XA9847289

INTEGRATED APPROACH TO KNOWLEDGE ACQUISITION AND SAFETY MANAGEMENT OF COMPLEX PLANTS WITH EMPHASIS ON HUMAN FACTORS

K.T. KOSMOWSKI
Technical University of Gdańsk,
Gdańsk, Poland

Abstract

In this paper an integrated approach to the knowledge acquisition and safety management of complex industrial plants is proposed and outlined. The plant is considered within a man-technology-environment (MTE) system. The knowledge acquisition is aimed at the consequent reliability evaluation of human factor and probabilistic modeling of the plant. Properly structured initial knowledge is updated in life-time of the plant. The data and knowledge concerning the topology of safety related systems and their functions are created in a graphical CAD system and are object oriented. Safety oriented monitoring of the plant includes abnormal situations due to external and internal disturbances, failures of hardware/software components and failures of human factor. The operation and safety related evidence is accumulated in special data bases. Data/knowledge bases are designed in such a way to support effectively the reliability and safety management of the plant.

1. Introduction

Potentially hazardous systems such as nuclear power or chemical plants are designed and operated according to national regulations and safety standards. However, due to complexity of the plant design and many interactions within the system: 'man'-'technology'-'environment' (MTE), the disturbances and abnormal situations, some of stochastic nature, occur during the plant operation. Frequencies and consequences of potential abnormal/emergency situations depend on the nature of the MTE system and the safety features of the plant. The reliability characteristics of its components change in time. Therefore, the permanent safety assessment and management are required starting from the conceptual design stage of the plant to its decommissioning.

The influence of so called human factor on the safety of complex industrial systems, nuclear power plants (NPPs) and hazardous chemical installations in particular, is widely recognized. Human-system or simply human interactions (HIs) is the term that describes all interfaces between humans and the system (Moieni et al. 1994). Errors committed by man managing, operating and maintaining these systems are often most significant causes of accidents and risk associated with their operation (Dougherty & Fragola 1988).

On the other hand the state of the art of the human reliability methodology and available at present methods/techniques for probabilistic assessment of human failures indicate that this methodology is not mature. It was confirmed by results of some experimental research, aimed at validation of the human reliability analysis (HRA) models, more frequently used in engineering practice. Another problem is associated with the fact that the human reliability assessments are profoundly dependent on expert judgment. Results of HRA benchmark exercises, summarized e.g. in (Poucet 1988), have shown that the human error probability (HEP) and assessed frequency of some accident situations for specified plant, obtained by different groups of HRA experts, can reach discrepancy as high as orders of magnitude.

HRA in the context of the probabilistic safety analysis (PSA) is an attempt to model HIs and predict the impact of such interactions on the reliability and safety of plants. When a system is complex with a large number of human interactions, in various phases of the plant normal operations or abnormal conditions, then HRA becomes an extremely important part of PSA for realistic assessment of plant safety (Moieni et al. 1994).

Therefore, considerable research efforts have been undertaken at some research institutions and regulatory bodies to improve the methodology, verify models and propose approaches standardizing HRA performed within PSA studies (IAEA 1992). It is very important for obtaining correct quantitative results, used often in engineering practice for the reliability management and safety related decision making. For accomplishing these objectives a tendency of growing interest in computer aided PSA and HRA is observed, especially in employing the expert system technology. In this paper an integrated approach to the knowledge acquisition and safety management of complex industrial plants is proposed and outlined.

2. Knowledge acquisition as modeling of the plant with emphasis on the human factor

2.1. Features of a software system for computer aided PSA

There is a growing interest to design supporting computer programming tools for managing more effectively the complexity of PSA and HRA and to reduce subjectivity of assessments, as these analyses should be adequately documented for future scrutinizing and modifying when new evidence will be available ("living" PSA). Lately this interest has been focused on employing the expert system technology (Wang & Modarres 1990, Poucet 1990, IAEA 1990, Kosmowski et al. 1994). The knowledge based systems (expert systems) are developed to imitate the knowledge of the domain experts and are designed to use various information sources including external data and expertise (IAEA 1990).

