Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 182 (2017) 611 – 618

Procedia Engineering

www.elsevier.com/locate/procedia

7th International Conference on Engineering, Project, and Production Management

Modelling and Design of Safety Instrumented Systems for Upstream Processes of Petroleum Sector

Yury Redutskiy*

Molde University College, P.O. Box 2110, NO-6402 Molde, Norway

Abstract

The adequacy of the decision-making regarding the specification of Safety Instrumented Systems (SIS) deployed for hazardous processes, contributes to avoiding incidents and corresponding losses. This paper proposes an approach to mathematically and economically substantiated design of SIS. Markov analysis is used for the stochastic process of SIS failures and technological incidents occurrence. The model is used further for multi-objective optimization of SIS design. The research is relevant to engineering departments and contractors, who specialise in planning and designing the technological solution.

Peer-review under responsibility of the organizing committee of EPPM2016

Keywords: emergency shutdown system; Markov process; multi-objective optimization; risk management; safety instrumented system

1. Introduction

The operations of hydrocarbons extraction from the deposits are associated with large expenditures and risks. Technology of upstream processes is carried out on hazardous industrial facilities, where occurrence of an incident may lead to significant economic losses, harm to personnel, environmental damage, etc. Petroleum production facilities and units function according to their design. Establishing petroleum production infrastructure and starting the operations is carried out as 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. Further further work is usually assigned to contractors, after the requirements specification is prepared. Those requirements are sought to be followed on the stage of a detailed engineering design, when a particular technological solution is developed. Later the facilities are commissioned and prepared for the operations. In 2003, British agency HSE conducted a careful analysis of a sample of incidents in petroleum industry. It revealed that in almost half of the cases the cause of hazards lies in the inadequacy of specification, leading to the safety-related control systems being designed inappropriately[5].

The IEC 61511 standard [6] introduces the term safety instrumented system (SIS) and defines it through its structure (see Fig. 1a), and its intended safety functions, e.g., protection of facility personnel, assets, etc. Several SIS are usually put in place, however the most significant risk reduction is ensured by the emergency shutdown (ESD) system, which

* Corresponding author. Tel.: +4-771-195-794 ; fax: +4-771-214-100.
E-mail address: Yury.Redutskiy@HiMolde.no

Peer-review under responsibility of the organizing committee of EPPM2016
doi:10.1016/j.proeng.2017.03.165

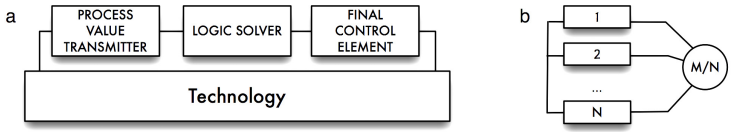

Fig. 1. (a) One control loop of SIS, based on [6]; (b) Structure of a subsystem, based on [6].

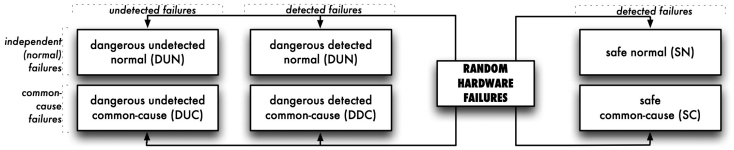

Fig. 2. Classification of failures, used in this work.

responds to critical situations that can quickly escalate to hazards [2]. Insufficient specificity of requirements to ESD formulated while planning the infrastructure, often results in development of a solution, that marginally achieves the required level of safety. A detailed analysis would reveal that among the alternatives of equipment the engineering contractor works with, there are far better options, then companies often choose. The objective of this work is to address the problem of optimising the ESD system design for the purpose of formulating straightforward requirements.

