FACTA UNIVERSITATIS
Series: **Working and Living Environmental Protection** Vol.11, N^{o} 2, 2014, pp. 145 - 152

RISK ASSESSMENT OF INDUSTRIAL AND ENVIRONMENTAL MONITORING SYSTEMS – THE SIGNIFICANCE OF HUMAN RELIABILITY ANALYSIS

UDC 005:331.468:502.31/.37

Evica Stojiljković, Srđan Glišović, Tatjana Golubović

University of Niš, Faculty of Occupational Safety in Niš, Serbia

Abstract. *In analyses of industrial safety systems, Risk Assessment procedures are foremost being performed in order to improve protection measures aimed to safeguard personnel and the equipment. However, environmental consequences of certain major industrial accidents clearly imply that Environmental Safety Assessment should not be neglected as an important component of overall Risk Assessment process. It has been proved that significant number of industrial accidents have been either caused or aggravated by actions (or lack of appropriate actions) of various operators in charge. Therefore, Human Error Assessment must be taken in consideration as an important part of Environmental Safety in industrial and infrastructural systems likewise.*
Some preliminary researches of the latest events indicate that certain serious consequences of natural disasters could be mitigated if the data obtained from environmental monitoring were coupled with the alerts from industrial systems and than properly handled by decision makers at various hierarchical levels. While some failures could be attributed to design errors in early stages of development, some others fall entirely in domain of improper communication or lack of adequate and timely response.
Standard techniques, methods and tools for Health and Safety Risk Assessment, Environmental Risk Assessment and Human Reliability Assessment have been developed for years. However, there will always be room for improvements in terms of integration, quality and comprehensiveness.
This paper strives to describe the possibilities of combining and/or integrating some standard procedures in order to improve Risk Assessment outcomes and safety performance of observed systems. Human Error Analysis has been emphasized as an important part of Risk Assessment procedure and a framework for performing assessment has been outlined in the paper.

Key words: *Risk assessment, human reliability analysis, environmental monitoring systems.*

Received September 22, 2014 / Accepted December 30, 2014
Corresponding author: Evica Stojiljković
Faculty of Occupational Safety in Niš, Čarnojevića 10A,18000 Niš, Serbia
Phone: +381 18 529 774• E-mail: evica976@gmail.com

1. INTRODUCTION

Safe performance of any large industrial compound relies on iterative safety reinforcement procedures that comprise planning, risk assessment (risk identification, risk analysis, risk evaluation), risk treatment, monitoring and reporting. An iterative nature of safety procedures imply that a reliable monitoring system must be established for every complex unit in order to timely provide information on vital changes of the objects under observation. No matter how automatized a procedure is, human involvement would be inevitable either in design process, system exploitation or in sudden emergency situations. Even advanced Decision Support Systems might not prove sufficient assistance when it comes to environmental accidents under specific external conditions. In such situations, Human Reliability would be of outmost importance for the appropriate judgment on data obtained by a monitoring system, as well for the course of action taken according to the monitored values.

Human errors might have serious implications on the environment and society if they cause or seriously contribute to major industrial accidents. Some system accidents that have occurred during last few decades (i.e. Bhopal, India and Chernobyl, USSR) have been largely influenced by human error. It has been concluded that some of the accidents could have been prevented, or even predicted if human error assessment techniques have been timely applied. Development of complex, hazardous industrial systems is the necessity of modern civilization, and Human Reliability Assessment (HRA) must be performed in a framework of Risk Assessment procedures in large industrial systems.

The common term "Human Error" has been defined by Swain [7] as "a member of a set of human actions that exceeds some limit of acceptability, i.e. an out of tolerance action (or failure to act) where the limits of performance are defined by the system". Human error may be triggered by different factors: insufficient qualifications of an operator, lack of precision, cognitive failure or concentration deficiency, failure to understand and follow rules, etc.

There are three specific preconditions for a human error to happen: there must be opportunity for an error (or requirement for human performance in response to some event), the error must occur and system must fail to correct or compensate it, and it must have negative consequences, as it is, or be combined with some other technical failure and/or environmental circumstances.

While some human errors have a relatively modest impact on system performance and safety, or are considered recoverable, the consequences of human errors in complex and potentially hazardous industries might cross boundaries of the plant itself and spread out to the local community and neighboring ecosystems.

Sudden technical failures are something few people are prepared or trained for. Some events are not immediately apparent to the operator, or information on hazardous event may be delayed as it is the case in most complex systems and some large-scale accidents involving multiple fatalities.