A prototype expert system REPSA1ES (*Reliability Evaluation and Probabilistic Safety Analysis-level 1-Expert System*) has been designed (Kosmowski et al. 1994). This system consists of a CAD system for graphical representation various diagrams, various data bases, a shell for building expert system and a coordinating module, all integrated in the programming environment of MS Windows 3.1. This knowledge based system has some interesting features, e.g. the user friendly interface with extensive graphical support using several CAD modules to represent the topological information and functional-logical knowledge. It enables effective data/knowledge acquisition as well as the iterative logical and probabilistic modeling of complex safety related systems.

2.2. Human reliability analysis (HRA) in the context of PSA

The HRA is often performed according to the SHARP procedure (Hannaman & Spurgin 1984). Introducing the human failure events into the structures of the fault and event trees is performed at present in REPSA1ES by the user. There is a general guidance to perform these tasks. Since the effects of slips during plan-directed activities usually do not propagate unassisted by other failures beyond the component(s) affected, they can be incorporated into the fault tree models. Mistakes, which are most significant in event-driven activities, because of their propagative potential, are to be incorporated best at the top of the fault trees or in the event trees. Recovery events are tacked on the end of the dominant accident sequences for which they apply and may not be formally included in the event or fault trees (they can be left as adjoins to cut-sets). In this way, the classification effort supports the integration effort (Dougherty & Fragola 1988).

After the selection of appropriate HRA method the assessment of HEP is carried out according to determined procedure with regard to attributes of the situation analyzed. Thus,

the system provides a computerized framework to perform HRA, calculate HEPs and document analyses. However, depending on the method selected more or less external expertise from the domain expert is required to provide the description of the situation of interest and some factors influencing human performance.

In the current version of this system a prototype version of simplified THERP technique, based on ASEP-HRAP approach, is available and tested. The evaluation of HEP is initiated when the human failure event is placed into the fault tree. Then some attributes of such event are determined in dialogue with the user according to the procedure available in the HRA module. At the end of the session the value of HEP is calculated and placed of the human reliability data base (HRDB), related to given PSA project.

In the HRA/PSA screening process only more important and probable human failure events are taken into account for further analysis (Hannaman & Spurgin 1984). Obtained HEPs are to be stored in a project human reliability data base (Kosmowski et al. 1994). Some data bases have been designed, related to specific HRA methods, to store values of attributes for the situations analyzed. Thus, the human reliability modeling process is documented.

2.3. Levels of details of computer aided PSA/HRA

Three levels of effort to carry out balanced PSA and HRA have been distinguished: I, II and III which correspond to the PSA and HRA basic methodological issues (methods applied, details of modeling and the contribution of experts required) and relevant scopes of the computer aided analyses (Kosmowski et al. 1993, 1994). The development of the software system with an open architecture has been scheduled for gradual and balanced realization of the research and designing works with regard to resources available.

At present the designing works are concentrated on selected methods of the scope II and III, namely: the THERP technique with graphical representation of the human reliability analysis event trees (HRAET) and a computerized version of modified SLIM technique. The situation specific HRAET enables representing possible paths of human actions and failures including errors and recovery potential. Obtained structure is then assessed based on the procedure and probabilistic data available within THERP.

3. Challenges associated with integrated approach to safety management of complex plants

3.1.A general concept of the knowledge acquisition and safety management

A general concept of an integrated approach to the safety management of the man-technology-environment (MTE) system is presented in Fig. 1. Safety monitoring of the plant includes abnormal situations due to external and internal disturbances, failures of hardware and software components and failures of human factor. The operation and safety related evidence is accumulated in special data bases. Several knowledge bases are conceptually designed in such a way to support effectively the reliability and safety management of the plant. Properly structured initial knowledge is updated in life-time of the plant to include changes of technical specifications or operation conditions.