An extensive research in the area of modelling and optimizing SIS has already been conducted. Modelling the systems is based primarily on reliability theory. A very comprehensive overview of the applied techniques can be found in Goble et al.[3]. The problem of SIS design falls into the category of Reliability and Redundancy allocation. An interested reader can find a detailed overview of such problems in a book by Kuo [9]. The source also provides the insight into algorithmic perspective for the problems. The author points out that classical discrete optimization methods have rather limited application to complex real-life instances, and thus, the metaheuristic algorithms are often applied. It is worth noting that many researchers, suggest multi-objective optimization of SIS design, e.g., address Torres-Echeverria [13]. The majority of researchers dealing with SIS design, e.g., see Mechri et al. [11] and Torres-Echeverria [13], focus entirely on SIS performance, which resulted in the lack of technological incidents representation. A few works, e.g., Bukowski [1], Jin et al. [7] and Shershukova [12], attempt to incorporate incidents occurrence into Markov models. However, in most cases the authors stick to aggregated models, where the multiple modes of ESD system failure are represented with generalised states of the model.

2. The problem of ESD system design

2.1. Problem description

Markov analysis will be applied further for modelling the safety characteristics of the process of failures and incidents occurrence. The approach to modelling is largely based on the ideas presented in works [7] and [12], meanwhile the necessary adaptations to the specifics of this work are made.

It is common to represent a structural unit of any SIS by a control loop, as shown in Fig. 1a. Process value *transmitters* are sensors monitoring the technological parameters. *Logic solver* is a programmable logic controller (PLC), which receives the data from transmitters, and generates an output control signal to actuators, or *final control elements*, which directly affect the process by opening/closing valves, starting/stopping pumps, compressors, etc. Each subsystem is represented by its a MooN redundancy scheme (see, Fig. 1b), with N identical components, M of which need to be in operating condition for the subsystem's function to be performed.

The random hardware failures of components in the subsystems of ESD can be either dangerous or safe. The former ones lead to hazards and contribute to the *probability of failure on demand* (PFD) safety indicator. The latter contribute to the *spurious tripping rate* (STR) indicator. Each device is assumed to reveal a certain share of dangerous failures by the means of self-diagnostics. This share is represented by diagnostic coverage ϵ. Additionally, we will address situations, when all components in a subsystem fail simultaneously due to a common cause. A share of common cause failures (CCF) would be referred to as β. A detailed classification of failures and mechanisms of their occurrence is given in Hauge et al.[4]. The classification used here, is summarised in Fig. 2. The maintenance of

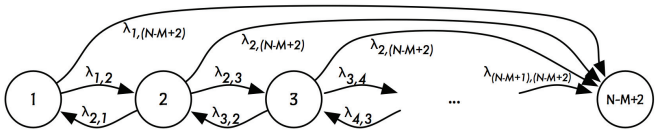

Fig. 3. Markov model of failure occurrence in a subsystem with MooN architecture.

equipment is executed in two forms: continuously during the course of the process, when failures are revealed by self-diagnostics, and periodically in a form of proof tests conducted with an period referred to as "test interval" (TI).

Mathematical modelling of failures and incidents occurrence, as well as restoration processes taking place, is considered further. The following assumptions are made:

- only random hardware failures are considered, failure classification presented in Fig. 2 is used; with this approach, we assume that all safe failures are detected
- failure occurrence is described by the exponential distribution, which corresponds to constant failure rate; this is a valid assumption for complex systems with electronic components [3]
- periodically conducted proof tests are considered perfect, i.e. all undetectably failed devices are restored.

2.2. Modelling a subsystem

The dangerous and safe failures of components of any subsystem are modelled for the time interval between two consecutive proof tests, which can be referred to as $\left[0, TI\right]$. Markov processes describing the failures in a subsystem with MooN architecture includes $(N - M + 2)$ states (see, Fig. 3). 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 when $(N - M + 1)$ components fail, which corresponds to the last state on the graph. Occurrence of independent failures and repairs is depicted by consecutive transitions between the states. Common cause failure occurrence is depicted by direct transitions from any state to the last state.

