Some Aspects Regarding Human Error Assessment in Resilient Socio-Technical Systems

GABRIELA TONŢ1, LUIGE VLĂDĂREANU2, RADU ADRIAN MUNTEANU3, DAN GEORGE TONŢ1

1Department of Electrical Engineering, Measurements and Electric Power Use, Faculty of Electrical Engineering and Information Technology, University of Oradea, Universităţii st., no. 1, zip code 410087, Oradea, ROMÂNIA, dtont@uoradea.ro, gtont@uoradea.ro, http://www.uoradea.ro
2Institute of Solid Mechanics of Romanian Academy, C-tin Mille 15, Bucharest 1, 010141, ROMÂNIA, luigiv@arexim.ro, http://www.acad.ro
3Faculty of Electrical Engineering, Technical University Cluj Napoca, Constantin Daicoviciu st. no 15, 400020 Cluj - Napoca, ROMÂNIA, radu.a.munteanu@mas.utcluj.ro, http://www.utcluj.ro/

Abstract: -The paper focuses on a human reliability analysis (HRA) that provides estimates of relative frequencies for human errors in particular critical tasks, highlighting the exposed areas of the system in which the improvements will be beneficial. The dynamic field of human reliability analysis assesses the performance shaping factors in the context of explicitly interactions of teams or individuals in operational regime. The errors are approached through the means of sociotechnical probabilistic risk assessment. Beside the available time for effective human action, variables affecting human performance are identified, including stress, workload, training and quality of procedures, system feedback.

Key-Words: - Risk, sociotechnical system, human factor qualitative, quantitative analysis

1 Introduction

The concept of human reliability represents a continuation of the technical reliability, the idea arising because of the existence and nature of human-machine systems (sociotechnical systems.). The sociotechnical system is a concept that reflects the integrative vision on an item or group of elements that have human, technical and economic features and is represented by any system that allows the taking, storage, processing, conversion of resources into goods or services with economic relevance and includes human, technical and technological elements. The constructive elements (input – process – output – feedback loops – feedforward loops) of sociotechnical systems create interdependencies with other systems or individual elements [1, 3]. Links may be physical or informational. Systemic approach of the economical entity (enterprise, firm, organization) emphasizes the interdependence between its components determining the leading influence of each element on other and, on business in general. Based on the concept of system and cybernetic system, systemic approach has the following main advantages:

- is a means of global approach of economic, social, environmental and technical aspects revealing the interconditionality and tuning of processes;
- through mathematical modeling highlights the qualitative and quantitative relationship between components of economical entity, allowing to find efficient, operational solutions for complex problems;
- allows an optimal balance between the components in terms of permanent reporting to the exogenous variables of economical entity (market, competition, technology, resources, the legal and political systems).

The concept of system appears, in embryonic form, in Greek philosophy, with the remark of Aristotle that "the whole is more than the sum of its parts", evolves over time and reaches its present form in the beginning of 21 century. The system can be approached as any section of reality in which are identified a set of phenomena, objects, processes, finite concepts or groups interconnected through a set of reciprocal relationships and orderly acts in common to achieve objectives well defined, defaulted through a plan. This depiction integrates the three essential elements: a goal that motivates the design and the existence of the system, a certain
organization (order) of its elements, the supplying with information, energy and materials of its elements in order to achieve the objectives. The set of relations between system components and relationships between components and the whole form the structure of the system [2]. The set of system characteristics at a given time determine its status. Any system is an integrated whole of its elements, being operational only when a number of elements begin to interact between them. The compliance of the concept is based on the following regarded as being the characteristics:

- connection between the elements of the whole and the system is stronger than links of the system with the environment;
- any system, regardless of complexity is a subsystem of a more comprehensive;
- the nature and complexity of a system requires a certain organization of its elements to operate as a system;
- any system is characterized by a certain structure, it can be regarded as such, i.e. the exact connection of all subsystems to the smallest components, or be seen by following the different characteristic structures;

Any system can have a multitude of response loop which can be closed on certain parts of the system or even the whole system. The concept of human reliability is so closely related to that error, hence the conclusion that human error identification and analysis becomes essential for assessing human reliability [4, 10, 11].

