 1 (24).

For the following periods $k = 2, 3, \ldots, K$, the initial distribution is defined in (25) under the assumption of perfect proof tests, i.e. all previously undetected failures become resolved. One can observe that the probabilities of being in states 2–8 are monotonic over the entire lifecycle of the system; however, the remaining probabilities fail to be well-behaved at the points of time when proof tests are conducted.

As a result of this modelling (22)–(25), we obtain the values of $p_1(t) \ldots p_{12}(t)$ over the entire lifecycle of the technological unit working with a particular configuration of SIS. Those are used to evaluate the necessary safety indicators: the average probability of failure on demand is obtained in (26) as the mean value of $p_{12}(t)$. Facility downtime of the process is obtained in (27) from the probability of the Markov process being in states 2–8.

Lifecycle modelling from the economic perspective

Design, operations, and maintenance of SIS deployed for hazardous technological processes are associated with certain expenditures throughout the entire lifecycle of the system. Three main items of these expenditures are procurement, operation and risk costs. The notations that will be used further for estimating these costs are given in Table 7.

The present value of the lifecycle cost is shown in (28). The procurement cost (29) includes start-up expenses associated with the project initiation and engineering design, i.e. preparing the documentation, construction work, software development, commissioning, etc., and the cost of purchasing the equipment.

The cost of operations is calculated for every year in (30). Here, the first term corresponds to yearly electricity consumption by the chosen devices. The second and the third terms describe the costs and losses associated with proof testing for the chosen maintenance frequency. The fourth term corresponds to production losses and spare parts replenishment due to dangerous failures. The last term corresponds to the yearly cost of facility maintenance. The cost of spare parts replenishment for each subsystem is set as a certain percentage of the corresponding procurement cost (31). The dangerous detected failure rate for the considered ESD system configuration is obtained in 32) from the model in the previous subsection (states 6–8 of the lifecycle Markov model) and the assumption of an exponential distribution of failures. Equations (33) show the impact of introducing electrical separation on the solution cost by choosing corresponding values of the cost modifiers for each subsystem.

Table 7
Notations used for lifecycle modelling from the economic perspective.

Notation	Description
q	index of subsystems
τ	time, [y]
LC_y	lifecycle, [y]
$\mathrm{C}_{\mathrm{lifecycle}}$	lifecycle cost [currency units (CU)]
$\mathrm{C}^{\mathrm{proc}}$	procurement cost [CU]
$\mathrm{C}_{\tau}^{\mathrm{oper}}$	the yearly operation cost [CU]
$\mathrm{C}_{\tau}^{\mathrm{risk}}$	the yearly risk cost [CU]
$\mathrm{C}^{\mathrm{design}}$	the design cost [CU]
$\mathrm{C}_{lq}^{\mathrm{purch}}$	the cost of purchasing one device chosen for subsystem q [CU]
$\mathrm{C}_{lq}^{\mathrm{cons}}$	yearly electricity consumption by one device in subsystem q [CU]
$\mathrm{C}_{lq}^{\mathrm{test}}$	the cost of conducting one proof test for one component of subsystem q [CU]
C^{PL}	hourly losses of production [CU/h]
$\mathrm{C}_{lq}^{\mathrm{rep}}$	the cost of repairing one component of subsystem q [CU]
$\mathrm{C}_{q}^{\mathrm{SP}}$	the cost of spare parts replenishment for subsystem q [CU]
C^{FM}	the yearly cost of facility maintenance [CU]
$\mathrm{C}^{\mathrm{inc}}$	the cost of an incident and hazardous consequences [CU]
β^{purch}	purchase cost modifier corresponding to the chosen circuitry configuration
β^{design}	design cost modifier corresponding to the chosen circuitry configuration
β^{cons}	consumption cost modifier corresponding to the chosen circuitry configuration
σ	spare part cost fraction
T_{SU}	start-up time after the shutdown necessary for maintenance before the facility can be restarted, [h]
DDR_y	dangerous detected failure rate for the given ESD, [y^{-1}]
STR_y	spurious tripping rate for the given ESD, [y^{-1}]

$$\begin{gathered}\mathrm{C}_{\mathrm{lifecycle}} = \mathrm{C}^{\mathrm{proc}} + \sum_{\tau=1}^{\mathrm{LC}_y} \left(\mathrm{C}_{\tau}^{\mathrm{oper}} + \mathrm{C}_{\tau}^{\mathrm{risk}}\right) \\ \cdot \frac{1}{(1+\delta)^{\tau-1}},\end{gathered} \tag{28}$$

