Human reliability analysis in power engineering

František Janíček
Zoltán Kovács
Emil Krondiak
Matej Korec

Abstract
The human reliability analysis is a study of the interactions between the humans (or system operators and maintainers) and the system and an attempt to predict the impact of such interactions on the system reliability. The purpose of this paper is to describe how to perform human reliability analysis in the context of PSA (Probabilistic Safety Assessment) for power engineering.

Key words: human error probability, initiating event, error of commission, error of omission

Introduction

The reliability of the power system depends on how it is planned, maintained, and operated. A critical part of the overall reliability design and assessment process is the criteria used to specify levels of reliability and those levels which are acceptable versus those which are unacceptable. One feature of present and past reliability criteria is that they are deterministic. An important implication of this feature is that power systems are required to withstand classes of outages with a specified limit on the consequence. For example, a common criterion, called n-1, is that for loss of a single element (e.g., a transmission circuit), the system performance must be acceptable. Acceptability of post-outage system performance generally means that no load interruption or equipment damage will occur.

The deterministic approach described above has been appropriate in the past because the industry could afford to operate its system in a very conservative manner, and deterministic limits were not routinely met in typical operating environments. Now, however, the competitive electric energy marketplace has caused an increase in the amount of long distance transmission usage. This has resulted in full utilization of existing equipment and stressed operating conditions, and transmission availability has become scarce. As a result, deterministic reliability criteria are no longer entirely adequate. There are two reasons for this:

1) Non-uniformity because the deterministic criteria are inherently non-uniform. In some cases, they result in a highly conservative operating or planning decision. In others, their application results in a very risky decision.

2) Economic concerns because the deterministic criteria do not easily translate into the economic language of today's marketplace. This deficiency is much more troublesome today than in previous years. Previously, utilities could rely on a mutually shared feeling of obligation to maintain system reliability. Today, it is almost universal that money is spent only in so far as it will contribute to profits. Inability to economically quantify reliability means that it will be ignored, at worst, or incorrectly assessed, at best.

A solution to the problems associated with use of deterministic reliability criteria in a competitive electric energy marketplace is to use PSA. This approach to decision making is heavily used in other industries such as nuclear and chemical industry. It is appropriate for use in power system reliability analysis because of the inherent stochastic nature of the problem, where a fundamental requirement is to predict the future, which cannot be done deterministically.

For complex systems such as power engineering, which involve a large number of human-system interactions, HRA (Human Reliability Analysis) becomes an important element of PSA to ensure a realistic assessment of safety. Examples of human interactions include: errors during installation, test, and maintenance of equipment, interactions during accidents, etc. The HRA analysts, with support from systems analysts, model and quantify these human interactions, which then will be incorporated as human basic events into the PSA logic models (e.g., event trees and fault trees).

Many classifications of human errors have been proposed in HRA literature. The proposed classifications consider different aspects of such as their timing with respect to the initiating event, human error type, and cognitive behavior of humans responding to accidents. Similar to hardware reliability modeling (e.g., failure on demand, running failure, etc.), classification of human actions is a key step in HRA that supports PSA model development, data collection, and quantification.

This paper describes types of human errors, task analysis and HRA models. An example is presented for HEP calculation which can be performed to support PSA activities.

1. Types of Human Errors

Human actions can affect safety or risk in various ways. It is important to be able to relate them to PSA structure to understand their potential effect on risk or safety. Three categories of actions can be defined which facilitate the incorporation of HRA studies into PSA structure:

- category A actions that cause equipment or systems to be unavailable (pre-accident human errors as maintenance errors, testing errors, calibration errors),
- category B actions that either by themselves or in combination with equipment failures lead directly to initiating events (human errors causing system trip or loss of power, etc.).
- category C actions occurring post-initiating event. These can either occur in the performance of safety actions or can be actions that aggravate the fault sequence (post-accident human errors also, called emergency actions actuating a manual safety system, backing up an automatic system). Type C actions are broken into two main elements of cognitive response and action (or execution) response. Cognitive response is a human action to perform correct detection (recognizing abnormal event), diagnosis and decision making to initiate a response within time available; and post-diagnosis action response to perform correct actions (or tasks execution) after the correct diagnosis has been made, within time available. Sometimes, the cognitive response is simply referred to as diagnosis failure or misdiagnosis.