A knowledge based 'living' Probabilistic Safety Analysis (PSA) and Human Reliability Analysis (HRA) is assumed to be a methodological basis for knowledge acquisition and safety management. The modeling process and analyses are performed based on a graphical and symbolic object-oriented representation of the plant. It includes the topology of systems (P&IDs), the hierarchical description of safety functions, directed graphs for defining relations between the states of functional objects and process variables, logical models (success trees, fault/event trees, HRA trees). The construction of logical structures (fault and event trees) can

be partly automated based on topological/logical information. These structures are then quantitatively assessed using special calculation modules.

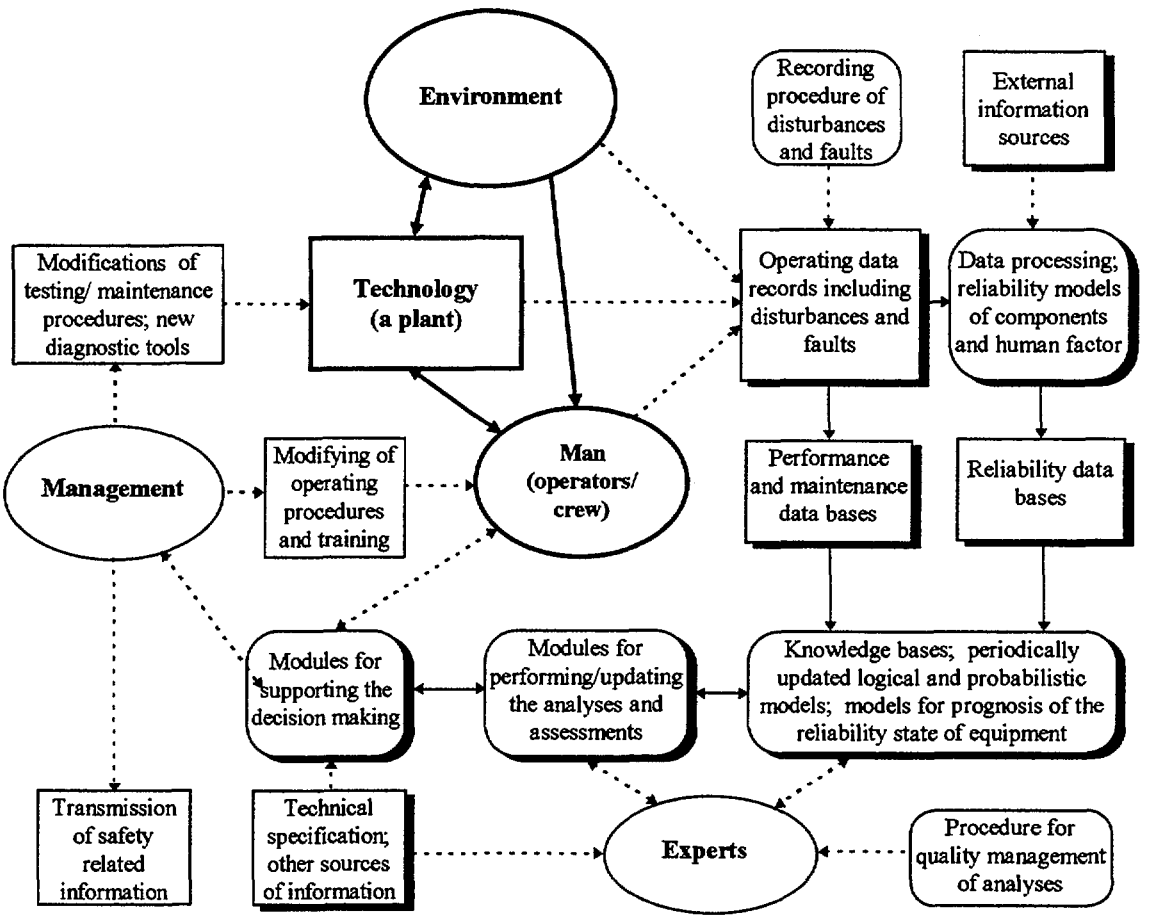

Fig.1. Schematic illustration of general concept of an integrated approach to the safety management of the man - technology - environment (MTE) system

Different modules are proposed to enable 'intelligent' reprocessing of information for given purpose, e.g. to support decisions concerning a testing strategy for safety systems, to evaluate safety-related limitations of the plant operation due to partial failures. Several diagnosis support modules are conceptually designed to be in accordance with the symptom oriented-operating procedures but with possibilities to support the operators in diagnosing of multiple failures and evaluating the recovery paths. Psychological aspects of human interactions within complex plant during abnormal situations have been also considered.