2 Risk analysis techniques

Risk assessment is a structured approach for identifying hazards, analyzing risk, and identifying risk reduction measures. Properly implemented in an organization that follows a long-term risk management process, it provides a cost-effective basis for maintaining risk within appropriate. In the sociotechnical systems, the technical and human components are considered interdisciplinary to include in risk assessment, human factors analysis and uncertainty analysis. Human performance modeling analysis based on logic model may utilize qualitative techniques if discrete or sufficient credible data required for quantitative assessments are unavailable, or if obtaining or analyzing data is not cost-effective. As the analysis is extended, it produces models of the scenarios, calculations of the frequencies of particular events, result, and estimates of specific consequences socioeconomic impacts. These outputs become more quantitative and the uncertainty of the results is narrowed as more detailed information is developed. Assessment of socioeconomic impacts and human factors evaluation rely on assumptions based on the best available data, uncertainties properly described, and analyses with the appropriate rigor for the level of assessment [6]. Experience from prior risk studies including human factor and expert opinion provide a sense of the confidence warranted in the characterization of risks and justifying the findings. For a holistic, integrative approach, risk analysis should include the use of hybrid modeling methods for risk scenarios, more detailed causal modeling, consideration of human factors and adoption of human-error analysis techniques, evaluation of rare high-consequence events, advanced modeling formal use of expert opinion and rigorous uncertainty and sensitivity analyses. Summary measures of risk presented in qualitative, semiquantitative, and quantitative formats, becoming more quantitative as the level of analysis deepens [7, 9].

The overall approach generally comprises the following steps (Fig.1):

- Hazard identification,
- Risk analysis,
- Risk control options,
- Cost–benefit assessment, and
- Recommendations for decision making

![Fig.1 Risk assessment framework in Formal Safety Assessment (FSA) approach](image-url)

The choice of techniques is influenced by the nature of the available information and the precision necessary to determine a credible risk value. Figure 2 illustrates how qualitative or quantitative techniques can be used for risk analysis (ABS 2000). Regardless of the techniques chosen, the goal of the analysis remains the same: to derive estimations of risk and to provide detail sufficient for examining risk reduction measures that can achieve a tolerable level of risk. The output of the risk analysis should be a refined characterization of
scenarios, their likelihood, and their consequences, allowing risks to be ranked in order of consideration for risk control options.

Another means, known as safety culture, has been introduced in the nuclear work domain and is being adopted in a number of other high-risk, industries (e.g., medical, aeronautics). A detailed explanation of this concept is beyond the scope of this book but, suffice it to say, it actively encourages a proactive approach to continuous improvement. It promote the active engagement of staff at all levels to enhance operations, in particular by identifying and removing technical and organizational problems even though they may not have yet led to an incident or accident. A good safety culture is a powerful tool in achieving a safer and more productive facility by actively searching out and removing latent and active problems, including organizational issues such as poor communication or work coordination.

3 Literature Review on Human Reliability Assessment

Human error has been credited as a contributing factor in most accidents that have occurred in high-risk domains. To try to understand why human error occurs, it is first necessary to identify the types of errors that can be made.

One popular error, which has proven to be a useful tool to reduce human error, classifies errors as being either slips or mistakes. The error of omission corresponds to the case where the operator carries out a well-known task but somehow omits one of the steps or performs a wrong one. Mistakes (or errors of commission) occur when either the operator does not know how to do something, and must therefore improvise, or when the environment leads down the wrong path. Slips may be mitigated by building error-prevention mechanisms, providing decision support functionality, and training the operator to distinguish between normal and abnormal situations. Another tool for approaching human error in complex systems has been to use a notion known as latent pathogen. A latent pathogen is an error, be it technical, social, or otherwise, that exists in a dormant state in a system and is normally well-tolerated by the system. Examples of latent pathogens are deficient operating procedures, plant configuration errors, and risky, but usually tolerated, operating practices. Latent pathogens originate from a number of sources, but have most often been related to maintenance activities in process control applications. There are various means used to control latent pathogens - such as work planning and control for maintenance and continuous improvement programs - and, where possible, to eliminate latent pathogens on a continuing basis.