Table 1. Notations used in modelling a subsystem.

i, j	indices of states for Markov models	β	common cause failure factor
TI	test interval, time period between proof tests, [h]	ϵ	diagnostic coverage
N	total number of components in MooN redundancy scheme	λ	dangerous failure rate for one component, [h^{-1}]
M	necessary number of operating devices in MooN scheme	λ^S	spurious trip rate for one component, [h^{-1}]
$p_j^{DU}(t)$	probability of $(j-1)$ dangerous undetected failures	$\lambda_{i,j}^{DU}(t)$	transition rates for the model of dangerous undetected failures
$p_j^{DD}(t)$	probability of $(j-1)$ dangerous detected failures	$\lambda_{i,j}^{DD}(t)$	transition rates for the model of dangerous detected failures
$p_j^{ST}(t)$	probability of $(j-1)$ spurious trips in a subsystem	$\lambda_{i,j}^{ST}(t)$	transition rates for the model of spurious trips
λ^{DU}	dangerous undetected failure rate for a subsystem	μ	repair rate
λ^{DD}	dangerous detected failure rate for a subsystem	f	superscript used as a generalization of failure modes,
λ^{ST}	spurious tripping rate for a subsystem		i.e. f stands for DU, DD and ST

A set of ordinary differential equations (1), known as Kolmogorov forward equations, describes the transitions presented on the graph. An interested reader can refer to [10] for theoretic insight into Markov analysis in reliability.

The notations used for the modelling are provided in Table 1. The non-zero elements of transition rate matrices are defined further. For the dangerous undetected failures, those rates are given in (2), for the dangerous detected rates - in (3), and for the spurious trips - in (4). The process begins in state 1, which corresponds to the initial probability distribution for every failure mode model given in (5). Finally, the result of Markov analysis is used in (6) for defining the dangerous undetected, dangerous detected and safe failure rates for the entire subsystem.

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

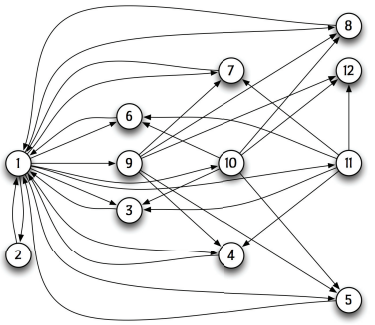

Fig. 4. Markov model of the lifecycle

Table 2. States of the Markov model. Here, the following notations are used: T - subsystem of transmitters, LS - logic solvers, FCE - final control elements, Tech - technology

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

$$\lambda_{i,i}^{DU} = -\lambda \cdot \left(1-\epsilon\right) \cdot \left[\left(N-i+1\right) \cdot \left(1-\beta\right) + \beta\right], \quad \lambda_{i,i+1}^{DU} = \left(N-i+1\right) \cdot \left(1-\epsilon\right) \cdot \left(1-\beta\right) \cdot \lambda,$$
$$\lambda_{i,(N-M+2)}^{DU} = \left(1-\epsilon\right) \cdot \beta \cdot \lambda, \quad i \in \left\{1, \cdots, (N-M+2)\right\} \tag{2}$$

$$\lambda_{1,1}^{DD} = -\epsilon \cdot \lambda \cdot \left[N \cdot \left(1-\beta\right) - \beta\right], \quad \lambda_{1,2}^{DD} = N \cdot \epsilon \cdot \left(1-\beta\right) \cdot \lambda, \quad \lambda_{1,(N-M+2)}^{DD} = \epsilon \cdot \beta \cdot \lambda,$$
$$\lambda_{i,i-1}^{DD} = \left(i-1\right) \cdot \mu, \quad \lambda_{i,i}^{DD} = -\epsilon \cdot \lambda \cdot \left[\left(N-i+1\right) \cdot \left(1-\beta\right) + \beta\right] - \left(i-1\right) \cdot \mu, \tag{3}$$
$$\lambda_{i,i+1}^{DD} = \left(N-i+1\right) \cdot \epsilon \cdot \left(1-\beta\right) \cdot \lambda, \quad \lambda_{i,(N-M+2)}^{DD} = \epsilon \cdot \beta \cdot \lambda, \quad i \in \left\{2, \cdots, (N-M+2)\right\}$$

