International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 16 (2017) pp. 5463-5471

Risk-oriented approach to design of the industrial safety system: problems, solutions

Kireeva Elena Vadimovna[1] and Kireev Maxim Sergeevich[2]

[1]Plekhanov Russian University of Economics, Department of finance and prices, Associated Professor, PhD, 115054 Moscow, Russian Federation.

[2]«Schneider Electric» company, Process Automation department, Process Safety & Turbomachinery Controls technical sales consultant, Functional Safety Engineer (TUV Rheinland, #10345/15, SIS), 115504 Moscow, Russian Federation.

[1]Orcid: 0000-0003-0667-9846

Abstract

In the past decade, industrial safety problems have been worsening tremendously. Risk in industry had increased over time due to shift from small, single train or batch operations to large multi-train, continuous operations. When an accident occurs, sometimes this is a cause of negative consequences: process shut down, loss of life, damages to environment and business losses as well. The damages reparation from state budget is undesirable due to the fact they can break a budget plan, moreover, the government reserve would be not sufficient to cover that needs. Risk-oriented methodology described herein conducted on basis of hazard analysis, which is aimed at risk management in the hydrocarbon industry. The methodology considers a comprehensive identification of hazardous with consequences ranking and further risk assessment of potential undesired events, proceeding from industry experience. This particular comprehensive approach can help designers of safety system to obtain thorough information at conceptual phase of a project. Findings: significant amount of industrial accidents (44% approximately) related to problem in specifications and formalistic approach to risk analysis during design of emergency shutdown systems. These concerns bring to groundless rise in price of integrated and control system without focus on functional safety. The given approach would be used by designers and end-users to avoid or minimize risk at a plant; it would increase a profitability as well as effectiveness of facilities in the hydrocarbon industry in Russia. Applications. The methodology includes a several complementary methods in accordance with process safety standards, which is synthesized in a common model. The model includes a flow chart of algorithms and methods, which aimed at identification of necessary risk reduction of potential accident as well as calculation of reliable characteristics of instrumented system designed to minimize process downtime, harm to people, social and financial losses.

Keywords: process safety, safety instrumented function, hazard and operability study, risk management, safety instrumented system, functional safety

INTRODUCTION

In today's circumstances any business decision, such as the industrial, financial or investment, operational or strategic, long-term or short-term is occurring in uncertain conditions. Quantitative measurement of this uncertainty is the risk. It is important to emphasize that absence of risk undermines the foundations of an efficient economy, so long as the risk provides an opportunity to use their intellectual, psychological, motivational and other qualities to maximize profits in uncertain circumstances. Let's emphasize the relevance of the present subject area due to the necessity of taking into account a direct communication between process safety in the hydrocarbon industry and the profitability of production, or the relationship between the expression of financial and operational risks. It is well-known that, in practice, the management of industrial sites in Russia is concerned about the safety of operation of processing facilities; in this connection, it should explore and identify ways and means for more effective management in area of industrial safety, and as a consequence, increase the profitability of hydrocarbon production. You must also take into account the correlation effects of operational risk and the risk of loss of financial benefits, i.e. the risk of non-profits at the disposal of another production, human resources. For example, loss of profits of the enterprise may be closing as a result of the accident, when it is more profitable to sell, than to continue business activity, investment of financial resources in the other assets of the same risk, etc. The account of this risk is conducted at discounted cash flow implications of the decision. For example, in case of choosing to open a new branch of the company, it is necessary to take into

account implicit costs in the form of investment funds in the old extension. If the Net Present Value (NPV) of investment in a new project exceeds the investments in the expansion of the old branch, this investment proposal should take. This discount rate characterizes the risk of loss of profits, because eventually become cheaper money, but not in relation to the goods and services (in this case, inflation process), but from the position that every ruble per unit of time, you can use the most efficient way, i.e. at the highest possible yield. It should be noted that today the search for solutions to the above issues occupies an increasingly important place in the system of corporate management priorities of the oil and gas industry. [1]; [2]; [3]; [4]

For decades industrial professionals have recognized that the cost of catastrophic events, such as fires or explosions, can be very high in terms of injury, death, equipment damage, facility damage, environmental damage, business interruption, and insurance (for reference: one hour of downtime of refinery could cost about 600K USD).

The hydrocarbon industry has answered to this tremendous potential cost through functional safety standards including emergency shutdown systems as well as reconsideration of risk analysis.