The concept of a software system IKASM (Integrated Knowledge Acquisition and Safety Management) have been developed and its basic modules specified (Kosmowski 1996). Some of them are modifications of modules of mentioned above expert system REPSA1ES. It was assumed that the knowledge acquisition and reprocessing of information within IKASM will be performed according to a procedure of quality management which includes issues of uncertainty representation and treating (Kosmowski 1996).

3.2. Recording of failures and analyzing their causes

To improve the performance of the plant it is important to reduce the hardware, software and human induced faults. It can be done effectively if the situation context and possible causes of a failure/ fault will be recognized. A data recording system and a software system should

support the analyst to answer "what", "how" and "why" questions. In the case of human faults "what" happened, corresponds to the initial conditions, the circumstances and consequences. "How" it happened, corresponds to the source of the error in the task, and "why" it happened to the failure mechanism. Mechanisms of failures can be divided into ergonomics, environment, documentation, communication, training, organization and personal factors. Most promising way to design such software system is to use the expert system technology (Ives 1991).

Identification of causes of human errors can be also valuable for programming of operator training through the development of intelligent computer-assisted instruction systems (Furuhama et al. 1995).

3.3. Adapting/developing HRA methods for knowledge based supporting computer tools

Theory of human reliability is not yet well established and there are expressed opinions about the necessity to develop the next generation of human reliability models (Dougherty 1993, Lydell 1992). Human reliability can be considered as a more general problem of human factors in complex organizations (Llory 1992). The HRA modeling approaches which now emerge fall into four categories: procedural, temporal, influential and contextual (Dougherty 1993). New HRA approaches should be based more than in existing techniques on psychological aspects of human error (Reason 1990). Some HRA approaches are evolving in the direction of the cognitive simulation environments using the artificial intelligence (AI) methods (Woods et al. 1990). Cognitive modeling is considered to be a fundamental issue for human reliability analysis (Cacciabue 1992).

It has been indicted (Dougherty 1993) that the analysis should remain a fundamental part of the human reliability assessment by examining cases of cognitive problems. The relevant methods should include four major efforts: (1) Identify the goal matrix for the situation and any possible goal conflicts, (2) Develop a functional chronology of the situation including time matrix of the actions and decisions to be made, personnel links and the impact of distributed decision making, (3) Perform a cognitive task analysis, and (4) Perform knowledge acquisition (interview of operators, make simulations and walk-downs). On that basis the quantification, using e.g. SLIM technique, will have substantial justification and the results obtained will be translatable to useful insight for further risk management.

3.4. Using the logical/probabilistic models for supporting diagnosis and safety related decision making

Fig. 2 shows relationship of the diagnosis and decision support modules for transients, abnormal and emergency situations. There are several proposals to design these modules using success trees, heuristic approaches using rule based expert systems, and neural networks (Kim et al. 1990). Bottom middle and right supporting modules in Fig. 2 are designed with regard to knowledge acquired during the logical and probabilistic modeling of the plant. The bottom right decision support module for abnormal/critical and emergency situations is presented in some details in Fig. 3.

The emergency operating procedures (EOPs) used in nuclear power plants are symptom oriented (Kang et al. 1994, Yang et al. 1994). It was assumed that in an early phase of an emergency situation the operators will follow steps of selected EOP, but then they start the identification process of possible causes of current situation which can be supported by a module A (Fig. 3). In the case of a redundant system the possible cases of its total fault are identified in inferring process on a set of rules in the form

$$IF\ S_i\ and\ S_j\ \ldots\ THEN\ F_l$$

where $S_i, S_j, \ldots$ are symptoms related to a minimal cut set (MCS) and F_l represents a set of components (failure events) of l-th MCS. Such rules are developed based on a fault tree constructed for given system (Schwarzblatt 1996). A modified approach to the construction of fault tress have been developed with a special treatment of symptoms assigned to gates and basic events. Because the number of rules considered in inferring process can be large a method has been developed to reduce the searching space using a measure of frequency of symptoms evaluated with regard to the reliability importance of components (basic events).