$$\lambda_{1,1}^{ST} = -\lambda^{S} \cdot \left[N \cdot \left(1-\beta\right) - \beta\right], \quad \lambda_{1,2}^{ST} = N \cdot \left(1-\beta\right) \cdot \lambda^{S}, \quad \lambda_{1,(N-M+2)}^{ST} = \beta \cdot \lambda,$$
$$\lambda_{i,i-1}^{ST} = \left(i-1\right) \cdot \mu, \quad \lambda_{i,i}^{ST} = -\lambda^{S} \cdot \left[\left(N-i+1\right) \cdot \left(1-\beta\right) + \beta\right] - \left(i-1\right) \cdot \mu, \tag{4}$$
$$\lambda_{i,i+1}^{ST} = \left(N-i+1\right) \cdot \left(1-\beta\right) \cdot \lambda^{S}, \quad \lambda_{i,(N-M+2)}^{ST} = \beta \cdot \lambda^{S}, \quad i \in \left\{2, \cdots, (N-M+2)\right\}$$

$$p_1^{DU}\left(0\right) = 1,\ p_i^{DU}\left(0\right) = 0;\ \ p_1^{DD}\left(0\right) = 1,\ p_i^{DD}\left(0\right) = 0;\ \ p_1^{ST}\left(0\right) = 1,\ p_i^{ST}\left(0\right) = 0;\ i \in \left\{2, \cdots, (N-M+2)\right\} \tag{5}$$

$$\lambda^{DU} = -\frac{log\left(1-p_{N-M+2}^{DU}(TI)\right)}{TI}, \quad \lambda^{DD} = -\frac{log\left(1-p_{N-M+2}^{DD}(TI)\right)}{TI}, \quad \lambda^{ST} = -\frac{log\left(1-p_{N-M+2}^{ST}(TI)\right)}{TI} \tag{6}$$

2.3. Modelling the lifecycle of technological unit functioning with ESD system

Failures of ESD system and technological incidents are described with the states of the stochastic process in Table 2. The transitions between the states are represented with the graph in Fig. 4. Modelling of the incidents, failures and repairs is conducted during the entire lifecycle of the technological unit with the deployed safety system. The lifecycle is divided into K periods (7).

During each k^{th} period the probability of the process being in each j^{th} state is described by equations (8). The non-zero transition rates λ_{ij} are given in (9). The initial distribution of probabilities for every period k is denoted by π_j^k. For the beginning of the lifecycle, the process is in state 1, for the following periods, initial distribution is defined in (10) under the assumption of the perfect proof tests.

$$LC_h : \left[0, TI\right), \quad \left[TI, 2 \cdot TI\right), \quad \cdots \quad \left[(k-1) \cdot TI, k \cdot TI\right), \quad \cdots \quad \left[(K-1) \cdot TI, K \cdot TI\right]; \qquad K = \frac{LC_h}{TI} \tag{7}$$

$$\frac{dp_j(t)}{dt} = \sum_{i=1}^{12} p_i(t) \cdot \lambda_{ij}, \quad j \in \left\{1, \cdots, 12\right\} \tag{8}$$

Table 3. Notations used for lifecycle modelling from the safety perspective.

i, j	indices of states for Markov models	$p_j(t)$	probability of the process being in the j^{th}ăstate
q	index of ESD subsystems, $q = 1$ corresponds to transmitters,	$\lambda_{i,j}$	transition rate from state i to j for the lifecycle model, [h^{-1}]
	$q = 2$ to logic solvers, $q = 3$ to final control elements	λ_q^{DU}	dangerous undetected failure rate for the q^{th} subsystem, [h^{-1}]
k	index of time periods between the proof tests	λ_q^{DD}	dangerous detected failure rate for the q^{th} subsystem, [h^{-1}]
K	number proof tests over the lifecycle	λ_q^{ST}	spurious tripping rate for the q^{th} subsystem, [h^{-1}]
t, τ	time, in [h] and [y] respectively	π_j^k	initial condition (probability of each j^{th} state) for k^{th} period
LC_h	duration of the lifecycle, [h]	δ	discount factor for the cost model
LC_y	duration of the lifecycle, [y] respectively	$PFD(t)$	probability of failure on demand
r	incidents occurrence rate, [h^{-1}]	PFD_{avg}	average probability of failure on demand
μ^t	restoration rate for the technology, [h^{-1}]	DT	mean down time of the process, [h]