$$\begin{gathered}\mathrm{C}^{\mathrm{proc}} = \mathrm{C}^{\mathrm{design}} \cdot \beta^{\mathrm{design}} + \sum_{q} \sum_{l\in S_q^{\mathrm{inst}}} \\ \sum_{r\in S_q^{\mathrm{red}}} \mathrm{C}_{lq}^{\mathrm{purch}} \cdot x_{lq}^{\mathrm{inst}} \cdot \beta^{\mathrm{purch}} \cdot N_{rq} \cdot x_{rq}^{\mathrm{red}},\end{gathered} \tag{29}$$

$$\begin{gathered}\mathrm{C}_{\tau}^{\mathrm{oper}} = \sum_{q} \sum_{l\in S_q^{\mathrm{inst}}} \sum_{r\in S_q^{\mathrm{red}}} \mathrm{C}_{lq}^{\mathrm{cons}} \cdot x_{lq}^{\mathrm{inst}} \\ \cdot \beta^{\mathrm{cons}} \cdot N_{rq} \cdot x_{rq}^{\mathrm{red}} + \frac{365 \cdot 24}{\mathrm{TI}} \\ \cdot \sum_{q} \sum_{l\in S_q^{\mathrm{inst}}} \sum_{r\in S_q^{\mathrm{red}}} \mathrm{C}_{lq}^{\mathrm{test}} \cdot x_{lq}^{\mathrm{inst}} \cdot N_{rq} \cdot x_{rq}^{\mathrm{red}} \\ + \frac{365 \cdot 24}{\mathrm{TI}} \cdot \mathrm{C}^{\mathrm{PL}} \cdot T^{\mathrm{SU}} \\ + \left(\mathrm{C}^{\mathrm{PL}} \cdot T^{\mathrm{SU}} + \sum_{q} \sum_{l\in S_q^{\mathrm{inst}}} \sum_{r\in S_q^{\mathrm{red}}} \mathrm{C}_{lq}^{\mathrm{rep}} \cdot x_{lq}^{\mathrm{inst}}\right. \\ \left. \cdot N_{rq} \cdot x_{rq}^{\mathrm{red}} + \sum_{q} \mathrm{C}_{q}^{\mathrm{SP}}\right) \cdot \mathrm{DDR}_y + \mathrm{C}^{\mathrm{FM}},\end{gathered} \tag{30}$$

$$\begin{gathered}\mathrm{C}_{q}^{\mathrm{SP}} = \sigma \cdot \sum_{q} \sum_{l\in S_q^{\mathrm{inst}}} \sum_{r\in S_q^{\mathrm{red}}} \mathrm{C}_{lq}^{\mathrm{purch}} \\ \cdot x_{lq}^{\mathrm{inst}} \cdot \beta^{\mathrm{purch}} \cdot N_{rq} \cdot x_{rq}^{\mathrm{red}},\end{gathered} \tag{31}$$

$$\begin{gathered}\mathrm{DDR}_y = -365 \cdot 24 \\ \cdot \frac{\log\left(1 - \sum\limits_{j=6}^{8} p_j \left(LC_h\right)\Big|_{X^{\mathrm{inst}},X^{\mathrm{red}},X^{\mathrm{sep}},\mathrm{TI}}\right)}{LC_h},\end{gathered} \tag{32}$$

$$\begin{gathered}\beta^{\mathrm{design}} = \beta_1^{\mathrm{design}} \cdot x_q^{\mathrm{sep}} + \beta_2^{\mathrm{design}} \cdot \left(1 - x_q^{\mathrm{sep}}\right), \\ \beta^{\mathrm{purch}} = \beta_1^{\mathrm{purch}} \cdot x_q^{\mathrm{sep}} + \beta_2^{\mathrm{purch}} \cdot \left(1 - x_q^{\mathrm{sep}}\right) \quad \forall q, \\ \beta^{\mathrm{cons}} = \beta_1^{\mathrm{cons}} \cdot x_q^{\mathrm{sep}} + \beta_2^{\mathrm{cons}} \cdot \left(1 - x_q^{\mathrm{sep}}\right),\end{gathered} \tag{33}$$