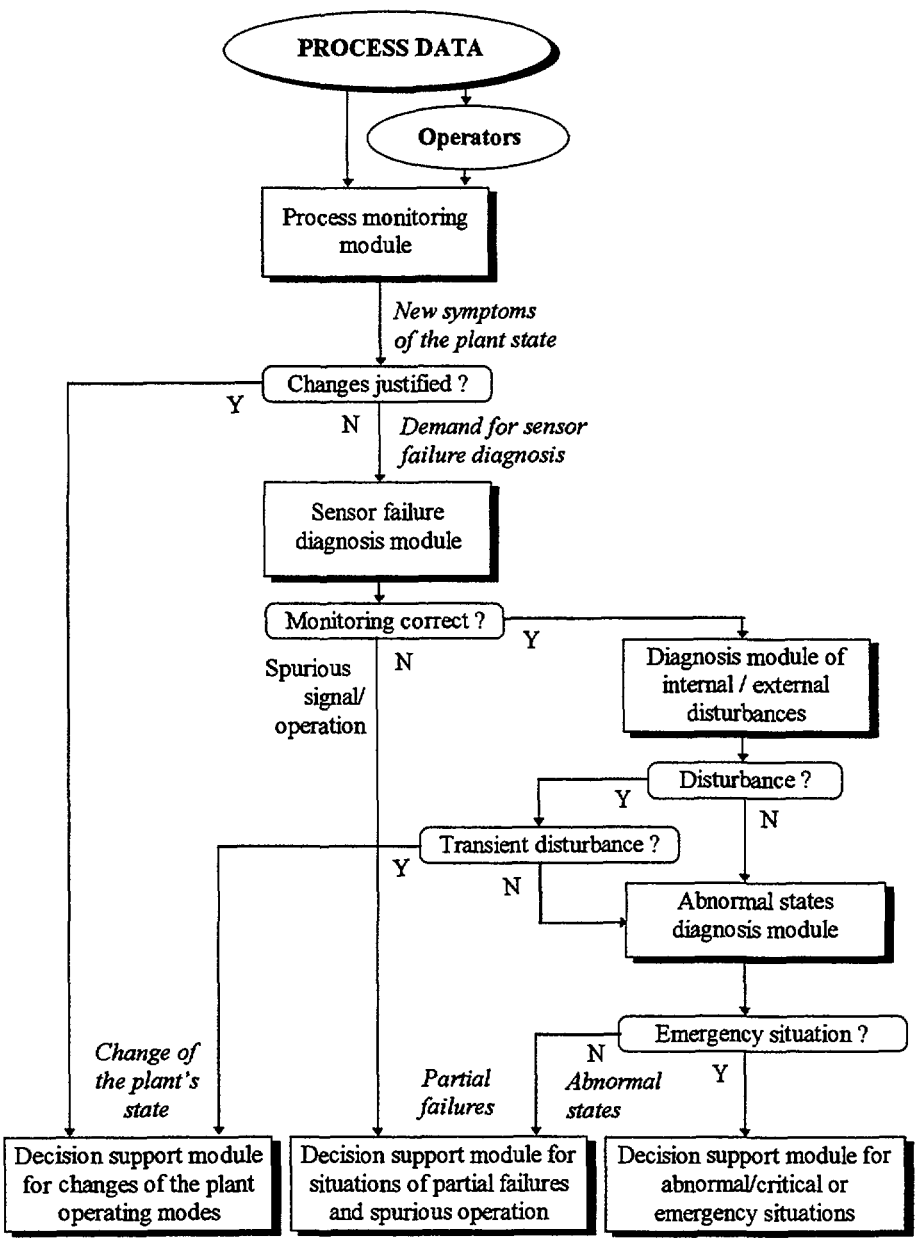

Fig. 2. Relationship of diagnosis and decision support modules for transients, abnormal and emergency situations