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

$$\begin{aligned}
&\pi_1^1 = 1, \quad \pi_2^1 = 0, \quad \cdots \quad \pi_{12}^1 = 0;\\
&\pi_1^k = p_1\Big((k-1)\cdot TI\Big) + p_9\Big((k-1)\cdot TI\Big) + p_{10}\Big((k-1)\cdot TI\Big) + p_{11}\Big((k-1)\cdot TI\Big) + p_{12}\Big((k-1)\cdot TI\Big),\\
&\pi_j^k = p_j\Big((k-1)\cdot TI\Big), \quad j \in \Big\{2,3,4,5,6,7,8\Big\}; \qquad \pi_j^k = 0, \quad j \in \Big\{9,10,11,12\Big\}
\end{aligned} \tag{10}$$

As a result of modelling (7)-(10), we obtain the values of $p_1(t), ..., p_{12}(t)$ over the entire lifecycle. We use them to evaluate the safety indicators for the process (11). The average probability of failure on demand is the mean value of $p_{12}(t)$. Mean downtime is calculated based on $p_2(t)...p_8(t)$.

$$PFD_{avg} = \frac{1}{LC_h} \cdot \int_0^{LC_h} PFD(t)dt = \frac{1}{LC_h} \cdot \int_0^{LC_h} p_{12}(t)dt; \quad DT = \sum_{j=2}^{8} \int_0^{LC_h} p_j(t)dt \tag{11}$$

Additionally, the lifecycle cost of ESD functioning for a particular technology is evaluated in order to address the economic efficiency of the applied safety measures. The net present value of the total cost includes three main components: procurement, operation and risk costs (12). The reader can address [3], [13] for the details of this model.

$$Cost_{lifecycle} = Cost_{procurement} + \sum_{\tau=1}^{LC_y} \Big(Cost_{operations}^{\tau} + Cost_{risk}^{\tau}\Big) \cdot \frac{1}{(1+\delta)^{\tau-1}} \tag{12}$$

2.4. Optimization of ESD system design

The mathematical model presented in the previous section allows to evaluate the safety and economic characteristics of a particular alternative of ESD system design. The three indicators, presented in (11) and (12) are considered as *objective functions* for the ESD design optimization problem. The set of the following *decision variables* would constitute a particular specification:

- particular devices (transmitters, logic solvers, and final elements) from the databases of alternatives
- redundancy scheme (MooN) for each subsystem
- circuitry separation for each subsystem, which in terms of modelling is represented as the CCF factor

- test interval, which corresponds to the schedule of proof tests.

The problem of ESD design becomes complete, when a constraint ensuring the necessary safety requirement is introduced. The standard [6] suggests the concept of *safety integrity level* (SIL) for this purpose. Requirements to SIL are given in the form of a value range for average probability of failure on demand PFD_{avg} and in the form of architectural constraints for the subsystems (see, Table 4). The latter suggest certain levels of *fault tolerance* (for MooN, it is calculated as $M-N$) and *safe failure fraction* (the percentage of detected failures). The upstream sector in petroleum industry deals with dangerous substances, thus, most processes require the safety system ensuring SIL 3.

Table 4. IEC 61511 [6] requirements for safety integrity level and minimum fault tolerance.