In an attempt to simplify the complex human cognitive behavior, there are proposed three categories of human cognitive behavior as follows: 1) skill-based response requiring little or no cognitive effort, 2) rule-based response driven by procedures or rules, and 3) knowledge-based response requiring problem solving and decision making.

Skill-based behavior is characterized by a quasi-instinctive response of the operator. It occurs when an operator is well trained on a particular task, independent of the level of complexity of the task. It is characterized by a fast performance and a low number of errors.

Rule-based behavior is encountered when an operator's actions are governed by a set of well-known rules, which he follows. The major difference between skill-based and rule-based behavior is in the degree of practice of rules. Since the rules need to be checked, the response of the operator is slower and more prone to errors.

Knowledge-based behavior is characteristic of unfamiliar or ambiguous situations. In such case, the operator will need to rely on his or her own knowledge of the system and situation. Knowledge-based behavior is the most error prone of the three types of behavior.

Two types of human error modes have been defined: 1) error of omission which is an error to initiate performance of a system required task (skipping a procedural step or an entire task), and 2) error of commission which is incorrect performance of a system required task, given that a task is attempted, or the performance of some extraneous task that is not required by the system and that has the potential for contributing to a system failure (selection of a wrong control, sequence error, timing error).

Category A human interactions are explicitly modeled and are usually included in the system fault trees at the component level. Category B human interactions are usually included in the database for assessing initiating event frequencies and usually do not require explicit modeling. One exception is that, if an fault tree is developed to assess a specific initiating event frequency (such as loss of power) then human errors causing the initiating event to occur are explicitly modeled in the initiator logic model. Category C human interactions are explicitly modeled and can be included at different levels of logic model: 1) in fault trees as simple manual backup responses to automatic safety systems failure, 2) in event trees as manual actions in response to accidents such as starting manual safety systems as identified in emergency procedures, and 3) in accident sequence cut sets as, recovery actions by using alternate equipment or repairing failed equipment.

2. Task Analysis

The task analysis is an analytical process for determining the specific behaviors required of the human performance in a system. It involves determining the detailed performance required of people and equipment and the effects of environmental conditions, malfunctions, and other unexpected events on both. Within each task to be performed by people, behavioral steps are analyzed in terms of 1) the sensory signals and related perceptions, 2) information processing, decision-making, memory storage, and other mental processes, and 3) the required responses. The level of detail in a task analysis should match the requirements for the level of human reliability analysis of interest. A screening analysis requires considerably less task analysis than a nominal analysis.

Many factors influence human performance in complex systems. These factors are called PSFs (Performance Shaping Factors). They can affect human performance in a positive (help performance) or negative (hinder performance) manner. PSFs can be broadly grouped into two types: 1) external PSFs that are external to the operators, such as task complexity, human-machine interface, written procedures, work environment, stress, and management and organizational factors and 2) internal PSFs that may be part of operators' internal characteristics, such as operator training, experience, and familiarity with task, health, and motivation.

There is not a universally accepted set of PSFs in HRA literature. However, typical PSFs considered in an HRA are as follows:

1. quality of procedures,
2. quality of human-machine interface (indications, control aids),
3. operator training practice,
4. task complexity (skill, rule and knowledge-based for cognitive response),
5. operator stress level,
6. time available,
7. environmental conditions (e.g., lighting, temperature, radiation, noise, gravity force),
8. communication between operating personnel and
9. previous actions.

The systems and the HRA analysts may identify a large number of human interactions in a PSA. Detailed task analysis, required for quantification is a time consuming and resource intensive task. It may not be possible, or necessary, to perform detailed quantification for all human interactions. Therefore, for practical reasons quantification in HRA is usually performed in two phases: screening analysis and detailed analysis.

The purpose of the screening analysis is to reduce the number of actions to be analyzed in detail in HRA. The screening analysis may be qualitative, quantitative, or a combination of both. Qualitative screening is usually performed early in HRA to exclude some human actions from further analysis and, hence, not to incorporate them into the PSA logic models. A set of qualitative screening rules is developed for each human action type. Examples of qualitative screening rules are as follows: 1) screen out misaligned equipment as a result of a test or maintenance error, when by design automatic re-alignment of equipment occurs on demand or full functional test is performed after maintenance, 2) screen out misaligned equipment as a result of a human error, when equipment status is indicated in the control room, 3) screen out human actions if its success or

failure has no influence on accident progression, e.g., verification tasks, 4) screen out human actions if there are physical limitations to carry out the task, e.g., time too short, impossible access due to hostile environment, lack of proper tools, 5) screen out human actions if operators are unlikely or reluctant to perform the action, e.g., training focuses on other priorities or performing the task may be perceived to have serious economical impact.