The figure presented below reflects relationship between industrial risk, financial risk as well as image risk. Thereby, safety is constantly surrounded by hazards that could express in terms of harm, fatalities, environmental impact, loss of profits and company reputation as well. And the major goal is to keep safety at a plant by elimination of inherent risks .

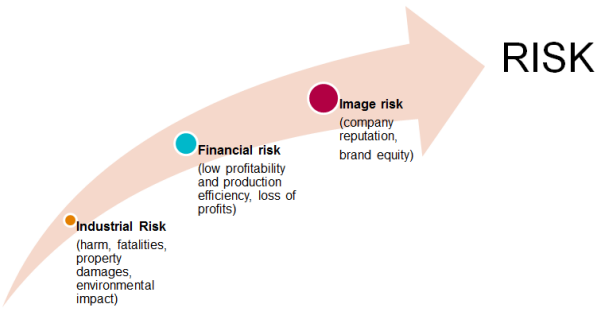

Figure 1. Consequences of getting safety wrong

Process risks minimization or the problem of industrial safety

Ensuring of industrial safety as well as cost-effective operation are superior and complicated tasks, which contain several non-trivial aspects, such as: the right design of technology, compliance of handling with hazardous substances, reliable distributed control system (DCS) as well as special devices and systems aimed at preventing of industrial accidents. These devices include various safety mechanisms like pressure relief valve and electronic emergency shutdown systems (ESD).

Safety can't be delegated. Safe operation of a plant is favor the company image, increases market value as well as allows receiving an additional discount where insurance of high-hazardous site is needed. Accidents rarely have a single cause and are usually a combination of improbable events that people initially assumed as independent and unlikely to happen at the same time. 90% of all accidents occur due to human error; in particular, it is our experience that approximately 44% of these accidents related to problems in specifications. In a context of given article errors in specification consider the ignoring of risk analysis phase during design of ESD system, which leads to formalistic approach to Safety system design and rise in prices of integrated control and safety system as well.

METHODOLOGY

There are two main approaches for risk assessment: quantitative and qualitative. Quantitative method uses different mathematical techniques, such as: probability theory, mathematical statistics. This is more objective and allows the proactive application of risk reduction to novel situation. Qualitative method is effective in situations where the process has a long history and its risk reduction techniques are well established.

Risk-oriented methodology presented in this article, has absorbed the best engineering practice and methods derived from IEC 61508/61511 standards. These methods adopted as a basis of design of reliable ESD system. The foundation of given methodology is an approach, which considers a comprehensive process hazard analysis and risk assessment in order to identify level of necessary risk reduction and safety integrity level (SIL) assigning for each safety instrumented function. The methodology includes a several complementary methods, which is synthesized in one model aimed to identification of failure rate of components that are going to be a part of safety system. Risk-related definitions, such as: functional safety, SIL, Hazard and operability study (HAZOP), layers of protection analysis (LOPA), etc. has been increasingly penetrating into the circle of automation specialists in Russia. However, many specialists haven't a thorough familiarity of understanding of these definitions and methods for SIL assignment. However, the safety lifecycle is being ignored. Requirement for safety instrumented systems (SIS) just cover only controller level, except sensors and final elements as well. In accordance with OREDA statistical information, controller is the most reliable component in a safety instrumented function (SIF) – 8% of failures, sensors – 52%, final element – 50%.

Safety is the number one priority, and safety is applicable to everyone and even in these challenging economic times customers will still invest in safety because the consequence of getting safety wrong has never been higher. The figure below estimates that the total costs of the historically 100 largest industrial incidents to be approximately $34 B US dollar. This number only reflects insured losses. It does not include losses in brand equity, loss of life, social responsibility etc. This is a leading reason why operators invest in safety solutions. Some other market drivers that lead users to invest in process safety include increasing regulatory focus. Recent industrial incidents have led to not only civil penalties but criminal prosecutions of plant personnel when accidents have occurred. Changing industry standards also require control systems to be upgraded. There's a need for safety systems to be more proactive, to diagnose and prevent events before they happen.

The figure presented below reflects distribution of accidents between different segments in the hydrocarbon industry in accordance with statistics of Marsch company.