Estimating the ways in which systems can fail is rather difficult since there are so many interacting components, of which the human operator is the most sophisticated one. Human behavior is multifaceted and very difficult to predict. It makes Human Reliability Analysis (HRA) a rather ambitious approach, particularly taking into account the fact that it deals with the complex area of human error combined with intricacy of large industrial or organizational systems. As stated in the work of Haugen, S. and Øien, "complex systems often require correspondingly complex assessment procedures" [2].

Operators are often relatively autonomous, and they can interpret inputs in many different ways. Operator performance is influenced by large number of factors in the work environment, and their behavior relies on acquired skills, knowledge and experience. Especially in high risk industries, the human error identification related to misdiagnosis under abnormal events has become of increasing concern. There is a shift of emphasis form quantifying HEPs toward understanding the causes of errors. It has been realized that some new error-reduction operator-oriented strategies might prove more effective.

Human performance is also found to be influenced by managerial and organizational factors. There are strong indications that managerial level influence can have adverse effect on the system vulnerability to human error related risks. The methods are being developed to estimate the quantitative impact of such influences on human reliability assessments and overall risk assessments.

Human Error Analysis (HEA) takes into consideration human contribution in development of certain hazard and risk. Usually it includes not only human error identification but also preliminary identification of error mitigation measures [1]. There is an obvious need both for methods and tools for proper assessing the risks that are attributable to human error and for approaches for reducing system vulnerability to human error impact. The three principal functions of HEA are: identifying errors that might occur, predicting likelihood of error occurrence and improving human reliability by reducing error probability.

This paper focus primarily on HRA in the risk assessment context, and attempts to describe a framework approach to HRA, taking into account existing HRA tools for error identification, quantification and reduction. Therefore, the paper comprises brief overview of HRA development and the role of human error in complex systems, emphasizing the significance of human reliability analysis for environmental safety of industrial compounds.

2. INDUSTRIAL AND ENVIRONMENTAL MONITORING SYSTEMS

Environmental monitoring systems are ultimately human dependant and thus risk prone. Therefore, an environmental monitoring system either in or beyond a large industrial compound, however advanced it might be, should always be considered a vital part of environmental safety and therefore subjected to a comprehensive Risk Assessment. This assessment might be a part of an overall assessment of industrial compound or an independent surveillance on the features and performances of a monitoring system itself. In the former, human error assessment would be an integral part of the procedure, while in the latter human reliability could be of particular concern, especially when it comes to inadvertent operator's actions with highly unpredictable outcomes (e.g. due to combination of anthropogenic and natural factors, or chain of events in and outside of the system).

It was common practice in many companies to place sampling locations for environmental monitoring according to so called grid approach (i.e. to segment the area observed and take a sample in each of the grids). However, certain regulations require risk based approaches in manufacturing, as well as in environmental monitoring. Therefore, environmental monitoring should be based on risk of contamination by an industrial process. Environmental monitoring sample site locations and sampling frequencies should be justified by appropriate risk assessments. It is vital to ensure that the collected data are meaningful and help to identify possible contamination problems related to products and processes. A new challenge would be to establish a risk-assessment-based environmental monitoring in various industrial sectors. The

following factors should be taken into account while composing an industrial environmental monitoring system:

- regulatory requirements for environmental monitoring,
- methods to select sample locations based on risk assessment,
- risk assessment to support existing environmental monitoring,
- monitoring methods and equipment,
- data collection and data processing options,
- overall system and human reliability assessment.

Apart from the possibilities for human error occurrences in environmental monitoring system design, exploitation and maintenance, there is also an issue of reliability of applied methodology. Environmental engineers are sometimes overconfident about the ability of their methods to correctly detect an infrequent hazard in environmental samples, and it raises another concern that some avoidable events might occur just because early warning signs have not been revealed. The proper assessment of environmental monitoring evidence is prerequisite for environmental risk analysis. It is of crucial importance to increase comprehension and correct interpretation of the quantitative environmental monitoring data to adequately support environmental risk management decision-making. In particular, when monitoring provides results that indicate an infrequent event or hazards, it is important to avoid any confusion that might have arisen from the different meanings and uses of terminology. Resolving communication issues should take place at joint trainings for all relevant players in an entire industrial safety system.

3. THE ROLE OF HUMAN RELIABILITY ANALYSIS IN RISK ASSESSMENT PROCESS

In spite of significant technological advances in systems design, accidents are still occurring. A systematic consideration of human error in system design and operations can lead to improved safety. The issue of human error is the most apparent in large high-technology systems [4], where human error in one area can affect other areas, or combine with a hardware failure.

Human error identification, prediction and reduction together form the Human Reliability Assessment (HRA), and require detailed qualitative and quantitative risk assessment (QRA) of complex systems [6]. Thus, "Human Reliability Analysis can be defined as a method employed to quantitatively assess the impact of potential human errors on the proper functioning of some system composed of equipment and people" [8].

Risk assessment is the overall process of the risk analysis and risk evaluation [5]. Risk assessment process, known as a Probabilistic Safety Assessment (PSA) takes in consideration hardware and software failures, environmental events and human errors. On other hand, Human Reliability Assessment fits into the overall system risk assessment process (Fig. 1). It is of outmost importance to identify HRA inputs, and the way HRA interface with the PSA. Various techniques for HRA might be used separately or in combination to identify system vulnerabilities to human error, either within PSA process or outside of it. However, in the foreseeable future, the HRA will continue to occur predominantly within the framework of risk assessment process [2].

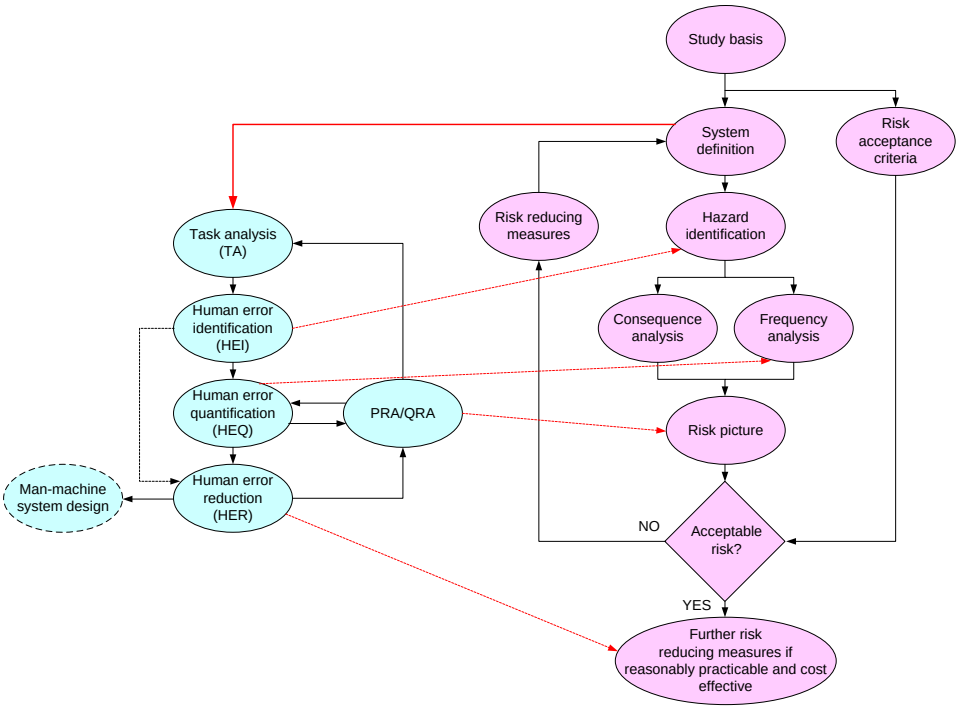

Fig. 1 The Human Reliability Analysis Procedure in Risk Analysis

Several different types of risk could be evaluated in a PSA for any industrial system, and selection will vary for different industrial sectors. Some common risk types for evaluation in industry are as follows:

- the discharge of toxins or pollutants into the environment, yearly,
- injuries of the employees per year,
- fatalities in the workforce per year,
- fatalities in the general public per year.

The PSA comprises the evaluation of risks to employees and general public safety, risks of damage to the facilities and risk of devastation of the environment. It identifies ways in which hazards can occur, calculates the probabilities and frequencies of undesirable events, decides on the consequences of such events and controls if summarized risks comply regulations. Sometimes, PSA may be used to improve the system design and thus reduce the risk to an acceptable level.

The PSA requires a number of significant inputs from HRA. Some level of human interactions with system elements exists in every large system. Therefore, the HRA should be carried out within all PSA. In this manner the effects of human error can be properly evaluated in the framework of overall system risk analyses.