Quantitative screening is performed to limit the detailed task analysis and quantification to important (risk-significant) human actions. Conservative human error probabilities are used in the PSA logic models to perform initial quantification. Human actions that are shown to have insignificant impact on risk (do not appear in dominant accident sequence cut sets) are screened out from further detailed analysis. The key elements of a coarse screening analysis are as follows. Conservative human error probabilities (HEPs) typically in the range of 0.1 to 1.0 are used for various actions depending on their complexity and timing as well as operators' familiarity with them. Usually, no recovery factors are considered. Complete dependence is assumed among multiple related actions that appear in the same accident sequence cut set, i.e., if operator fails on the first action with an estimated HEP, then the HEPs on the second and third (and so on) related actions are unity.

Detailed analysis is performed for human actions that survived the screening analysis. Based on task analysis and availability of human performance data experts, the purpose is to select an HRA model, assess the HEPs, and incorporate them as human basic events into the PSA logic models (fault trees, event trees or accident sequence cut sets). In principle, one can quantify the human basic events or HEPs using any of the probability distributions if sufficient actuarial or experimental data on human error is available, and if one of the distributions is found to fit the data set. However, due to lack of such data, specific human reliability models have been developed to quantify errors. These models have been mainly developed for the nuclear industry, and one should be cautious in extending their applicability to the power engineering.

3. HRA Models

There are a number of HRA methods developed over the years to mainly support PSA studies for nuclear power plants. Some new HRA methods are also under development. One common feature of all these models is their dependency on expert judgment due to lack of human error data, particularly for category C human actions. HRA methods are:

1. Technique for Human Error Rate Prediction (THERP)
2. Success Likelihood Index Methodology was developed to quantify human errors included in PSAs (especially category C human errors),
3. Time Reliability Curve (TRC) with general applicability to nuclear and non-nuclear applications,
4. Human Cognitive Reliability (HCR) model (mainly for nuclear power PSAs; may be used in non-nuclear applications),
5. Decision Tree method with general applicability to nuclear and non-nuclear applications),
6. Human Error Assessment and Reduction Technique mainly for nuclear power PSRAs) and
7. A Technique for Human Error Analysis under development for nuclear power PRAs.

TRCs, in general, can be used for quantification of any time-dependent human action, given availability of data on operator response time. The HCR model consists of three special TRCs for quantification of three types of human cognitive behavior response (i.e., skill, rule, and knowledge-based behaviors). Since HCR model parameters were mainly based on data from small scale tests that represented three categories of human cognitive behaviors, and also the TRCs are normalized (they depend on both available time window and crew median response time), one may be able to apply it to power engineering PSA studies.

4. The Example

HEP is calculated using THERP method for manipulation of circuit breakers from the control room of substation.

A human error occurs when there is failure of either the cognitive or the manual part of a human action and the consequence of the failure is detrimental to safety. Thus, a general mathematical model for quantifying post-initiator and recovery human errors is given by:

$$Pr\{HE\} = Pr\{C\} + Pr\{M\} - Pr\{C\}Pr\{M\} \quad (1)$$

In this example Pr(C) = 0, than Pr(HE) = Pr(M).

Mathematically, the simplified THERP model may be expressed as:

$$Pr\{M\} = BHEPxF_{CREW}xF_{STRESS} \quad (2)$$

The BHEP value is assumed to equal the screening value of the manual error from THERP. The detailed analysis of manual errors included PSFs for the redundancy within the crew (the so-called „crew factor" or and the psychological stress level .

The crew factor addresses the probability that a manual error may be prevented or recovered due to redundancy among the staff. For example, it may be required to perform a certain action (manipulation of circuit breakers from the control room of substation); if operator makes an error (for example, by selecting the wrong circuit breaker), the other persons may notice the error and take corrective action (by instructing the operator). The crew factor is computed by multiplying factors for each person in the control room:

$$F_{CREW} = F_1xF_2xF_3xF_4 \quad (3)$$

In this equation, F1 denotes the factor for the operator, F2 - F4 denotes the factor of other persons present in the control room. The individual factors are based on an assessment of the degree of dependency between the various crew members:

F_i (i = 1, 2, 3, 4)	Degree of Dependency
1	Not applicable – operator whose dependency is being assessed is the one performing the action.
1	Not involved – operator does not perform the action and does not monitor its execution.
0.5	High – operator does not perform the action, but is closely associated with its execution.
0.14	Medium – operator does not perform the action, but is somewhat associated with its execution.
0.05	Low – operator does not perform the action, but monitors its execution as an independent observer.

Values for the psychological stress level factor (F_{STRESS}) are:

F_{STRESS}	Stress Level	Characteristics
2	Very low task load	Simple or repetitive tasks in which the operator may become distracted or careless.
1	Optimal, step-by-step	Tasks involving a set of sequential actions, characterised by a task load that is within normal human physical capabilities (the pace of actions is not too fast, there is adequate lighting, etc.). There is a large margin between the current plant situation and a serious emergency condition. The operator is relatively unemotional (not worried, anxious, or confused).
1	Optimal, dynamic	Tasks involving a set of complex actions (including feedback and/or self-regulating functions), characterised by a task load that is within normal human physical capabilities. There is a large margin between the current plant situation and a serious emergency condition. The operator is relatively unemotional.
2	Heavy, step-by-step	Tasks involving a set of sequential actions, characterised by a task load that approaches the limits of human physical capabilities (the pace of actions is very fast, there is poor lighting, etc.). There is a little margin between the current plant situation and a serious emergency condition. The operator is relatively emotional (worried about his personal well-being and the plant's safety and/or confused).
5	Heavy, dynamic	Tasks involving a set of complex actions (including feedback and/or self-regulating functions), characterised by a task load that approaches the limits of human physical capabilities. There is a little margin between the current plant situation and a serious emergency condition. The operator is relatively emotional.

The results of calculation are summarised in table 4.1.

Manual contribution				
Basic human error probability, BHEP =		1.00E-01		
Description				Value
F1		Not applicable		1
F2		Not applicable		1
F3		Medium		0.14
F4		Medium		0.14
Crew Factor, F_{CREW} = F1 x F2 x F3 x F4 =		1.96E-02		
Psych. stress level factor, F_{STRESS}	heavy, step by step	2	EF - error factor =	5
SIGMA = ln(EF)/1.645 =		0.98	Mean /exp (SIGMA**2/2) =	2.43E-03
Probability of manual error - P(M) = BHEP x F_{CREW} x F_{stress} =		**3.92E-03**		
95th percentile = median x EF input =		**1.21E-02**		
5th percentile = median / EF input =		**4.86E-04**		
Error Factor = EXTRACTION(95th/5th) =		**5.00E+00**		
Human error probability				
Total error probability (without truncation)	**P(HE) = P(C) + P(M) - P(C) x P(M) =**	**3.93E-03**		
EF =		**8.74E+00**		

Tab. 4.1 Calculation of human error probability

5. Conclusion

In PSA, one must identify the events of concern and quantify their probability and cost-consequence. Philosophically, the main difference between a PSA approach to reliability assessment and the present day deterministic one is that PSA assesses probability and cost-consequence quantitatively. The deterministic approach does so in only a qualitative way. In addition to component reliability analysis detailed HRA is needed to support PSA activities. Then the risk can be quantified.

Because PSA quantifies the risk also in financial units, it provides a uniform assessment basis that is compatible with economic decision making. As a result, PSA can be used to

distinguish good risks from bad ones and consequently more effectively identify the optimal planning or operating decision. In addition, PSA reliability assessment is attractive because it is capable of quantifying not only the risk associated with single, credible events, but also that associated with catastrophic events, normally classified as a low probability, high consequence event.

Failure or mis-operation of system protection is normally unlikely (and deterministic studies normally assume it is completely unlikely), but its occurrence can be extremely costly. PSA can quantify its risk and also provide guidance regarding how to mitigate it. A final attractive feature of PSA is that it also enables calculation of variance. This quantity is an essential quantity for good decision making. Whereas the risk is the average value given the event occurs many times, the fact that most reliability events occur infrequently requires that we also quantify the amount of uncertainty regarding the outcome. Thus, the average together with how far we can expect the actual value to deviate from the average can provide useful information into the decision making process.