$$\begin{gathered}\mathrm{C}_{\tau}^{\mathrm{risk}} = \left(\mathrm{C}^{\mathrm{PL}} \cdot T^{\mathrm{SU}} + \sum_{q} \sum_{l\in S_q^{\mathrm{inst}}} \sum_{r\in S_q^{\mathrm{red}}} \mathrm{C}_{lq}^{rep}\right. \\ \left. \cdot x_{lq}^{\mathrm{inst}} \cdot N_{rq} \cdot x_{rq}^{\mathrm{red}}\right) \cdot STR_y + \mathrm{C}^{\mathrm{inc}} \cdot r \cdot \mathrm{PFD}_{\mathrm{avg}}\end{gathered} \tag{34}$$

$$\begin{gathered}\mathrm{STR}_y = -365 \cdot 24 \\ \cdot \frac{\log\left(1 - \sum\limits_{j=3}^{5} p_j \left(LC_h\right)\Big|_{X^{\mathrm{inst}},X^{\mathrm{red}},X^{\mathrm{sep}},\mathrm{TI}}\right)}{LC_h}.\end{gathered} \tag{35}$$

Risk cost calculated for every year outlines the negative impact of the deployed SIS. It includes the losses of production and the costs of overhaul initiated by spurious trips as well as estimated losses due to the potential dangerous consequences in the event of a hazard, calculated for a particular ESD design as shown in (34). Spurious tripping rate (35) of the process is obtained from the states 3–5 of the Markov model in the previous subsection.

Multi-objective optimization

The mathematical models presented in the preceding subsections of this paper allow assessing the safety and economic characteristics of a particular SIS configuration. Mathematical and programming capabilities of Mathworks Matlab software were employed to run the presented models. Markov analysis of system safety and the lifecycle cost evaluation were implemented in the form of Matlab script functions. The inputs of the functions are the design variables representing a particular SIS configuration and the time interval for the planned maintenance (2). The outputs of the programmed functions provide the values of the three mentioned indicators. Thus, the scripts represent the objectives for the multi-criteria optimization problem, i.e. the functions manifested in (1).

To make the presented SIS design optimization problem (1)–(6) tractable, a black box optimization algorithm needs to be employed. Matlab's optimization toolbox provides gamultobj solver, which implements the multi-objective controlled elitist genetic algorithm (a variant of NSGA-II). For the details of the applied heuristic algorithm, Mathworks refers the users to [21].

Computational experiment

Case data

The suggested methodology is applied to a case provided by a Russian company: an oil terminal with a storage tank.

The storage facility is used for temporary storage of crude and substandard oil and for the duration of several days in case the throughput of the oil processing facility is exceeded, or in the case of an emergency at the facility.

The critical situations that can quickly escalate into hazards were identified, and the measures for the shutdown were developed (Table 8).

The Markov model for the lifecycle has been adapted for this example following the logic in Fig. 1d. The ESD corresponding to the description in Table 8 will consist of 6 subsystems linked in series. The modified lifecycle safety model has 21 states. The optimization model has 54 binary design decision variables and 1 integer decision variable.

The following settings for multi-objective genetic algorithm were applied: population size: 300; initial population created with the uniform distribution applying a customized population creating function adapted for integer variables; selection function: tournament; generational gap: 0.8 (or 80%); crossover and mutation functions: custom functions for integer values of decision variables.

The optimization problem was first solved with the target SIL constraints (3) and (4) dropped from the formulation, i.e. only the three objective function values (average probability of failure on demand, facility downtime, and lifecycle cost) were desired to be minimized with only logical constraints (5) and (6) applied. The obtained 105 solutions, Pareto solutions are demonstrated in Fig. 5. Afterwards, the constraints (3) and (4) defined by the standards (Table 1) specifying the target SIL 3 were enforced, which resulted in 9 solutions demonstrated in Table 10.

Discussion of the results

Several observations can be made from the Pareto-front plots with the pairs of the objectives, demonstrated in Fig. 5:

- PFD_{avg} and DT do not demonstrate conflicting behaviour. This is reasonable because the failures of the devices and the subsystems directly contribute to both indicators.
- The reliability indicators prove to be conflicting with lifecycle cost (PFD_{avg} vs. $C_{lifecycle}$, and DT vs. $C_{lifecycle}$), which consistent with the SIS design problem pursuing the trade-off between the safety and the cost of the solution.

Table 8
Shutdown procedure description.

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

Table 9
Equipment database and process parameters.