4. THE PROCEDURAL STEPS OF HUMAN RELIABILITY ASSESSMENT PROCESS

A successful HRA requires a systematic approach consisting of the following methodological steps (see Fig. 2):

- *Problem definition* – in this phase the scope of HRA is determined: would it be a part of PSA or stand alone assessment, in which stage of development is the system, which criteria the risk assessment is trying to meet and how vulnerable is the system to human error?
- *Task analysis* – defines the roles of the operators within the system and provides clear definition of what an operator should do to achieve the desired performance.
- *Human Error Analysis* – it has been shown that human errors very often occur in a limited number of forms, some of which are rather predictable. However, *Human Error Identification* (HEI) process is perhaps the most critical part of the HRA, since if an important error is not identified, it will not appear in the risk assessment, and for this reason the risk may be underestimated. HEI may also identify factors that affect human performance – so called Performance Shaping Factors (PSF), which are then used in the error/probability/quantification phase of the HRA process.
- *Human Error Representation* – is achieved by representing the human errors along with other failures in logic trees known as fault and event trees. It is important that the combined risk probabilities of all failures and combination of failures (human, environmental, hardware and software) are summed to decide on the total level of the risk in the system. Another area of concern within representation phase is the modeling of dependencies between identified human errors. It is intricate and relatively underdeveloped area of HRA, but it can have dramatic effects on the level of risk calculated in a PSA.
- *Human Error Reliability Quantification* – is rather developed part of the HRA process. There is a plethora of tools available in the public domain for the purpose, and thus entirely accessible to practitioners.
- *Impact assessment* – when the errors are represented and quantified, it is possible to carry out PSA risk calculations and to determine the overall system risk. If the system is found not to be acceptably safe, it is necessary to reduce risk to an acceptable level. Sometimes, the exact human error is being identified as a dominant factor in undesirably high risk levels.
- *Human Error Reduction* – is performed if the impact of human error on the risk level in the system is found to be significant. Error reduction mechanisms can be based on information obtained from the task analysis, on the identified causes of the human error, or on the Performance Shaping Factors used during the quantification phase. Reduction measures can be achieved either by engineering design, or by blocking the system to protect the operators and the environment from the consequences of the human/hardware failure combinations.
- *Quality assurance and documentation* – is the final phase of the HRA process. All assumptions and findings made by the assessor should be documented and clearly exposed to the management team which is running the system. This is of particular importance if error reduction mechanisms are proposed.

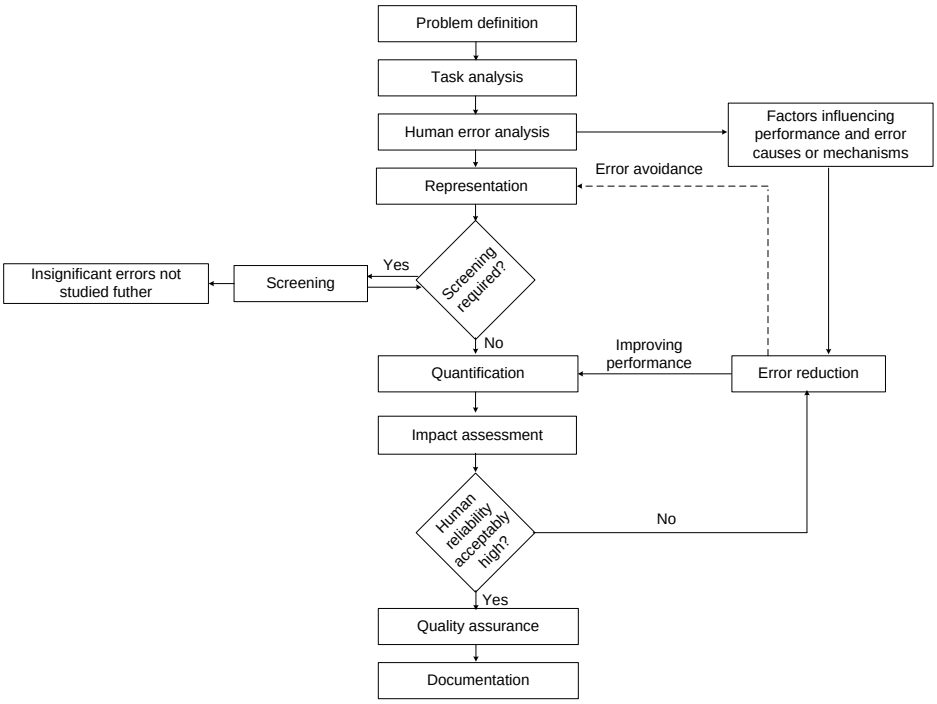

Fig. 2 The HRA process [3]

5. CONCLUSION

The assessments of the impacts of different anthropogenic activities require innovative approaches that allow risks comparison and that comprise all the possible risk interactions. It is always useful to put forward some basic principles for cumulative risk assessment. The principal issue should be how to overcome the problem of making different hazards comparable. Another one should be to find out how and when the possible interactions among different threats may become significant.

A new approach is needed for exploration and monitoring migrations of harmful substances from manufacturing sites and waste collection areas. Characteristics of the emissions and their interaction with water and soil/sediment should be assessed through appropriate analyses and modeling. In addition, monitoring and field measurement equipment, operators' reliability and data processing methods should be regularly assessed to provide risk free operation.

Comprehensive researches are needed to evaluate and test new methods for environmental monitoring, modeling and human-error-based risk assessment. The ultimate goal is to enhance environmentally sustainable manufacturing by characterizing and quantifying the anthropogenic emissions, modeling reactions and pathways of contaminants, and assessing the health, safety and environmental risks.

Acknowledgement. *This paper is a part of the research done within the projects III 43014 financed by the Ministry of Education, Science and Technological Development of the Republic of Serbia.*

REFERENCES

1. Grozdanovic, M. and Stojiljkovic, E.: *Risk Assessment Methods*. Nis: University of Nis, Faculty of Occupational Safety, 2013 (in Serbian).
2. Haugen, S. and Øien, K.: *Risk Analysis Application – HRA*. Trondheim, Norway: NTNU, 2009.
3. Kirwan, B.: *A Guide to Practical Human Reliability Assessment*. London, UK: Taylor & Francis, 1994.
4. Perrow, C.: *Normal accidents: Living with high risk technologies*. New York: Basic Books, Inc., 1984.
5. Rausand, M.: *Risk Assessment: Theory, Methods, and Applications*. New Jersey: John Wiley & Sons, Inc. Hoboken, 2011.
6. Stojiljkovic, E.: Methodological Framework for Human Error Assessment. *Ph.D. Thesis.* Nis: University of Nis, Faculty of Occupational Safety, 2011 (in Serbian).
7. Swain A. D.: Comparative evaluation methods for human reliability analysis. *Report No. GRS-71*. Köln, Germany: Gessellschaft für Reaktorsicherheit, 1989.
8. Swain, A. D.: Human reliability analysis: Need, status, trends and limitations. *Reliability Engineering and System Safety*, Vol. 29, No 3, pp. 301-13, 1990.

ZNAČAJ ANALIZE LJUDSKE POUZDANOSTI U PROCENI RIZIKA INDUSTRIJSKIH I MONITORING SISTEMA ŽIVOTNE SREDINE

U analizi industrijskih zaštitnih sistema, procedure procene rizika pre svega se sprovode radi poboljšanja mera zaštite ljudi i opreme. Međutim, ekološke posledice velikih industrijskih akcidenata jasno ukazuju da se procena ekološke bezbednosti ne sme zanemariti i mora se posmatrati kao deo celokupnog procesa procene rizika. Dokazano je da je veliki broj industrijskih akcidenata prouzrokovan neadekvatnim aktivnostima (ili propustima) nadležnih operatera. Prema tome, procena ljudskih grešaka se mora razmatrati i kao važan deo ekološke bezbednosti u industrijskim i infrastrukturnim sistemima.

Preliminarna istraživanja najnovijih događaja nagoveštavaju da su se neke ozbiljne posledice prirodnih katastrofa mogle delimično ublažiti da su podaci iz monitoring sistema životne sredine u kombinaciji sa upozorenjima iz industrijskih sistema bili na raspolaganju za pravilno postupanje donosicima odluka na različitim hijerarhijskim nivoima. Neki propusti mogu se pripisati strukturi sistema nastaloj u ranijim fazama razvoja, dok su neki drugi u potpunosti u domenu nepravilne komunikacije ili nedostatka adekvatnog i pravovremenog reagovanja.

Standardne tehnike, metode i alati za procenu rizika po bezbednost i zdravlje na radu, za procenu ekološkog rizika i procenu ljudske pouzdanosti razvijaju su već godinama. Međutim, uvek ima prostora za njihovo poboljšanje u pogledu integracije, kvaliteta i sveobuhvatnosti.

Ovaj rad nastoji da opiše mogućnosti kombinovanja i/ili integrisanja standardnih procedura sa ciljem poboljšanja rezultata procene rizika i bezbednosnih performansi posmatranih sistema. U radu su prikazane osnove metodološkog okvira za procenu ljudske pouzdanosti, a analiza ljudskih grešaka istaknuta je kao važan element postupka procene rizika.

Ključne reči: *procena rizika, analiza ljudske pouzdanosti, monitoring životne sredine.*