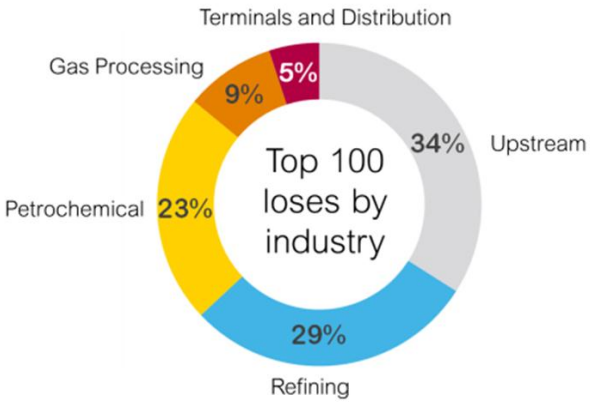

Figure 2. The total accumulated value of the 100 largest property losses in the hydrocarbon industry

It's well known, that the senior management is not always aware of this responsibility. 90% of all accident occurs due to human error. To find a solution new standards have been created. International Electrotechnical Commission (IEC) 61508/61511 functional safety standards cover all activities throughout the safety lifecycle. This means that efforts are focused on development of specific procedures to avoid human error. In spite of all these learning's and available standards why do accidents still occur? There are 3 possibilities.

1. The operators don't know the standards.
2. The operators can't implement them because of a lack of appropriate knowledge.
3. All the operators just don't consider this reasonable.

Risk minimization model. When considering an industrial process, it is recognized that there is an inherent risk of operation. Things do go wrong. When evaluating safety, the frequency of an accident and the consequences (the costs) of an accident are both taken into consideration. Risk is defined as the probable rate of occurrence of a hazard causing harm and the degree of severity of the harm. Thus, risk evaluation includes a combination of frequency and cost.

The figure presented below reflects layers of protection, which is proven-in-use model consisting in several levels aimed at minimization of risks at the different levels: from the process plant up to community emergency response.

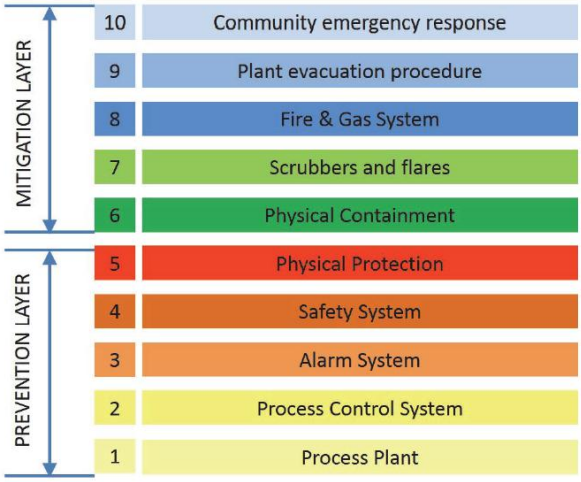

Figure 3. Layers of protection

Layer number one takes into consideration all processes, plants and activities which may generate hazardous situations. The basic process control system is the second safety layer. It controls the plant for an optimization of fuel usage, production quality, etc. It attempts to keep all process variables, such as pressure, temperature, range, level, flow, within safe limits..

Third layer is an alarm system. Requirements for Monitoring and alarm systems.

1. Detect problems as soon as possible, to a low enough level to ensure that corrective actions can be taken before reaching hazardous conditions.
2. Be independent from the control devices they are monitoring, which means they should not fail even if the system they are monitoring fails.
3. Be easy to maintain, check, and calibrate.

Alarm and monitoring systems are considered to be the safety layers in which the operators are actively involved: not everything can be automated.

However this is a double-edged sword because operators may not believe that rare events, alarmed by the system, are real or genuine; operators may take wrong decisions, and fail to act, because overloaded with multiple alarms.

Fourth level is ESD system.

If the control system (DCS) and the operators fail to act, the automatic shutdown system (ESD) takes action. These systems are always completely separated, with their own sensors, logic systems and final elements.

Design of Safety systems.

1. Allow the process to move forward in a safe way when specified conditions require so.
2. Automatically brings the process to a safe.
3. Take action to mitigate the consequences, of an industrial hazard.

Fifth level is physical protection.

Release valves and rupture discs are one mean of physical protection that could be used to prevent, for example, an overpressure condition.

Functional Safety

The concept of functional safety is fundamental for most safety-related systems. The hydrocarbon industry, nuclear plants, the manufacturing sector, all relies heavily on Functional safety to achieve safety in areas where the operation of equipment could give rise to hazards.

Functional safety is part of the overall safety relating to the process and basic process control systems which depends on correcting functioning of SIS and other active independent layers.

Generally, risk is the result of multiplication between the frequency of accidents and their consequences. [5]; [6]

Calculations:

Risk=Frequency of accidents x Consequences (1)

The IEC 61511 standard describes technical requirements for safety system using in the process industries. The SIS consists of all devices necessary to implement safety functions. There are two key conceptions in IEC 61511: safety lifecycle and safety integrity level (SIL).

You can find Safety Lifecycle of Safety Instrumented System on the picture below. It consists of three interrelated phases: analysis, implementation, operation. At the first stage we have to identify all process-related hazards and determine a necessary risk reduction. At second stage we should implement a safety instrumented system based on results of first stage. And at third stage we should keep safety by specified proof-test procedures of the components, which contains Safety Instrumented System.

First of all, SIL-oriented methodology focused on «Analysis» phase, which is being unfortunately ignored by many operators and design institutes in Russia and it leads to severe consequences.

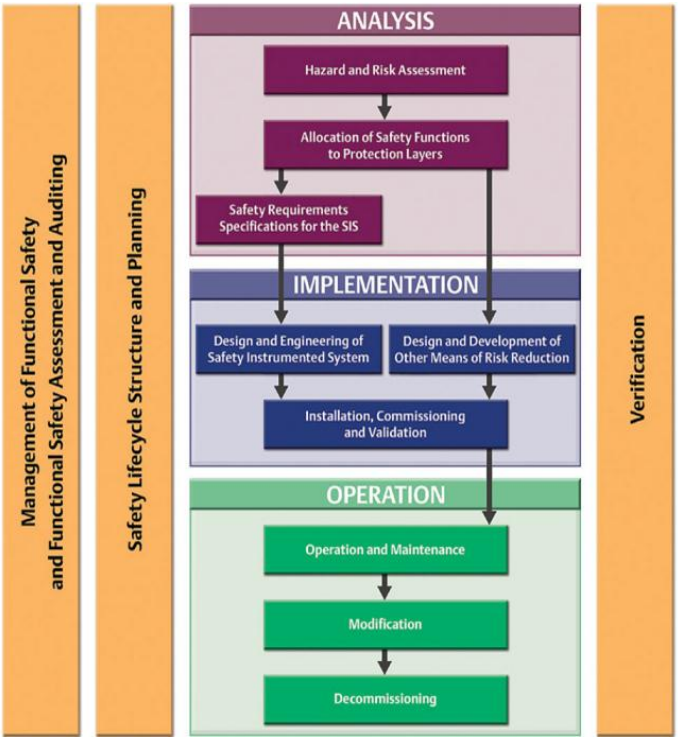

Figure 4. Safety Lifecycle

ANALYSIS

«Analysis» phase considers a comprehensive process and hazard analysis (PHA), which helps in systematic assessments of the potential hazards associated with a process. PHA helps to employees in establishment decisions for improving safety.

Methods for PHA

There are a several methods for PHA. In the given methodology established method is a hazard and operability studies (HAZOP).

HAZOP is a systematic analysis of an existing or new process in order to evaluate concerns, which can represent risk to people, equipment or business. The purpose of performing a HAZOP is to examine the design and identify process-related gaps. The technique is based on segmentation the overall design of the process into a number of sections called 'nodes' which are have to be individually reviewed.

NO FLOW
Wrong flow path - blockage - incorrect slip plate – incorrectly fitted return valve - burst pipe - large leak - equipment failure - incorrect pressure differential - isolation in error

MORE FLOW
Increase pumping capacity - increased suction pressure - reduced delivery head - greater fluid density - exchanger tube leaks - cross connection of systems - control faults

MORE TEMPERATURE
Ambient conditions - failed exchanger tubes - fire situation - cooling water failure - defective control - internal fires

Figure 5. Examples of guidewords

The HAZOP technique is qualitative. It is focused on identification of potential hazards and operability problems. Structure is given to the process reviewing by applying guidewords in order to examine each node. Examples of guidewords below.

RESULTS

Results of a HAZOP is a table with process hazards aligning with ranking of consequences.

After a HAZOP session is finished, it is recommended to allocate of safety function to protection layers. First of all it should be considered a possibility to use mechanical facilities – relief valves, dikes etc... In case of mechanical facilities is not suffice, there is a necessity to use safety instrumented function (SIF).

You can find a manufacturing scheme below, which is extracted from piping and instrumentation diagram (P&ID) at the one of the refinery in Russia. The hydrarbons is being dispensed by two pumps (main and reserve) into the sedimentation drainage. After that, part of oil go to reactor and further processing and residual oil go to exhaust. There are several sensors for measure and process control. And main idea of the HAZOP (hazard and operability study) procedure is to identify all of the hazards that could lead to catastrophic consequences in order to develop an adequate steps to eliminate risk.

We normally use the following algorthytm: first of all, guide-word methods to have a thorough familiriaty of understanding of deviation for the process, then reveal possible cause and consequences and eventually propose actions to be done as well.

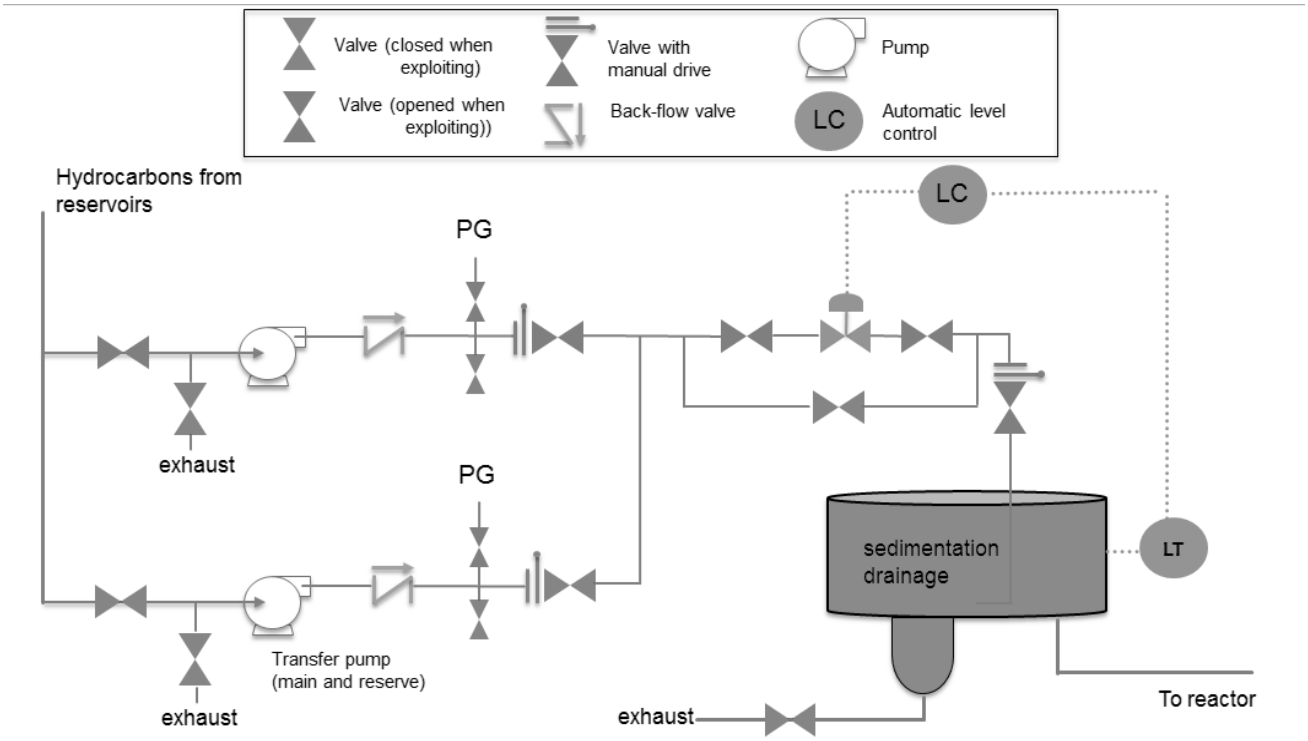

Figure 6. HAZOP at a section between two nodes

Table 1: Results of a HAZOP applied to drawing at the figure 6

Guide-word	Devia-tion	Possible causes	Consequences	Actions to be done
NO ***or NOT***	No feed	No resources from reservoir (hydrocarbons)	Loss of hydrocarbons in reactor, formation of polymers in heat exchanger	1) Consider a connection with a reservoir
		Transfer pump failure (motor failure, power loss, corrosion of the pump wheels, etc.)	Loss of hydrocarbons in reactor, formation of polymers in heat exchanger	
More	More flow	FV valve failure (opened)	Pressure increasing in a reservoir. Risk of explosion and release of materials	Consider to design a safety instrumented function to be allocated in a SIS
		Field devices failure. LT sensor (bottom scale)	Pressure increasing in a reservoir. Risk of explosion and release of materials	Consider to design a safety instrumented function to be allocated in a SIS

The conception of risk reduction

The picture below demonstrates the main conception of the risk reduction. At first, we have an inherent risk of the process. And starting from this point we're moving to target tolerable risk level through different activities: changing in design, pipes, creation of mechanical integrity, using independent layers of protection and finally we achieve a necessary risk reduction by using Safety Instrumented Systems (SIS).

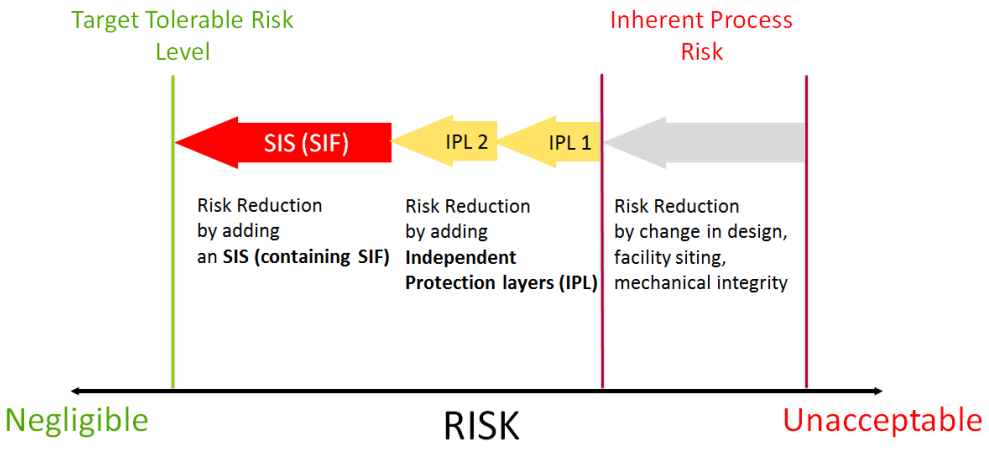

Figure 7: Risk management

Key terms and definitions of IEC 61511.

Safety instrumented function (SIF) – function to be implemented by a SIS which is aimed at achieving and maintaining safe state for the process. A SIF is included any combination of sensors, controller and final element.

Safety Integrity Level (SIL) – Discrete level (from 1 to 4) which is assigning for each SIF.

First of all, SIL defines two main characteristics:

1. Necessary Risk Reduction;
2. Reliability requirements for SIF:
   - Probability of failure on demand (PFD);
   - Hardware fault tolerance (HFT).

Probability of failure on demand (PFD**) –** effectiveness of SIF can be expressed by quantitative probability of failure on demand - figure 8. [7]

Sometimes when a system is already successfully commissioned, over the time it tends to degrade in terms of mathematical reliablility (see on picture below) due to occurring of unrevelead internal failures, which calls dangerous undetected. In order to keep safety at appropriate level we should develop a clear proof-test interval of the SIS components and do not allow to exceed above the specified safety integrity level.

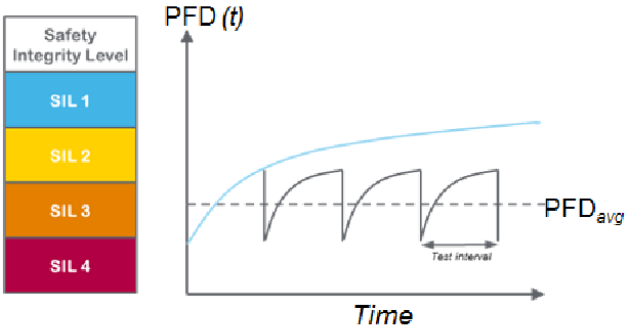

Figure 8. Average probability of failure on demand

Probability of failure on demand

Calculations: Probability of whole loop (SIF) from sensor to valve (final element) is $PFD_{SIF} = PFD_{sen} + PFD_{lsv} + PFD_{fin}$ = sensor probability of failure on demand + logic solver probability of failure on demand + final element probability of failure on demand.

Calculations:

Average probability of failure on demand $PDF_{avg} = \lambda_{du} * (TI/2)$

= dangerous undetected failure rate * (proof-test interval / 2) (2)

Following that, it's must be calculated a necessary risk reduction and define SIL for SIF by using quantitative method- LOPA.

DISCUSSIONS

The LOPA concept is to provide Independent Layers of Protections (IPL) around hazardous processes to prevent undesired consequences from occurring (e.g. explosion, fire, toxic releases, etc.). LOPA is a tool that is used after a HAZOP and the definition of tolerable risk.

Table 2: Typical initiating cause frequency

Initiating cause	**Frequency**
Human error	0,10
Control loop failure	0,10
Relief valve	0,001
Vessel pressure rating above maximum challenge from internal and external pressure source	10^{-4} or low

Thereby, let's apply the methodology to our example. In accordance with table 2, after the HAZOP session we've identified of a necessity of SIF to be allocated to SIS.

Fault tree analysis (FTA) for our example below.

We have a diagram, which consists following columns:

1. initiation causes- failure of control loop, it occurs once a 10 years,
2. independent layer of protection (IPL #1), which is operator failure (standards require to use 0,1 value for failure),
3. we also have an additional independent layer of protection (IPL #2)

Further we have to multiply all IPL's failure magnitudes and receive a frequency of undesired frequency (see on picture beelow).

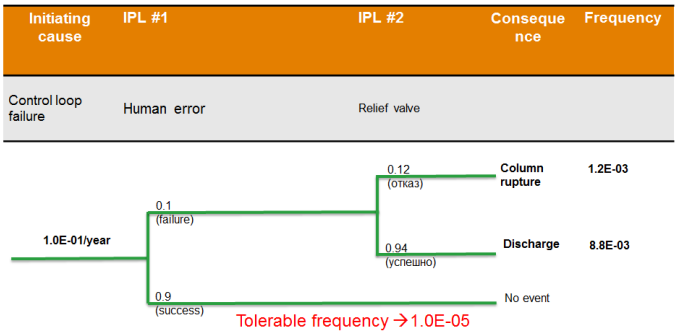

Figure 9. LOPA tree for undesired consequence

On the basis of diagram it's obvious that existing IPLS aren't sufficed to avoid undesired consequence (tolerable frequency < actual frequency of column rupture).

Let's consider a SIF in a SIS in accordance with our HAZOP results and define a necessary risk reduction (NRR).

Calculations:

NRR = TF / IPLs = necessary risk reduction

= tolerable frequency / frequency with existing layers of protection

(3)

Necessary risk reduction = 1.0E-05/ 1.2E-03 = 0,0083.

Thus PFDavg for SIS = 0,0083. Risk Reduction Factor (RRF) = 1/PFD=1/0,0083=120 (which get in the SIL2 level).

Solution is to increase RRF up to 200 in order to achieve safety. Let's do a checking calculation.

We have add a new additional IPL layer of protection – Safety Instrumented Systems (SIS) and receive acceptable value of undesired event, so now we are able to develop a SIS using specific components.

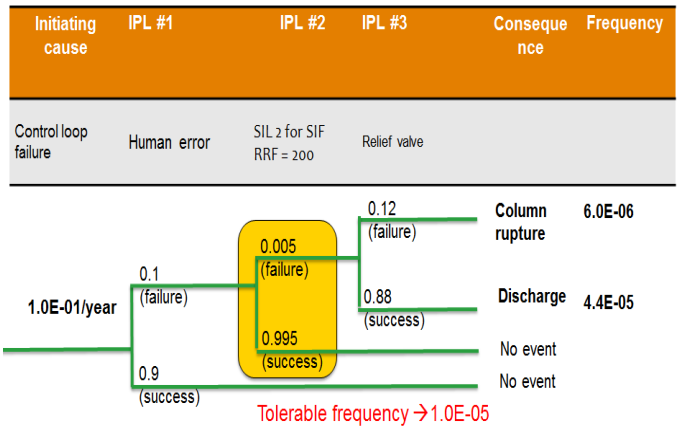

Figure 10. LOPA tree for undesired consequence after new IPL adding

CONCLUSIONS

On the basis of new calculation, its can concluded that new IPL as a SIF with SIL2 will bring down a frequency of undesired event.

