Safety Measures Optimization for Complex Technological System

Aleksandr Moshnikov[1][0000−0002−3689−2472]

ITMO University, 49 Kronverksky Pr., St. Petersburg, Russia
moshnikov.alex@gmail.com

Abstract. The article is devoted to the approach to the development of a process safety system according to IEC 61511 standards. With the development of technologies and increasing the specific energy stored in the equipment, the issue of safety during operation becomes more urgent 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. The classification of safety measures is given, the model of risk reduction based on deterministic analysis of the process is considered. It is shown, that the task of changing the composition of safety measures can be represented as the knapsack discrete optimization problem, solution is based on the Cross entropy Monte-Carlo method. A numerical example is provided to illustrate the approach. The considered example contains a description of failure conditions, an analysis of the types and consequences of failures that could lead to accidents, and a list of safety measures. When solving the optimization problem used real reliability parameters and cost of equipment. Based on the simulation results, the optimal composition of safety measures providing cost minimization is given. This research is relevant to engineering departments, who specialize in planning and designing the technological solution. [1]

Keywords: Safety measures · Safety instrumented system · Discrete optimization · Monte-Carlo method · System reliability.

1 Introduction

With the development of technologies and increasing the specific energy stored in the equipment, the issue of safety during operation becomes more urgent [1]. To ensure safety, emergency protection systems have been widely used. At the heart of the development of such protection systems is the international standard IEC 61511 [13], which introduces the term "Safety instrument system" (SIS) and defines it as a system consisting of sensors, logic solvers and finite element controls, together they implement one or more functions that provide

safety. Such systems may contain a set of safety features that act as layers or barriers aimed at deeply layered risk reduction

As the first level of protection, we can consider a distributed control system [2], which is designed to ensure the technology of the process and the formation of control in the normal operation of the equipment. The next barrier is the emergency shutdown system (implemented on the SIS), which brings the object to a safe controlled state. The development of the design of the SIS for industrial facilities is associated with the choice of architecture, nomenclature of components, aspects related to the discipline of service and additional measures to guarantee the development [3].

The purpose of this work is to solve the problem of optimization of the choice of a set of safety measures used in SIS, with the provision of specified safety requirements and cost [4].

A recommended way to classify barrier systems is shown in Figure 1. However, note that active barrier systems often are based on a combination of technical and human/operational elements. Even though different words are applied, the classification in the fourth level in Figure 1 is similar to the classification suggested by Hale [8]. A safety barrier is a physical and/or non-physical means planned to prevent, control, or mitigate undesired events or accidents

As regards the continuous time aspect, some barrier systems are available (functioning continuously), while some are off-line (need to be activated). Further, some barriers are permanent, while some are temporary. Permanent barriers are implemented as an integrated part of the whole operational life cycle, while temporary barriers only are used in a specified time period, often during specific activities or conditions.

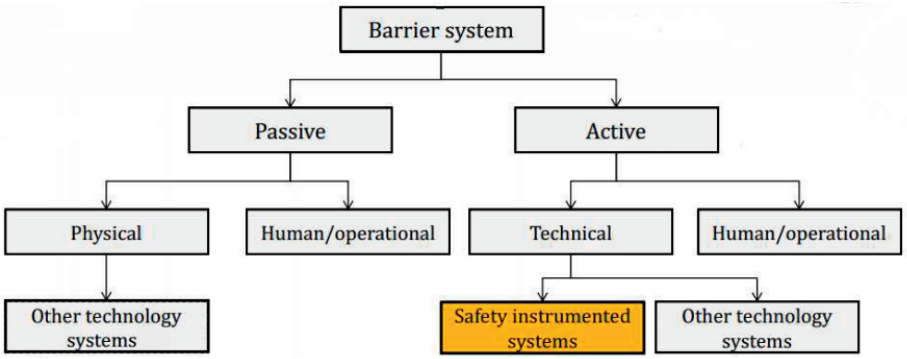

Fig. 1. Safety barrier classification, adopted from [3]

Authors [9] note that identifying technical (physical) safety barriers, usually, it is quite simple, but in the case where the safety barrier includes an action for example, the operator's response to an alarm), you should be careful and distinguish between the action itself, which performs the barrier function, and

the factors that help the operator in making the correct decision (technological instructions, training, precise information presentation, etc.). [10] offers a somewhat different approach classification of safety barriers based on evaluating their effectiveness in the event of a potentially dangerous situation. In depending on the degree of efficiency (high, medium, low) distinguish the following types of safety barriers.Technical (high efficiency). Can prevent the spread of risk factors, reduce the risk of a situation, mitigate the consequences, or reduce the likelihood of risk factors [10]. If there is a technical barrier if it doesn't work, the threat is transferred to another one technical barrier to implementation of potentially dangerous event (until the triggering event is reached). The same applies to further escalation from the triggering event to consequences. The following subcategories are distinguished technical barriers: technical barriers that are triggered on demand (emergency cut-off valve, drencher system, emergency tank); technical passive, operate on a permanent basis, perform barrier function by its mere presence (safety valve, collapse, fire-proof and explosion-proof partitions etc.); technical control barriers that activate other barriers that prevent or mitigate the consequences of a dangerous event (gas detectors, fire alarm system, accident notification system, etc.).

Risk reduction of Equipment under control (EUC) or technological process is shown in Figure 2. Barriers of this type cannot prevent the development of

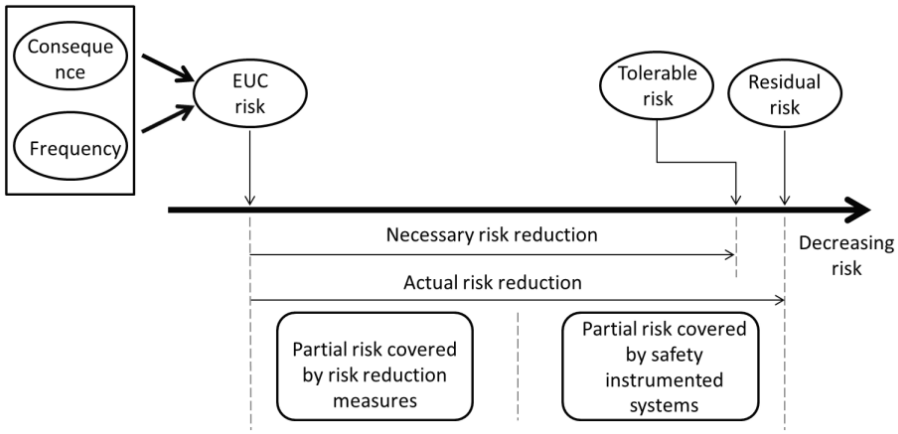

Fig. 2. Risk reduction of Equipment under control (EUC) or technological process

the accident, but can activate other barriers that will do this. Human (organizational) (average efficiency). Contribute to the control of a process or activity. This type of barrier can reduce the probability of the triggering event by strengthening other barriers or preventing them from being weakened, but if a potentially dangerous event has already been initiated, then this type of barrier,

offen can prevent its development, or reduce the consequences. The following subcategories are distinguished: types of barriers: procedural (inspections and observations, control tools, process management, work risk assessment, work permit system etc.); human (operational) (control by the operator, supervision, periodic detours, etc.). Fundamental (low efficiency in the immediate vicinity of the event). Their effect is divided in time from the occurrence of the threat to the implementation of the factor risk. However, fundamental barriers make a huge difference an important and effective contribution to the safety of the system by checks and controls for vulnerabilities system and the original causes of failures. The following subcategories are distinguished this type of barriers: the fundamental procedural (analysis of the project, assessment of commissioning, checking the internal regulations, analysis of operation, confirmation of qualification); fundamental human (good health of workers, etc.) [11]. A number of standards and guidelines have been issued to assist in designing, implementing, and maintaining reliable SISs. The most important of these is the international standard IEC 61511 [13], which is a generic standard that outlines key requirements to all phases of the SIS life-cycle.

2 Problem statement

The problem of optimizing the composition of the SIS is to select the necessary and sufficient set of sensors, logic elements and final performers, taking into account the constraints on the budget of the project. IEC 61511 [13] suggests that consideration should be given to the introduction of any safety measures, applying the principle of risk reduction ALARP (as low as reasonably practicable) [14].

The level of risk reduction taking into account safety barriers is shown in the Figure 3.

The probability of failure of safety measures can be determined by $q(t) = e^{-\lambda t}$, where λ is the equipment failure rate.