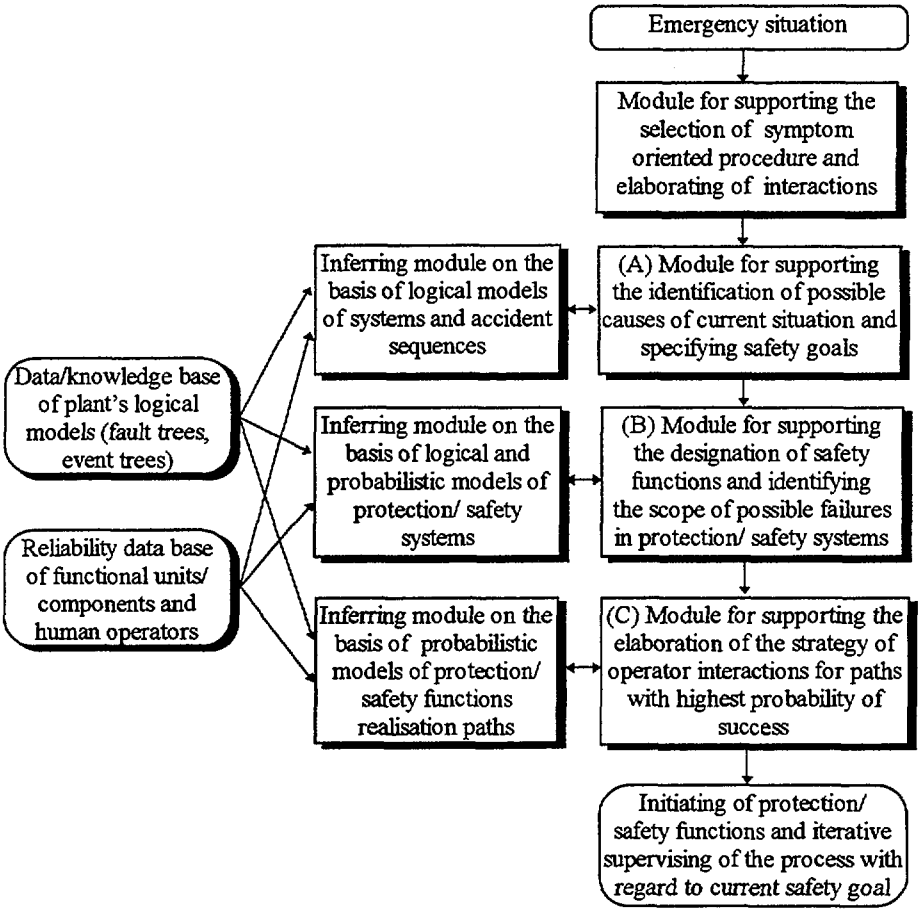

Fig. 3. A proposal to use of object oriented logical and probabilistic models of the plant for supporting the diagnosis and decision making in emergency situations

3.5. Quality aspects of logical/probabilistic modeling

There is an increasing interest to apply the probabilistic safety analysis and human reliability analysis not only in nuclear industry to support the reliability and safety related decision making. There are, however, problems of quality of analyses (Rouhiainen 1993) making the results obtained questionable for safety related decision making. There are several important sources of uncertainties:

- defining and decomposing of systems to be analyzed,
- scope and assumed level of details of analyses,
- uncertainties in the statistical data and models available,
- modeling the topological, functional and statistical dependencies,
- modeling the human factor reliability,
- subjectivity of expert judgment (Mosleh et al. 1988),
- issues related to quality control and management of safety analysis.