4 Human Reliability Assessment Methods

The human reliability assessment (HRA) uses systems engineering and behavioral science methods in order to render a complete description of the human contribution to risk and to identify ways to reduce that risk.

The first generation of HRA uses an event tree representation called probability tree diagram as a modeling tool of an accident sequence based on the simplified model in fig. 3.

Another means to analyze human reliability is a straightforward extension of probabilistic risk assessment (PRA) because in the same way that equipment can fail in a plant, so can a human operator commit errors. In both cases, an analysis (functional decomposition for equipment and task analysis for humans) would articulate a level of detail for which failure or error probabilities can be assigned. This basic idea is behind the Technique for Human Error Rate Prediction (THERP) (Swain & Guttman, 1983). THERP is intended to generate human error probabilities that would be incorporated into a PRA. The Accident Sequence Evaluation Program (ASEP) Human Reliability Procedure is a simplified form of THERP; an associated computational tool is Simplified Human Error Analysis Code (SHEAN) (Wilson, 1993). More
recently, the US Nuclear Regulatory Commission has published the Standardized Plant Analysis Risk (SPAR) human reliability analysis method also because of human error (SPAR-H) (Gertman et al., 2005). All methods have successfully accounted for contribution of human performance to overall risk and reliability allowing quantification of human error probability, being applied extensively to nuclear power plants, and some to the space domain. The first characteristic of 2nd generation of HRA identified is that the central position of the context in predicting and explaining human failures: failures are triggered by an error-forcing context. The second characteristic is that the operator’s cognition must be considered in order to identify what failures the context may trigger; i.e., the context may trigger error-mechanisms if the human’s information processing capacity is exceeded or if the strategies and methods humans apply in solving problems does not fit to the requirements of the task. The approach for the second generation of HRA methods is framed in the fig. 4.

Fig. 4 Second generation of HRA processing modeling flow

CREAM – Cognitive Reliability and Error Analysis Method CREAM (Cognitive Reliability and Error Analysis Method) is a specific proposal for a second generation HRA. CREAM will enable an analyst to achieve the following:
- Identify those parts of the work, as tasks or actions, that require or depend on human cognition, and which therefore may be affected by variations in cognitive reliability;
- Determine the conditions under which the reliability of cognition may be reduced, and where therefore these tasks or actions may constitute a source of risk;
- Provide an assessment of the consequences of human performance on system safety which can be used in a probabilistic risk assessment (PRA) and probabilistic safety assessment (PSA);
- Develop and specify modifications that improve these conditions, hence serve to increase the reliability of cognition and reduce the risk.
Steps 1 - 3 are the core of CREAM. Step 4 serves the purpose of ensuring that the proper conclusions are drawn from the analysis, and that the necessary changes to the system are correctly specified [4].

CREAM can be used in several different ways: as a stand-alone analysis method, for either retrospective or prospective analyses, using a consistent taxonomy for error modes and error causes, as part of a larger design method for complex, interactive systems, as an HRA in the context of an Integrated Safety Analysis (ISA) or Probabilistic Safety Analysis (PSA). CREAM provides the core functionality of these services, i.e., the concepts, the classification system, the cognitive models, and the methods. In order to be properly used it is necessary to supplement with application or plant specific information, e.g. in the form of values for specific performance parameters, detailed operational and process knowledge that defines the context [5].

Human Error Assessment and Reduction Technique (HEART) was developed by Williams in 1986. It assumes that basic human reliability is dependent upon the generic nature of the task to be performed. HEART also assumes that any predicted reliability of task performance may be expected to change as a function of the extent to which identified Error Producing Conditions (EPC) might apply.

5 Human Cognitive Reliability
Three Performance Shaping Factors (PSFs) – Operator Experience, Stress Level, and Quality of Operator/Plant Interface influence the average (median) time taken to perform the task [1]. Combining these factors enables response-time curves to be calibrated and compared to the available time to perform the task. Using these curves, the analyst can then estimate the likelihood that an operator will take the correct action, as required by a given stimulus (e.g. pressure warning signal), within the available time window. The relationship between these normalised times and Human Error Probabilities (HEPs) is based on simulator experimental data.