In general, can introduce

$$\begin{cases} \min \sum\limits_{i=1}^{n} (S_j b_i) \\ \sum\limits_{i=1}^{n} (q_i) \prod q_{lock_j}^{b_j} \prod q_{diag_j}^{b_j} \prod q_{ems_j}^{b_j} < q_{req_1} \\ \dots \\ \sum\limits_{i=1}^{n} (q_i) \prod q_{lock_j}^{b_j} \prod q_{diag_j}^{b_j} \prod q_{ems_j}^{b_j} < q_{req_n} \end{cases} \tag{1}$$

q_i - probability of failure of the i-th component of the process system,

S_j – the cost of implementing the j-th safety measure,

q_{lock_j} - the probability of failure of the j-th lock;

q_{ems_j} – the probability of failure of j-th emergency stop;

q_{diag_j} -probability of failure of the j-th diagnosis, revealing preemergency conditions;

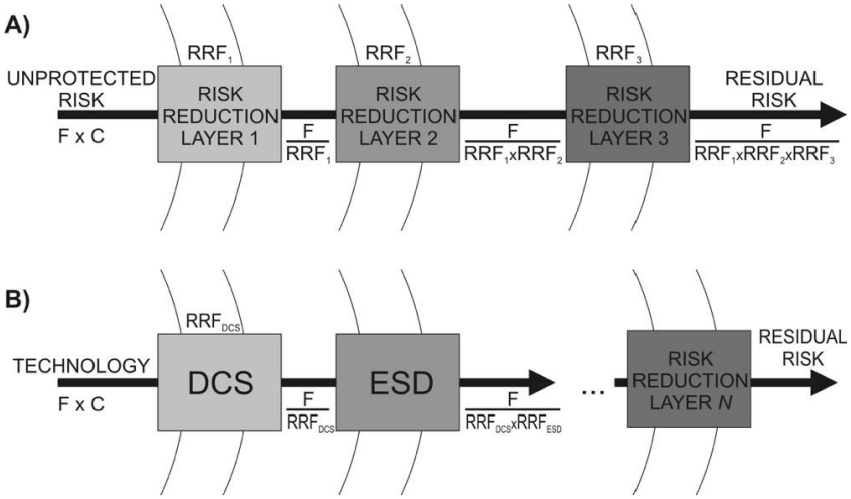

Fig. 3. Model of Risk Reduction layers. A) general view, B) SIS view

q_{req} - the probability of occurrence of a dangerous situation, specified in regulations or determined during the analysis.

3 Approach to problem solving

3.1 Optimization

The problem of optimization of the choice of safety measures is a modification of the "backpack Problem" [6], class of combinatorial optimization problems, which can be formulated as follows:

$$\begin{aligned} &\max_x \sum_{j=1}^{n} (p_j x_j), x_j \in 0..1, j \in 1..n \\ &\sum_{j=1}^{n} (\omega_{i,j} x_j) < c_j, i \in 1..m \end{aligned} \tag{2}$$

where p_j and $\omega_{i,j}$ are weights, and c_i is a cost, and $\mathbf{x} = (x_1, ..., x_n)$.

The backpack problem can be solved in several ways: the method of dynamic programming [7]; brute force; the method of branches and boundaries [16]; the method of statistical modeling. Consider the application of the statistical modeling method. In general, the approach can be represented as follows, find the maximum of the function $S(x)$ on a given set $\mathbf{X}$. Let's assume that the maximum is achieved for only one value of the parameter x^*. Let us denote the maximum by γ^*.

$$S(x^*) = \gamma^* = \max_{x \in \mathbf{X}} S(x) \tag{3}$$

Optimization problem can be related to the calculation of probability $l = P(S(\mathbf{X}) \geq \gamma)$, where $\mathbf{X}$ has some probability density $f(x;u)$ on the set X (for example, having a uniform distribution density) and γ is close to the unknown γ^*. As is correct, l is the probability of a rare event, so a sampling-by-significance approach can be used. Thus, sampling from such a distribution yields optimal or nearly optimal values. The last value $\gamma^* = \gamma$ is usually unknown, but using statistical modeling, a sequence $\hat{\gamma_t}$ is formed at each step of the simulation, which tends to the optimal γ^*, as well as at each step the change of the modeled vector $\hat{\mathbf{v}}^*$ is fixed [15].