References

[1] Janíček, F., et all: Obnoviteľné zdroje 1. Technológie pre udržateľnú budúcnosť. Bratislava : FEI STU, 2007. ISBN 978-80-969777-0-3. (in Slovak)

[2] Banas, I., Mucha, Martin: Využitie ATP na simuláciu vn linky ZSE a.s. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Roč. 13, č. 1 (2007), s. 32-35. (in Slovak)

[3] Eleschová, Ž., Beláň, A.: Metódy posúdenia statickej stability elektrizačnej sústavy. EE - časopis pre elektrotechniku a energetiku, mimoriadne číslo, 2007. ISSN 1335-2547.

[4] Janíček, F., Chladný, V., Beláň, A., Eleschová, Ž.: Digitálne ochrany v elektrizačnej sústave. Bratislava, STU 2004.

[5] Masný, M., Mucha, M.: Určovanie elektrických parametrov prenosových elektrických vedení pomocou MKP. In: EE časopis pre elektrotechniku a energetiku. - ISSN 1335-2547. - Roč. 13, mimoriadne č (2007), s. 88-92

[6] Janíček, F., Kovács, Z.: Spoľahlivostné inžinierstvo a pravdepodobnostná analýza bezpečnosti. Bratislava, FEI STU 1997.

[7] Tuma, J., Rusek, S., Martínek, Z.: Spolehlivost v elektroenergetice. ISBN 80-239-6483-6

[8] Trojánek, Z., Tůma, J.: Rízení elektrizačních soustav: určeno pro stud. fak. elektrotechn. 2. vydanie. Praha: ČVUT, 1990. 260 s.

[9] Tůma, J., Žák, P.: Spolehlivost dodávek elektriny v liberalizovaném prostredí, Česká energetika, ISSN 1213-4117, 2003, s. 23-28.

[10] Ferenc, M., Kovács, Z., Mucha, M.: Maintenance Optimization of the Electric Power System. In: CO-MAT-TECH 2007 : Proceedings of the 15th International Scientific Conference. Trnava, Slovak Republic,18.-19.10. 2007. - Trnava : AlumniPress, 2007. - ISBN 978-80-8096-032-2. - p. 147-152. (in English)

[11] Ferenc, M., Kovács, Z., Mucha, M.:, Poljovka, P.: Optimization of Preventive Maintenance for Equipment in Electrical Power Industry. In: Energomatika 2007 : International Conference. Prague, Czech Republic, 17.-18.4.2007. - Prague : Wirelessscom, s.r.o., 2007. - ISBN 978-80-239-9076-8. - CD-Rom. (in English)

[12] Ferenc, M., Kovács, Z., Mucha, M..: Optimization Principles of Preventive Maintenance. In: Elektroenergetics 2007 : 4th International Scientific Symposium. Stará Lesná, Slovak Republic, 19.-21.9.2007. - Košice : Technická univerzita v Košiciach, 2007. - ISBN 978-80-8073-844-0. - p. 651-654. (in English)

Acknowledgement

This project was supported by the agency VEGA MS SR under Grant No. 1/3092/06, Department of Education of the Slovak Republic, under Grant No. AV-0120/06 and by Slovak Research and Development Agency under Grant No. 0337/07.

Abstrakt

Analýza ľudského faktora študuje vzájomné pôsobenie človeka a systému a usiluje sa predpovedať vplyv takýchto vzťahov na spoľahlivosť systému. Cieľom predkladaného článku je popísať spôsob akým sa vykonáva spolahlivostná analýza ľudského činiteľa v kontexte PSA (pravdepodobnostná analýza bezpečnosti) pre energetické systémy.

prof. Ing. František Janíček, PhD.
Slovenská Technická Univerzita
Fakulta elektrotechniky a informatiky
Katedra elektroenergetiky
Ilkovicova 3
812 19 Bratislava
Tel.: +421 2 602 91 783
frantisek.janicek@stuba.sk

Ing. Zoltán Kovács
RELKO Ltd.
P.O.Box 95, Račianska 75,
830 08 Bratislava 38
tel.: +421 2 444 60 137
kovacs@relko.sk

Ing. Emil Krondiak
Slovenská elektrizačná prenosová sústava, a.s.
Mlynské nivy 59/A
824 84 Bratislava 26, SR
krondiak_emil@sepsas.sk

Ing. Matej Korec
VUJE, a.s.
Okružná 5
918 64 Trnava
korec@vuje.sk