	Risk reduction requirement	Fault tolerance requirement for logic solvers			Fault tolerance requirement
SIL	PFD_{avg}	with $SFF < 60\%$	with $60\% \leqslant SFF < 90\%$	with $SFF \geqslant 90\%$	for sensors and actuators
1	$(10^{-2},\ 10^{-1}]$	1	0	0	0
2	$(10^{-3},\ 10^{-2}]$	2	1	0	1
3	$(10^{-4},\ 10^{-3}]$	3	2	1	2
4	$(10^{-5},\ 10^{-4}]$		special requirements		special requirements

The multiobjective ESD design problem is solved in Matlab with the help of `gamultobj` solver, which runs the controlled elitist genetic algorithm (a variant of NSGA-II). For the details of the applied algorithm, refer to [8].

3. Computational experiment and analysis

The suggested methodology is applied to a case of an oil terminal facility with a storage tank, provided by a Russian company. The emergency situations, shutdown measures, and the necessary data are presented in Tables 5 and 6. For this example, the optimization model has 19 decision variables. The following settings for multi-objective genetic algorithm were applied: population size: 300; selection function: tournament; generational gap: 0.8; initial population creation, crossover and mutation functions were customized for integer variables. Initially, the problem was solved in the unconstrained formulation, i.e. only the three objective functions were sought to be minimised. The resulting Pareto-front of 105 solutions is demonstrated along with the initial population in the Fig. 5. Constraints, set by Table 4, ensuring SIL 3 were further applied, which resulted in 9 solutions, given in Table 6.

Table 5. Data for the model. Shutdown procedure description.

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

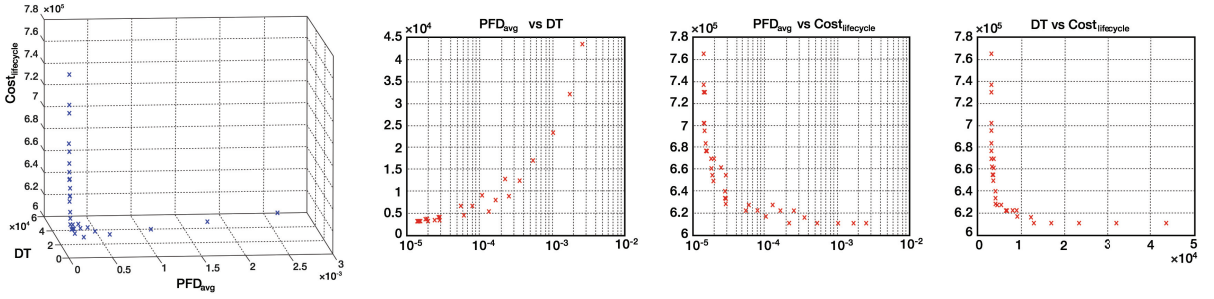

Fig. 5. Results of ESD system design optimization. Pareto front and its pairwise representation with respect to objective functions.

Table 6. Data for the model. Equipment database and process parameters.

	Level transmitter					Fire detector			Logic solver			Safety valve			Pump drive	
Alternatives	1	2	3	4	5	1	2	3	1	2	3	1	2	3	1	2
Vendors	V1	V1	V2	V3	V3	V4	V4	V5	V6	V1	V3	V7	V1	V8	V3	V1
Failure rate, [$\times 10^{-6}$ 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
Safe failures	1	4	15	1.2	3	10	4	2.28	0.8	1.1	5.5	33	33	30	13	9
Diag.coverage ϵ, [%]	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	58	85	22500	12500	7500	1300	1750	1400	750	1250
Test cost, [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 for level transmitters; 2oo2, 2oo3, 2oo4, 2oo5, 2oo6, 2oo7, 2oo8 for fire detectors;
1oo1, 1oo2, 1oo3, 1oo4, 2oo3 for PLC; 1oo1, 1oo2, 1oo3, 1oo4 for valves, and 1oo1, 1oo2, 1oo3 for pump drive.
CCF factor: for the standard circuits: $\beta = 0.035$; for electrical separation of the circuits: $\beta = 0.02$.
Repair rate for the subsystems: $\mu = 0.125$ [h^{-1}] Other parameters:
Technological incidents: $r_1 = 0.075$ [y^{-1}] and $r_2 = 0.03$ [y^{-1}] Lifecycle: 15 [y] Cost of hazard: 500,000[CU]
Facility restoration rate$\mu' = 0.0625$ [h^{-1}] Discount rate: $\delta = 0.05$ Loss of production: 5,000 [CU/h]
Interval between proof tests TI is chosen from a set of values from 1 month to 24 months with 1 month step.