3.2 Algorithm

1. Choose the initial vector of parameters $\hat{\mathbf{v}}_\mathbf{0}$, let $N^e = [eN]$. Take the counter $t = 1$;
2. Generate N random vectors $X_1, ..., X_N$ with density $f(*; \hat{\mathbf{v}}_{t-1})$, determine the values of $S(X_i)$ for all i, and arrange them in ascending order from smaller to larger: $S_(1) \leq ... \leq S_(N)$. Let γ_t be the $(1-e)$ quantile of the obtained values, thus $\hat{\gamma_t} = S_{(N-N^e+1)}$;
3. Using the same sample of random vectors $X_1, ..., X_N$ solve the equation $\max_v \frac{1}{N} \sum\limits_{i=1}^{n} I_{S(X_k) \geq \hat{\mathbf{v}}_\mathbf{0}} \ln f(X_k; n)$ denote the solution as $\hat{\mathbf{v}}_\mathbf{t}$;
4. If the stop criterion is reached, then end the algorithm, otherwise change the counter $t = t + 1$ and proceed to step 2.

4 Numerical example

4.1 Brief description of the model

As an example, we will consider the fuel supply subsystem shown at fig. 1, it includes a fixed volume tank (Tank), a level sensor (LV), a pumping valve to the next section of the process (V1) and a feed pump (PD) with a control system implemented on the control unit (CU). During the preliminary analysis, it was revealed that two dangerous conditions are possible at this site: the occurrence of a fire and its propagation, as well as tank overflow. Assume that the required probability of preventing the development of fire and exceeding the level in the tank should be less than $1 \cdot 10^{-5}$ and $1 \cdot 10^{-4}$ per year, respectively.

Modeling of safety-related systems is based on the theory of reliability. IEC 61511 [13] offers the following methods for assessing reliability: quantitative evaluation using simplified equations based on block diagrams of reliability and analysis of failure trees. In some cases, Markov analysis can be used, a more complex approach allows working with dynamic models that take into account the development of failure over time. The qualitative analysis as Failure Mode and Effect Analysis (FMEA) in accordance [13] is given in Table 1.

Table 1. FMEA of technological subsystem.

Element	Failure type	Consequences	Safety measures
Tank	Destruction of the hull	Fire	D_1 - control of the hull by ultrasonic control device D_2 - magneto resistive monitoring device H_1 - switching on the fire pump and water supply H_3 - emergency opening of the emergency drain
Level sensor	False values	Exceeding the limit	D_5-monitoring of the sensor Z_2-emergency stop of process equipment (pump) H_3 - emergency opening of drain valve
Level sensor	The absence of values	Shutdown	not required
Feed pump	Feed loss	Shutdown	not required
Feed pump	Overheat	Fire	D_3 - monitoring the state of the windings D_4 - housing temperature control H_1 - switching on the fire pump and water supply
Feed pump	False start	Exceeding the limit	Z_2 - emergency stop of process equipment (pump) H_3 - emergency opening of drain valve
Transfer valve	Failure to respond	Shutdown	not required
Transfer valve	False opening	Shutdown	not required
Control system	Loss of control signal	Shutdown	not required
Control system	Erroneous command	Exceeding the limit	Z_2 - emergency stop of process equipment (pump) B_1 - pump control limitation when 70 % of the tank valume H_3 - emergency opening of drain valve

Taking into account various variants of implementation of safety measures it is possible to receive the following optimization problem:

$$\begin{cases} \min \sum\limits_{j=1}^{9} (\mathbf{S}_j b_j) \\ (\mathbf{q}_{tank}) q_{D_1}^{b_1} q_{D_2}^{b_2} q_{S_1}^{b_6} q_{S_3}^{b_8} + (\mathbf{q}_{PD.H}) q_{D_3}^{b_3} q_{D_4}^{b_4} q_{S_1}^{b_6} < q_{fire} = 10^{-5} \\ (\mathbf{q}_{LV.F}) q_{D_5}^{b_6} q_{D_2}^{b_2} q_{S_3}^{b_8} + (\mathbf{q}_{PD.F}) q_{S_2}^{b_7} q_{S_3}^{b_8} + (\mathbf{q}_{CU.F}) q_{S_2}^{b_7} q_{S_3}^{b_8} q_{L_1}^{b_9} < q_{o.l.} = 10^{-4} \end{cases} \tag{4}$$

It is needed to find the vector $B = \{b_1, b_2..b_9\}$, at which (1) is executed, on a set of initial data from table. 2-3. For example, the vector $B = \{1, 0, 1, 0, 0, 0, 1, 0, 0\}$ means that as part of the safety instrument system, safety measures are used: monitoring the condition of the tank body by the ultrasonic method (D_1), monitoring the condition of the feed pump windings (D_3), emergency opening of the drain valve (Z_3). The total number of combinations $2^9 = 512$.

4.2 Initial data

The initial data on the reliability of the equipment of the production line and safety measures are presented in tab. 2. and tab. 3, respectively.

Table 2. Dangerous failure rate

Event	Code	FR, h^{-1}	α	Probability per year
Tank. Destruction	q_tank	$1 \cdot 10^{-7}$	80 %	$7.01 \cdot 10^{-4}$
Feed pump. Overheating	$q_{PD.H}$	$1 \cdot 10^{-5}$	50 %	$4.29 \cdot 10^{-2}$
Level sensor. False	$q_{LV.F}$	$1 \cdot 10^{-6}$	30 %	$2.62 \cdot 10^{-3}$
Feed pump. False start	$q_{PD.F}$	$1 \cdot 10^{-5}$	5 %	$4.37 \cdot 10^{-3}$
Control system. Erroneous response	$q_{CU.F}$	$1 \cdot 10^{-6}$	5 %	$4.38 \cdot 10^{-4}$

The fuel supply subsystem works 8760 hours a year, without safety measures: $q_{fire} = 4.36 \cdot 10^{-2}$, $q_{o.f.} = 7.43 \cdot 10^{-3}$.

4.3 Optimization parameters

For optimization we introduce a single target function:

$$S(x) = \mu \sum_{i=1}^{m} I_{\sum \omega(i,j) x_j > c_i} + \sum_{i=1}^{n} p_j x_j \tag{5}$$

Where $\mu = -\sum\limits_{j=1}^{m} p_j$. In this case, $S(x) < 0$ if one of the inequalities fails and S (x)= if satisfied. Since the vector $\mathbf{x}$ is binary, the multivariate Bernoulli distribution with density f(x,v)= is chosen as the initial distribution. As initial parameters we will accept the following $N = 10^2$ and $N^e = 10$, and $\hat{\mathbf{v}}_\mathbf{0} = (1/2, ..., 1/2)$.

Table 3. Baseline data on safety measures

#	safety measures	Cost, c.u.	Probability per year
q_{D_1}	Control of the body condition by ultrasonic method	100	$1.00 \cdot 10^{-3}$
q_{D_2}	Magneto resistive monitoring device	200	$1.00 \cdot 10^{-3}$
q_{D_3}	Control condition of winding	10	$1.00 \cdot 10^{-5}$
q_{D_4}	Housing temperature control	25	$1.00 \cdot 10^{-4}$
q_{D_5}	Monitoring of the sensor status by initial test	10	$1.00 \cdot 10^{-5}$
q_{S_1}	The inclusion of the fire pump and water flow	400	$1.00 \cdot 10^{-3}$
q_{S_2}	Emergency stop of process equipment (pump)	200	$1.00 \cdot 10^{-3}$
q_{S_3}	Emergency opening of the discharge valve	200	$1.00 \cdot 10^{-4}$
q_{L_1}	Pump control limitation at 70 % of tank volume	5	$1.00 \cdot 10^{-4}$

We will not use the mixing parameter to define $\hat{\mathbf{v}}_\mathbf{0}(\alpha = 1)$, so at each iteration $\hat{\mathbf{v}}_\mathbf{t}$ will be as follows:

$$\hat{\mathbf{v}}_{\mathbf{t},\mathbf{j}} = \frac{\sum\limits_{k=1}^{m} I_{S(\hat{X}_k) \geq \hat{\gamma}_\mathbf{0}} X_{k,j}}{\sum\limits_{k=1}^{m} I_{S(\hat{X}_k) \geq \hat{\gamma}_\mathbf{0}}}, j = 1, .., n \tag{6}$$

Where $X_{k,j}$ is the j-th component of the k-th random vector $\hat{\mathbf{X}}$. The expression is used as a stop criterion $d_t = \max\limits_{1 \leq j \leq n} \{\min\{\hat{v}_t, 1 - \hat{v}_t\}\} \leq 0.01$. For each population t of generated values, calculate the threshold $\hat{\gamma}_\mathbf{0}$ and the largest value $S(X_k)$ and the value of the stop criterion d_t.

4.4 Modeling results

To demonstrate the convergence of the method, 100 independent modeling cycles were performed. In each cycle, changes in the density of the vector $\hat{\mathbf{v}}_\mathbf{t}$ were recorded after calculation using the formula (6). Fig. 4 present average change value of the parameter vector while 100 independent iteration.

The final decision, the value of the vector $\hat{\mathbf{v}}_\mathbf{t}$ corresponds to the following composition of equipment and measures: the application of monitoring the condition of the pump winding's, and the emergency opening of the drain valve. Vector $B = \{0, 0, 1, 0, 0, 0, 1, 0, 0\}$ is optimal, with total cost S=210, and $q_{fire} = 4.99 \cdot 10^{-07}$ and $q_{o.f.} = 7.43 \cdot 10^{-07}$.

The results of the dynamics of the vector $\hat{\mathbf{v}}_\mathbf{t}$ is presented in fig. 5.

5 Conclusion

The paper presents a method of bringing the problem of optimization of a set of safety measures provided in the SIS to the problem of discrete optimization. The method of statistical modeling with significance sampling was used as a

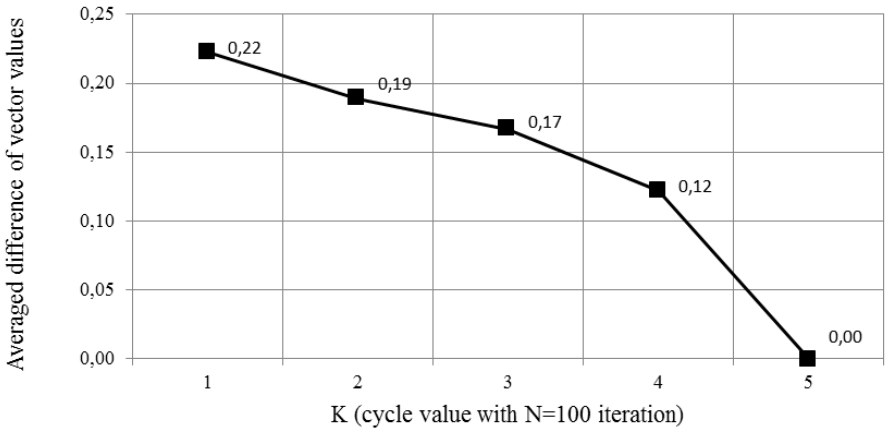

Fig. 4. Averaged difference of vector values

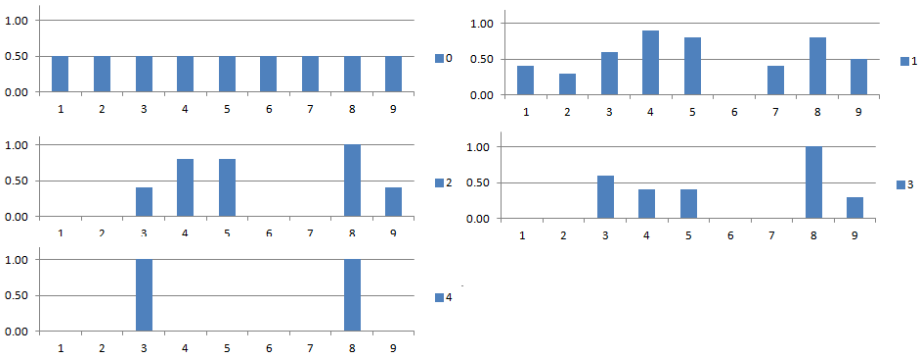

Fig. 5. Dynamics of the probability vector $\hat{\mathbf{v}}_\mathbf{t}$

solution method. The obtained solution corresponds to the solution obtained by brute force. The obtained result can serve as a basis for the development of the requirements specification in accordance with the requirements for the life cycle of the system. Development of a risk model including safety barriers that may prevent, control, or mitigate accident scenarios with in-depth modeling of barrier performance allows explicit modeling of functional common cause failures (e.g., failures due to functional dependencies on a support system). The classification of safety measures is given, the model of risk reduction based on deterministic analysis of the process is considered. It is shown, that the task of changing the composition of safety measures can be represented as the knapsack discrete optimization problem, solution is based on the Cross entropy Monte-Carlo method. A numerical example is provided to illustrate the approach. The considered example contains a description of failure conditions, an analysis of the types and consequences of failures that could lead to accidents, and a list of safety measures. When solving the optimization problem used real reliability parameters and cost of equipment. Based on the simulation results, the optimal composition of safety measures providing cost minimization is given.

References

1. V. A. Bogatyrev On interconnection control in redundancy of local network buses with limited availability. 1999. Engineering Simulation, 16 (4), pp. 463-469
2. Bogatyrev V. A. , Bogatyrev S. V. , Bogatyrev A. V. , "Model and Interaction Efficiency of Computer Nodes Based on Transfer Reservation at Multipath Routing," 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), Saint-Petersburg, Russia, 2019, pp. 1-4. doi: 10.1109/WECONF.2019.8840647
3. Bogatyrev A. V. , Bogatyrev V. A , Bogatyrev S. V. , "Multipath Redundant Transmission with Packet Segmentation," 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), Saint-Petersburg, Russia, 2019, pp. 1-4. doi: 10.1109/WECONF.2019.8840643
4. Yury Redutskiy.: Optimization of safety instrumented system design and maintenance frequency for oil and gas industry processes. Management and Production Engineering Review Volume 8, Number 1
5. Marengo. C.R., J. Flores, A.L. Molina, R. Román, V. C. Vázquez, M. S. Mannan: A formulation to optimize the risk reduction process based on LOPA, J. Loss Prev. Proc. Ind., 1-6, 2012.
6. Andonov, Rumen; Poirriez, Vincent; Rajopadhye, Sanjay (2000). "Unbounded Knapsack Problem : dynamic programming revisited". European Journal of Operational Research. 123 (2): 168–181.
7. S. Martello, D. Pisinger, P. Toth, Dynamic programming and strong bounds for the 0-1 knapsack problem, Manag. Sci., 45:414–424, 1999.
8. Hale, A., Note on barriers and delivery systems, PRISM conference, Athens, 2003.
9. Safety barrier function analysis in a process industry: A nuclear power application/ L.J. Kecklund, A. Edland, P. Wedin, O. Svenson// Industrial Ergonomics. — 1996. — Vol. 17. — Iss. 3. — P. 275–284
10. Delvosalle C., Fievez C., Pipart A. Accidental Risk Assessment Methdology For Insustries in the context of the Seveso II directive. Deliverable D.1C. WP1. — Mons: Major Risk Research Centre, 2004.

11. Svenson O. The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries// Risk Analysis. — 1991. — Vol. 11. — Iss. 3. — P. 499–507.
12. R. Y. Rubinstein. Combinatorial optimization, cross-entropy, ants and rare events. In S. Uryasev and P. M. Pardalos, editors, Stochastic Optimization:Algorithms and Applications, pages 304–358, Dordrecht, 2001. Kluwer.
13. International Electrotechnical Commission (IEC), 61511 Functional safety – safety instrumented system for the process industry sector, IEC, Geneva, Switzerland, 2003.
14. Smith. D.J. and Simpson. K.J.L, Functional safety: A straightforward guide to applying IEC 61508 and related standards, 2nd edition, Elsevier Butterworth-Heinemann, 2004.
15. R. Y. Rubinstein and D. P. Kroese.: The Cross-Entropy Method: A Unified Approach to Combinatorial Optimization, Monte Carlo Simulation and Machine Learning. Springer-Verlag, New York, 2004.
16. D. P. Kroese, T. Taimre, and Z. I. Botev. Handbook of Monte Carlo Methods. Wiley Series in Probability and Statistics. John Wiley and Sons, New York, 2011b.
17. S. Martello, P. Toth, Knapsack Problems: Algorithms and Computer Implementations, John Wiley and Sons, 1990