To manage the quality of safety analyses the standardization concept is needed (Rouhiainen 1993). The safety analysis always includes subjective decisions. However, systematic tools for integrating quality management in the planning and execution of the safety analysis are needed to standardize the practice and to limit individual variations. A promising direction is to develop tools and perform the computer aided analyses, e.g. based on the expert system technology. Quality of such software systems would be accepted by regulatory bodies and users if a proper verification and validation (V&V) procedure were carried out with regard to standardization requirements.

4. Concluding remarks

So called human factor significantly influences the reliability and safety of complex plants and, therefore, should be adequately included and quantified in the overall probabilistic assessments. It is crucial for assuring a high quality of results to be used for safety related decision making. The human reliability analysis is significantly dependent on expert opinions.

To facilitate the HRA and PSA studies the use of the expert system technology is proposed, although designing the software system based on this technology requires considerable effort. According to current practice in performing PSA and HRA three scopes of studies have been distinguished. The design effort is now concentrated on the scope I and II of this software system. The process of PSA and HRA in such knowledge based software system will be documented to enable scrutinizing and auditing of results. Employing the expert system technology would be an important step in standardizing of relevant analyses.

The quality of the human reliability analyses can be improved by selection of the appropriate method for the case considered to include if possible psychological aspects of human actions and errors. The human reliability analysis should be not aimed only at obtaining quantitative results. No less important are qualitative results of analyses which should be considered for improving the man-machine interactions to minimize possibilities to commit errors or to limit their consequences.

Additional research effort is required to include following topics:

- the event driven simulation of the plant and human cognitive performance, including intention failures (Woods et al. 1990), aimed at qualitative and quantitative modeling of the human factor,
- an advanced framework for representing and treating of imprecision and uncertainties in PSA and HRA at different levels of the model hierarchy of the complex plant,
- methods for combining quantitative information from various sources of different quality (credibility) including experts,
- the quantitative evaluation of accident scenarios under uncertainties with regard to different kinds of dependencies (topological, functional and statistical),
- integrated treating of human, organization and management factors in safety analyses.

Artificial intelligence methods, and the expert system technology in particular, offer a promising platform to deal more systematically with some challenging issues of PSA and HRA. However, the development of advanced PSA/HRA methods and related software tools will require a considerable research and design effort. The verification and validation procedures must be also developed related to the quality management procedures.

References

Cacciabue, P.C. 1992. Cognitive modelling: A fundamental issue for human reliability assessment methodology?, Reliability Engineering and System Safety, Vol. 38, pp. 91-97.

Dougherty, E.M., J.R. Fragola 1988. Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications. A Wiley-Interscience Publication, John Wiley & Sons Inc., New York.

Dougherty, Ed 1993. Context and human reliability analysis. Reliability Engineering and System Safety, Vol. 41, pp. 25-47.

Furuhama Y., Furuta K., Kondo Sh. 1995. Identification of causes of human errors in support of the development of intelligent computer-assisted instruction systems for plant operator training. Reliability Engineering and System Safety, Vol. 47, pp. 75-84.

Hannaman, G.W., A.J. Spurgin 1984. Systematic Human Action Reliability Procedures (SHARP). EPRI NP-3583, Research Project 2170-3.

Humphreys, P. (ed.) 1988. Human Reliability Assessor Guide. Safety and Reliability Directorate, UK, RTS 88/95Q.

IAEA 1990 (International Atomic Energy Agency). Use of Expert Systems in Nuclear Safety. IAEA-TECDOC-542, Vienna.

IAEA 1991 (International Atomic Energy Agency). Case study on the use of PSA methods: Human reliability analysis. TECDOC-592, IAEA, Vienna, April 1991.

IAEA 1992 (International Atomic Energy Agency). Procedure for Conducting Human Reliability Analysis in Probabilistic Safety Assessment (a draft report).

Ives G. 1991. Developing expert system to analyze human performance in NPP events. Journal of ENS (European Nuclear Society), Nuclear Europe Worldscan 11-12.

Kang K.S., Chang H.S., Chang S.H. 1994. Developed of the advanced procedure for emergency operation using task allocation and synthesis of PRA results. Reliability Engineering and System Safety, Vol. 45, pp. 249-259.