The picture below is a comprehensive block-diagram based on all methods which are being considered in the given aticle and consists a specific actions to be done in order to reduce process-related risks

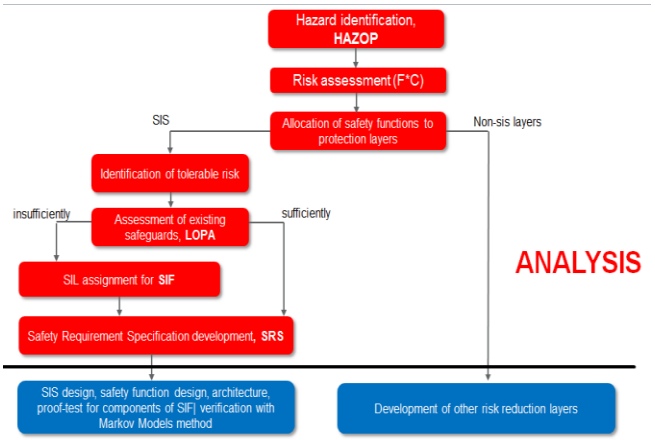

Figure 11. Specified risk-oriented model for managing risk on the analysis phase

Subsequently, we have to design a new SIF considering requirement of PFD=0,005. There were a calculation in the given article which shown that new IPL is needed. So, SIL-oriented methodology can expressed as below.

Departments, which are responsible for the industrial safety, have reacted to this tremendous consequences by development of functional safety standards as well as process safety standards. History of process safety standards development is being evolved since 70th of last century, when two major accidents had occurred in Europe in the chemical industry. Some people believe technology has all of the answers, but technology alone can't ensure safety. To guarantee safety at a plant, or on a production side, sound processes and procedures must be established and establishment of this is a senior management responsibilities. Establishment of the risk-oriented processes and procedures is a senior management responsibility. The main target of that is not just avoiding risk, but minimization of losses. The company must focus at risk managing rather than avoiding of them. The effectiveness of the risk management of the process depends on the understanding by senior management. At the same time, the risk analysis is not being considered by Russian economy as a supreme part of safety. In conclusion, we emphasize that the occurrence of process hazards is a threat to the preservation and enhancement of financial resources. Effective risk management is tough related with profitability. The proposed methodology is mainly focuses at the comprehensive risk analysis. The given solution avoids a formalistic approach to design of a SIS and provide Customers with state-of-the-art method to managing of industrial safety system on high-hazardous facilities.

REFERENCES

[1] Grèze L, Pellerin R, Leclaire P, N. Perrier N. Evaluating the effectiveness of task overlapping as a risk response

strategy in engineering projects. Int. J. of Project Organisation and Management. 2014. Vol. 6; 1: 33 – 47.

[2] Gheorghe A, Muresan L. Risk assessment of large industrial complexes in Eastern Europe: a comparative prospective. Int. J. of Environment and Pollution. 1996. Vol. 6, 4: 649 – 655.

[3] Nojoumi A, Givehchi S. Identifying and Prioritizing Factors that Affect Technological Hazards in the Iranian Gas Refining Industry using Multi-criteria Decision-making Techniques (Case Study: South Pars Gas Complex). Indian Journal of Science and Technology. 2015. Vol. 8, 20: 34-35.

[4] Pinto C, McShane M, Bozkurt I. System of perspective on risk: towards a unified concept. Int. J. of Systems Engineering. 2012. Vol. 3; 1:33 – 46.

[5] Popov V. dissertacija ... kandidata tehnicheskih nauk: 05.02.23. Moskva.[Internet]. 2009 [cited 2017 Feb 2]; Evailable from: http://dlib.rsl.ru.

[6] Roghanian E, Moradinasab N, Afruzi E, Soofifard R. Project risk management using fuzzy failure mode and effect analysis and fuzzy logic.Int. J. of Services and Operations Management. 2015. Vol. 20, 2: 207 – 227.

[7] Tjrres E, Alejandro C. 2009. Modelling and optimization of Safety Instrumented Systems based on dependability and cost measures. http://etheses.whiterose.ac.uk