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, $\times 10^{-6}$ $[\mathrm{h}^{-1}]$																
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]	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/h]	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	

Common cause failure				
CCF factor for all subsystems		Cost modifier	Baseline solution	Electrical separation
Baseline solution (standard circuits)	0.035	Purchase cost	1	1,35
		Design cost	1	1,1
Additional electrical separation	0.02	Consumption cost	1	1,35

Other parameters	
Subsystem repair rate: $\mu = 0.125$ $[\mathrm{h}^{-1}]$	Cost of hazard: 500 000 [CU]
Facility restoration rate: $\mu^t = 0.0625$ $[\mathrm{h}^{-1}]$	Start-up cost: 500 000 [CU]
Lifecycle: $\mathrm{LC}_y = 15$ [y]	Production loss: 500 000 [CU/h]
TI is chosen from a set of values from 1 month to 24 months with a 1 month step	Discount rate: $\delta = 5\%$

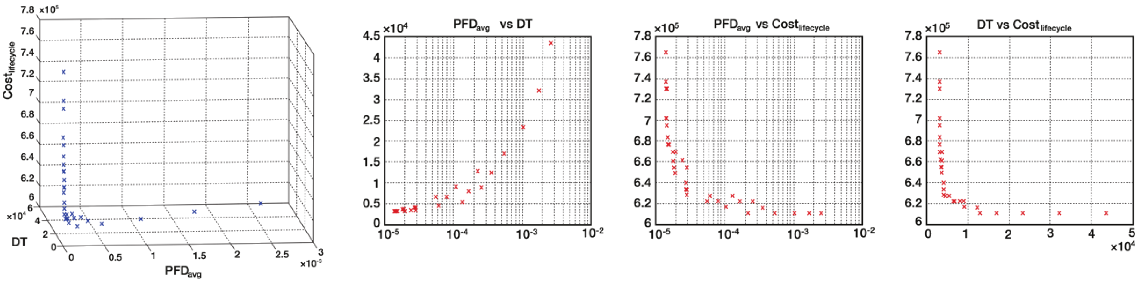

Fig. 5. Results of ESD system design optimization. Pareto front and its pairwise display with respect to the objectives.

Table 10
Optimization results. Problem solutions 1–9 achieved SIL 3, PS – project solution, implemented by the company
Here, "b" stands for baseline solution, whereas "e" stands for additional electrical separation.

#	Specification							Modelling results		
	Level transmitter	Fire detector	PLC	Safety valve 1	Safety valve 2	Pump drive	TI [month]	$\mathrm{PFD}_{\mathrm{avg}}$ $\times 10^{-5}$	DT [h]	$\mathrm{C}_{\mathrm{lifecycle}}$ $\times 10^5$ [CU]
1	LT4/1oo2/e	FD2/2oo8/e	PLC2/1oo2/e	SV2/1oo3/e	SV2/1oo3/e	PD2/1oo3/b	2	1.4136	320	6.9517
2	LT4/1oo2/b	FD2/2oo8/e	PLC2/1oo2/e	SV2/1oo3/e	SV2/1oo3/e	PD1/1oo2/e	1	1.7773	369	6.6075
3	LT4/1oo2/e	FD2/2oo8/e	PLC3/1oo2/e	SV2/1oo3/e	SV2/1oo3/e	PD2/1oo3/e	2	1.4895	323	6.7679
4	LT4/1oo2/e	FD2/2oo8/e	PLC3/1oo2/e	SV2/1oo3/e	SV2/1oo3/e	PD2/1oo2/e	2	1.9521	329	6.6943
5	LT5/1oo3/e	FD2/2oo8/e	PLC2/1oo3/e	SV2/1oo3/e	SV2/1oo4/e	PD2/1oo3/b	2	1.3974	320	7.3049
6	LT5/1oo3/e	FD2/2oo8/e	PLC3/1oo2/e	SV2/1oo3/e	SV2/1oo4/e	PD2/1oo3/e	2	1.4734	323	6.8414
7	LT5/1oo3/b	FD2/2oo8/e	PLC2/1oo2/e	SV2/1oo3/e	SV2/1oo4/e	PD2/1oo3/e	2	1.3975	320	7.0253
8	LT5/1oo3/e	FD2/2oo8/e	PLC3/1oo2/e	SV2/1oo4/e	SV2/1oo3/e	PD2/1oo3/b	2	1.4734	323	6.8414
9	LT5/1oo3/e	FD2/2oo8/e	PLC3/1oo3/e	SV2/1oo3/e	SV2/1oo4/e	PD2/1oo3/e	2	1.3976	320	7.3049
PS	LT1/1oo3/e	FD2/2oo4/e	PLC2/1oo3/e	SV3/1oo3/e	SV3/1oo4/e	PD1/1oo3/e	3	9.2834	445	7.1463

- In the middle of the pairwise representations of the Pareto-front (approximately at the range $\mathrm{PFD}_{\mathrm{avg}} < 2 \cdot 10^{-4}$) the relations between the pairs of objectives become to some extent erratic. This could be explained by addressing the nature of the failure modes considered by the safety indicators. $\mathrm{PFD}_{\mathrm{avg}}$ encompasses only the dangerous failures, while DT is attributed to both dangerous and safe failures. Since the reliability characteristics of the device options that the companies use do not change monotonically from one device to another, the roles of the two failure modes change when different device options are considered. This leads to the abrupt growth of spurious trips contribution to certain SIS design solutions.

The acquired optimization results may be of use for laying out certain preferences on the early stages of the project by formulating certain requirements to the SIS specification that are followed further during the detailed design of the ESD system for the given project. Below, several observations that can assist in formulating the requirements are presented while analysing the results in Table 10:

- For the given problem setting, the optimization algorithm mostly prefers the field devices (sensors and actuators) with better reliability characteristics despite potentially higher purchase costs.
- Adding electrical separation to the circuit configuration for mitigating the common cause failure possibility is also preferred over the alternative.
- For the subsystem of level transmitters, the devices supplied by vendor V3 are preferred; however, the architecture 1oo2 is chosen for one device model (LT4) of the sensor offered by the vendor, and 1oo3 – for the other model (LT5).
- For the subsystem of fire detectors, the highest redundancy architecture (2oo8) is preferred. This can be attributed to the low cost of the fire detectors in comparison to the devices in other subsystems. Among the alternatives, one particular model FD2 offered by V4 is preferred.
- For the subsystem of logic solvers, the algorithm suggests the controllers manufactured by V1 and V3, and the redundancy options 1oo2 and 1oo3. No obvious correlations between the preferred device models and architectures are revealed, and so the particular configuration choices for this subsystem during the detailed design phase must be accompanied with careful substantiations.
- For the subsystems of final control elements, two types of redundancy architectures are generally preferred: 1oo3 and 1oo4. The device models selected by the optimization algorithm are SV2 for the two subsystems of safety valves and PD2 for the pumps. The chosen device models are supplied by V1.
- The last row in Table 10 represents the decisions made in the actual project, whose data was analysed for the computational example in this research. The solution, developed by the engineering contractor corresponds to SIL 3 by both risk reduction and fault tolerance requirements. However, one can observe that seven solutions of the optimization algorithm dominate the chosen project solution.

Conclusions

This research addressed the problem of safety instrumented system design in the context of the engineering project stages. The presented multi-objective optimization of the system design and maintenance frequency addressed both safety and economic indicators of the safety system performance. The problem aimed at reflecting the perspectives of the three main parties involved in petroleum sector projects, namely E&P operator, engineering design contractor, and government with its regulations on safety.

Modelling and design have been conducted for the example of emergency shutdown systems. The Markov analysis was applied for quantification of safety indicators of a particular alternative of the system configuration. The employed Markov model addressed the occurrence of the following events: device failures and repairs, technological incidents and restorations, and periodic system maintenance.

The proposed modelling and design approach is relevant for the planning and design stage of petroleum facilities infrastructure when the requirements specification for the safety system is developed. The suggested model can facilitate the E&P companies with formulating straightforward requirements for the safety system. The analysis of the computational experiment outcome reveals that the proposed design optimization approach can suggest advisable redundancy schemes for the subsystems and to narrow down the vendors for the necessary system components. The application of the proposed model is not limited to only formulating the requirements. It can also be applied as a starting point for detailed engineering design or for the purposes of research for reasonable engineering solutions.

The limitations of the presented research are recognized by the author. One of the directions of elaborating the proposed models is to incorporate the diverse redundancy, i.e. allowing different device models to be included in one subsystem. Another direction of improving the models is a detailed consideration of proof testing. In practical instances, the proof tests are not perfect, and moreover, they can become the cause of failure occurrence. Additionally, different testing policies, i.e. parallel, sequential, and other proof testing schemes, can be introduced. Such modelling could be used for strategic and tactical maintenance planning decisions, e.g., establishing the staffing size and determining the crew schedules.

This could be a research direction especially relevant for the companies operating in remote regions, where the personnel usually work shifts. The transportation costs will play a considerable role in the design decisions since it could be expensive to transport the crews to the remotely located facilities for the purpose of conducting the testing procedures in order to ensure the correct work of the facility.

7th International Conference on Engineering, Project, and Production Management (EPPM2016) was co-organised by the Agency for Restructuring and Modernisation of Agriculture (Poland).

References

[1] International Electrotechnical Commission (IEC), *61511 Functional safety – safety instrumented system for the process industry sector*, IEC, Geneva, Switzerland, 2003.

[2] Boudreaux M., *Safety Lifecycle Seminar*, Emerson Global Users Exchange – Annual Technical Conference, 27 September – 1 October, 2010, San Antonio, Texas, USA.

[3] CCPS (Centre for Chemical Process Safety), *Guidelines for Safe Process Operations and Maintenance*, John Wiley & Sons, New York, 2010.

[4] HSE (Health and Safety Executive), *Out of Control*, 2nd ĺd., HSE Books, UK, 2003.

[5] International Electrotechnical Commission (IEC), *61508 Functional safety of electrical/electronic/programmable electronic safety-related systems*, IEC, Geneva, Switzerland, 1997.

[6] Bukowski J., *Using Markov models to compute probability of failed dangerous when repair times are not exponentially distributed*, in RAMS'06 Annual Reliability and Maintainability Symposium, IEEE, 273–277, 2006.

[7] Mechri W., Simon C., Ben Othman K., *Switching Markov chains for a holistic modeling of SIS unavailability*, Reliability Engineering & System Safety, 133, 212–222, 2015.

[8] Hauge S., Lundteigen M.A., Hokstad P., Håbrekke S., *Reliability prediction method for safety instrumented systems. PDS method handbook*, 2010 edition, SINTEF, Trondheim, 2010.

[9] Andrews J.D., Ericson C.A., *Fault tree and Markov analysis applied to various design complexities*, 18th International System Safety Conference (ISSC), 2000.

[10] Goble W.M., *Control Systems Safety Evaluation & Reliability*, 3rd ed., Research Triangle Park: ISA, 2010.

[11] Hellmich M., Berg H.P., *Markov analysis of redundant standby safety systems under periodic surveillance testing*, Reliability Engineering & System Safety, 133, 48–58, 2015.

[12] Torres-Echeverria A.C., Martorell S., Thompson H.A., *Modelling and optimization of proof testing policies for safety instrumented systems*, Reliability Engineering & System Safety, 94, 838–854, 2009.

[13] Kuo W., *Optimal Reliability Design: Fundamentals and Applications*, Cambridge University Press, Cambridge, 2001.

[14] Kuo W., Zuo M.J., *Optimal reliability modeling. Principles and applications*, John Wiley & Sons, Hoboken, New Jersey, 2003.

[15] Martorell S., Sánchez A., Carlos S., and Serradell V., *Alternatives and challenges in optimizing industrial safety using genetic algorithms*, Reliability Engineering & System Safety, 86, 1, 25–38, 2004.

[16] Torres-Echeverria A.C., *Modelling and optimization of safety instrumented systems based on dependability and cost measures*, PhD thesis, University of Sheffield, 2009.

[17] Bukowski J., *Incorporating process demand into models for assessment of safety system performance*, RAMS'06 Annual Reliability and Maintainability Symposium, IEEE, 577–581, 2006.

[18] Shershukova K.P., *Modelling Safety System Integrated into PCS of Gas Condensate Processing*, [in Russian: *Modelirovanie sistemy bezopasnosti v sostave ASU TP pererabotki gazokondensata*], Dissertation abstract, Moscow, 2013.

[19] The Norwegian Oil and Gas Association, *070 – Application of IEC61508 and IEC61511 in the Norwegian Petroleum Industry*, Norwegian Oil and Gas, Sandnes, 2001.

[20] Closed Joint-Stock Company Scientific technical center of industrial safety problems research, *Federal law On industrial safety of hazardous production facilities*, STC Industrial safety CJSC, Moscow, 2014.

[21] Deb K., *Multi-Objective Optimization using Evolutionary Algorithms*, John Wiley & Sons, Chichester, 2001.