Kim I.S., Modares M., Hunt R.N.M. 1990. A model -based approach to on-line process disturbance management: the models. Reliability Engineering and System Safety, Vol. 28, 1990, pp. 265-305.

Kosmowski, K.T.,K.Duzinkiewicz 1993. An integrated approach in probabilistic modelling of hazardous technological systems with emphasis on human factor. Proceedings of ICOSSAR'93 - the 6th International Conference on Structural Safety and Reliability, Innsbruck, Austria, 9-13 August 1993. A.A. Balkema/Rotterdam/Brookfield/1994, Vol.3, pp. 1889-1896.

Kosmowski, K.T., K. Duzinkiewicz, M. Jackowiak, J. Szczęśniak 1994. Representation of topological and functional-logical knowledge in an expert system for probabilistic safety analysis. IAEA-TECDOC-796, p.123-136.

Kosmowski, K.T., G. Degen, J. Mertens, B. Reer 1994. Development of Advanced Methods and Related Software for Human Reliability Evaluation within Probabilistic Safety Analyses. Berichte des Forschunszentrum Jülich; 2928. June 1994.

Kosmowski K. T. 1995. Issues of the human reliability analysis in the context of probabilistic studies, International Journal of Occupational Safety and Ergonomics, Vol. 1, No. 3.

Kosmowski K T.. 1996. Integrated approach to probabilistic modeling and safety analysis of man-machine systems (in Polish). VI Safety Conference. Kiekrz 10-13.06.1996, pp. 97-104.

Llory M.A. 1992. Human reliability and human factors in complex organizations: epistemological and critical analysis - Practical avenues to action. Reliability Engineering and System Safety, Vol. 38, pp. 109-117.

Lydell, B.O.Y. 1992. Human reliability methodology. A discussion of the state of the art. Reliability Engineering and System Safety, Vol. 36, pp. 15-21.

Moieni, P., A.J. Spurgin, A. Singh 1994. Advances in human reliability analysis methodology. Part I: Frameworks, models and Data. Reliability Engineering and System Safety, Vol. 44, pp.27-55.

Moieni, P., A.J. Spurgin, A. Singh 1994. Advances in human reliability analysis methodology. Part II: PC-based HRA software. Reliability Engineering and System Safety, Vol. 44, pp.57-66.

Mosleh, A., V.M. Bier, G. Apostolakis 1988. A Critique of current practice for the use of expert opinions in probabilistic risk assessment. Reliability Engineering and System Safety, Vol. 20, pp. 63-85.

Poucet, A. 1988. Survey of methods used to assess human reliability in human factors reliability benchmark exercise. Reliability Engineering and System Safety, Vol. 22, pp. 257-268.

Poucet, A. 1990. STARS: knowledge based tools for safety and reliability analysis. Reliability Engineering and System Safety, Vol. 30, pp. 379-397.

Reason, J. 1990. Human Error. Cambridge University Press.
Rouhiainen, V.: Importance of the quality management of safety analysis. Reliability Engineering and System Safety, 1993, Vol. 40, pp. 5-16.
Schwarzblat M., Arellano J., Mendoza P.R., Smith J.E. 1996. The use of probabilistic safety analysis assessment results for the development of diagnostic and alarm processing expert systems, in: Development of safety related expert systems. International Atomic Energy Agency, IAEA-TECDOC-856, Vienna, pp. 59-66.
Wang, J., M. Modarres 1990. REX: An intelligent decision and analysis aid for reliability and risk studies. Reliability Engineering and System Safety, Vol. 30, pp. 195-218.
Woods, D.D., H.E. Pople, E.M. Roth 1990. The Cognitive Environment Simulation as a Tool for Modeling Human Performance and Reliability. Westinghouse Science and Technology Center. Pittsburgh, USA. NUREG/CR-5213, Vol. 1.
Yang J.-E., Jeong K.-S., Park Ch.K. 1994. Development of an emergency operation supporting system for nuclear power plants. Reliability Engineering and System Safety, Vol. 43, pp. 281-287.