From pairwise display of the Pareto-front solutions (see Fig. 5) we can draw the following conclusions on the objectives' relation to one another. DT and PFD_{avg} are not conflicting objectives. This is consistent with the fact that the device failures notably contribute to the downtime of the system. PFD_{avg} and $Cost_{lifecycle}$ demonstrate conflicting relation, and so do DT and $Cost_{lifecycle}$. The erratic relation between the pairs of objectives in the middle part of the Pareto-front can be interpreted as a changing role of spurious trips.

With regards to the requirements specification for the ESD system design, we can make several observations, while analysing Table 7. For our problem setting, the optimization algorithm generally prefers the devices with better reliability characteristics despite of potentially higher cost. Using electrical separation for reducing the CCF is also preferred. For the level transmitters, the architecture 1oo2 is chosen for one sensor model offered by vendor V3, and 1oo3 for another model from the same vendor. For the fire detectors, the architecture with the highest redundancy is always chosen. It can be attributed to the relatively low cost of the sensors. For the subsystem of logic solvers, the algorithm suggests vendors V1 and V3, and the architectures 1oo2 and 1oo3. No obvious correlation between the chosen options and architectures was revealed, so further implementation must be carefully substantiated. For the subsystems of final control elements the devices supplied by V1 are chosen with architectures 1oo3 and 1oo4.

The last line in Table 7 represents the actual choices made by the company for the project, taken here as an example. It can be observed that 7 solutions of optimization algorithm dominate the chosen project solution.

Table 7. Optimizaion results. Solutions 1-9 achieved SIL 3. PS is the project solution, implemented by the company. Here, LT - level transmitter, FD - fire detector, LS - logic solver, Val1 and Val2 - valves, "b" is baseline solution (no additional separation), and "e" - for electrical separation.

	Specification												Results			
#	Architecture						Type						TI	PFD_{avg},	DT,	C_{LC},
	LT	FD	LS	Val1	Val2	Pump	LT	FD	LS	Val1	Val2	Pump	[month]	$\times 10^{-5}$	[h]	$\times 10^5[CU]$
1	1oo2,e	2oo8,e	1oo2,e	1oo3,e	1oo3,e	1oo3,b	4	2	2	2	2	2	2	1.4136	320	6.9517
2	1oo2,b	2oo8,e	1oo2,e	1oo3,e	1oo3,e	1oo2,e	4	2	2	2	2	1	1	1.7773	369	6.6075
3	1oo2,e	2oo8,e	1oo2,e	1oo3,e	1oo3,e	1oo3,e	4	2	3	2	2	2	2	1.4895	323	6.7679
4	1oo2,e	2oo8,e	1oo2,e	1oo3,e	1oo3,e	1oo2,e	4	2	3	2	2	2	2	1.9521	329	6.6943
5	1oo3,e	2oo8,e	1oo3,e	1oo3,e	1oo4,e	1oo3,b	5	2	2	2	2	2	2	1.3974	320	7.3049
6	1oo3,e	2oo8,e	1oo2,e	1oo3,e	1oo4,e	1oo3,e	5	2	3	2	2	2	2	1.4734	323	6.8414
7	1oo3,b	2oo8,e	1oo2,e	1oo3,e	1oo4,e	1oo3,e	5	2	2	2	2	2	2	1.3975	320	7.0253
8	1oo3,e	2oo8,e	1oo2,e	1oo4,e	1oo3,e	1oo3,b	5	2	3	2	2	2	2	1.4734	323	6.8414
9	1oo3,e	2oo8,e	1oo3,e	1oo3,e	1oo4,e	1oo3,e	5	2	3	2	2	2	2	1.3976	320	7.3049
PS	1oo3,e	2oo4,e	1oo3,e	1oo3,e	1oo3,e	1oo3,e	1	3	2	3	3	1	3	9.2834	445	7.1463

4. Conclusions

This research addressed the problem of emergency shutdown system modelling with further optimization of the system design. Both safety and economic indicators were considered for the design purposes, which allowed to explore the tradeoff between the cost of safety measures and the achieved level of safety.

The application of the proposed approach is relevant for petroleum production infrastructure planning and design stage, when the requirements specification is developed. The suggested model can facilitate the E&P companies with formulating straightforward requirements for the safety system. The analysis reveals the advisable architectural decisions for the subsystems and narrows down the vendors for the necessary components. The proposed approach can also be applied as a starting point for the detailed engineering design.

The limitations of the research are recognized by the author. Incorporating the diverse redundancy (e.g., transmitters and switches, organized into a subsystem), ageing, imperfect proof testing could improve the modelling. Another suggestion for further development of the presented model is introducing different testing policies, i.e. parallel, sequential and other schemes. Such modelling could be used to determine the number of crews and their work schedules in order to ensure the correct work of the facility.

Acknowledgements

Ministry of Science and Higher Education
Republic of Poland

7th International Conference on Engineering, Project, and Production Management (EPPM2016) was financed in the framework of the contract no. 712/P-DUN/2016 by the Ministry of Science and Higher Education from the funds earmarked for the public understanding of science initiatives.

7th International Conference on Engineering, Project, and Production Management (EPPM2016) finansowana w ramach umowy 712/P-DUN/2016 ze środków Ministra Nauki i Szkolnictwa Wyższego przeznaczonych na działalność upowszechniającą naukę.

ARiMR

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] Bukowski JV. Incorporating process demand into models for assessment of safety system performance. In *RAMS'06. Annual Reliability and Maintainability Symposium, 23-26 Jan. 2006, California, USA*. IEEE; 2006, p. 577–581.
[2] CCPS (Centre for Chemical Process Safety). *Guidelines for Safe Process Operations and Maintenance.* New York: John Wiley & Sons; 2010.
[3] Goble WM. *Control Systems Safety Evaluation and Reliability. 3rd ed.* Research Triangle Park: ISA; 2010.
[4] Hauge S, Lundteigen MA, Hokstad P, Håbrekke S. *Reliability prediction method for safety instrumented systems.* Trondheim: SINTEF; 2010.
[5] HSE Books. *Out of Control. Second Edition.* UK: Health & Safety Executive; 2003.
[6] IEC 61511. *Functional safety - Safety instrumented system for the process industry sector.* Geneva, Switzerland: IEC; 2003.
[7] Jin H, Lundteigen MA, Rausand M. Reliability performance of safety instrumented systems: A common approach for both low- and high-demand mode of operation. *Reliability Engineering & System Safety*. 2011;96(3):365–373.
[8] Deb K. Multi-objective optimization using evolutionary algorithms. Chichester, UK: John Wiley & Sons; 2001.
[9] Kuo W. *Optimal reliability design: fundamentals and applications*. Cambridge, UK: Cambridge University Press; 2001.
[10] Mathew J, Shafik RA, Pradhan DK. (eds.) *Energy-efficient fault-tolerant systems*. New York, USA: Springer; 2014.
[11] Mechri W, Simon C, BenOthman K. Switching Markov chains for a holistic modeling of SIS unavailability. *Reliability Engineering & System Safety*. 2015; 133:212–222.
[12] Shershukova KP. *Modelirovanie sistemy bezopasnosti v sostave ASU TP pererabotki gazokondensata* [Modelling of the Safety System Integrated into PCS of Gas Condensate Processing]. Dissertation abstract. Moscow; 2013.
[13] Torres-Echeverria AC. *Modelling and Optimization of Safety Instrumented Systems Based on Dependability and Cost Measures.* PhD thesis. The University of Sheffield; 2009.