The HCR methodology is broken into a sequence of steps as given below:
The first step is for the analyst to determine the situation in need of a human reliability assessment. The median response time to perform the task in question is thereafter determined. This is done by expert judgment, operator interview or simulator experiment. In literature, this time is referred to as \( T_{1/2 \text{ nominal}} \).
The median response time, \( T_{1/2} \), requires to be revised to make it specific to the situational context. This is done by means of the PSF coefficients \( K_i \).
(Operator Experience), $K_2$ (Stress Level) and $K_3$ (Quality of Operator/Plant Interface) given in the literature and using the following formula:

$$T_{1/2} = T_{1/2}^\text{nominal} \times (1 + K_1)(1 + K_2)(1 + K_3)$$  \hspace{1cm} (1)

Performance improving PSFs (e.g. worker experience, low stress) will take negative values resulting in quicker times, whilst performance inhibiting PSFs (e.g. poor interface) will increase this adjusted median time.

5. For the action being assessed, the time window ($T$) should then be calculated, which is the time in which the operator must take action to correctly resolve the situation.

6. To obtain the non-response probability, the time window ($T$) is divided by $T_{1/2}$, the median time. This gives the normalised time value. A simplified version of the cognitive model is shown below in fig. 5. [6].

$$HEP = Fr(T_A > T_C) = \int_0^\infty f_{T_A}(t)[1 - F_{T_A}(t)]dt \hspace{1cm} (2)$$

where $f_{T_C}$ is the probability density function for the stochastic variability of the critical time ($T_C$) and $F_{T_A}$ denotes the cumulative probability distribution for the stochastic variability of operator response time ($T_A$), [11]. The lognormal approximation for the input in the fault tree with these estimated HEPs was evaluated. The goodness of fit tests accept the model for the lognormal distribution for the measurements of the operator response time ($T_A$) in the case of heat and cooling agents transport system failure, samples size =500 measurements, $\sigma=1.0272$ and $\mu=0.96076$ where: $\sigma$ is the scale parameter of the included normal distribution and $\mu$ is the location parameter of the included normal distribution (table 1).

### Table 1 Goodness-of-fit of the operator response time ($T_A$) in the case of heat and cooling agents transport system failure

<table>
<thead>
<tr>
<th>Goodness-of-fit</th>
<th>Kolmogorov-Smirnov</th>
<th>Anderson-Darling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null Hypothesis (H0)</td>
<td>$\alpha$ Conclusion</td>
<td>$\alpha$ Conclusion</td>
</tr>
<tr>
<td>Lognormal distribution</td>
<td>0.90 Accept H0</td>
<td>1.64 Accept H0</td>
</tr>
</tbody>
</table>

Fig. 5 The cognitive model

Fig. 6 Fault tree of the heat and cooling agents transport system

The application of this concept in human reliability is that the success or failure of the operator action in any circumstance is governed by the critical time ($T_C$) available for that response (i.e., before an undesired event occurs) and the time ($T_A$) required for the correct diagnosis of the situation and execution of the required action [6], as illustrated in fig. 7. These two competing times are random variables that human error probability (HEP) can be defined as the fraction of the time that $T_A$ is greater than $T_C$ as in relation (2)
The estimated human error probabilities for lognormal distribution of operator response time is presented in table 2.

Table 2 The estimated human error probabilities

<table>
<thead>
<tr>
<th>σ [min]</th>
<th>μ [min]</th>
<th>Mean</th>
<th>Median</th>
<th>Variance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>244.960</td>
<td>54.590</td>
<td>1.2088</td>
</tr>
</tbody>
</table>

Fig. 7. Estimated human error probabilities

The graphical representation of for lognormal distribution of operator response time depending on the sample size is presented in fig. 7.

7 Conclusion

Applying probabilistic risk assessment (PRA), on the fault tree was revealed probability of the best of circumstances, probability assessment models are subject to missed failure paths, poor characterized dependencies between errors, and misestimated failure rates. The difficulties of applying PRA methodology appears in the attempt to use the operational experience to assess a failure probability, experience may or may not be unique. Human performance can be enhanced through appropriate skill-based and rule-based training and refined by knowledge-based education. Taking into account the inherent limitations of the probabilistic risk assessment methodology offers advantages over risk.

References: