Abramova N.A., Kovriga S.V., Makarenko D.I.

PRINCIPLES OF QUALITY MANAGEMENT OF COMPLEX HARDWARE AND SOFTWARE SYSTEMS PRIORITIZING MITIGATION OF RISKS CAUSED BY HUMAN FACTOR

In order to reduce the impact of human factor on risks of hazard in operation for the design of safety-critical hardware and software systems, several new principles have been suggested to increase the quality of such systems' design. The findings presented in this paper are based, on the one hand, on psychological and interdisciplinary researches and, on the other hand, on the analysis of the designing practice of complex hardware and software systems of the atomic energy industry.

***Keywords**: hazardous facility, safety, hardware and software system, reliability, human factor-related risks, design quality management.*

Introduction

Today there is a progressive complication of potentially hazardous facilities that use management or decision support methods and systems based on formal methods. The concept of facility (system) complexity, along with more conventional characteristics (quantitative complexity, structural complexity, mathematical models complexity – «organized complexity»), includes the human aspect of complexity when the intellectually complex stage of control and safety ensurance is the initial structuring and formalization of knowledge regarding the designed facilities and the specified requirements.

[1]Because of the inevitable human involvement, the currently used knowledge structuring and formalization methods in the design of complex facilities are generally unable to ensure the reliability of final results. In other words, the results bear reliability risks. Thus, the search for the solution for the problem of human factor-related risks must cover not only the facilities themselves, but also the design process that also involves people. That means that human factors of risk may be related not only with people involved in the facility operation process, but also the developers of management and information technology methods and systems as well as the scientists providing theoretical justification of management methods.

The practical significance of the risks in question with regards to the management of complex facilities is largely confirmed by experimental research of the control subject's thinking process in complex problem situations and analysis of the causes of cognitive errors made during their resolution [1].

[1] Here the reliability is interpreted broadly as the reliability of the results of such methods' application.

The article presents a classification of risks depending on the nature of their influence on the safety of potentially hazardous facilities operating HSSs, proposes several new principles and methods aimed at improving the quality of HSS design. The presented results are based, on the one hand, on psychological and interdisciplinary research and, on the other hand, on the analysis of the design practice of HSS for nuclear power plants.

1. Variety of indirect sources of risk during operation of safety critical hardware and software systems

In order to identify and classify the human factors and risk mechanisms (1) manifesting themselves within the HSS development, deployment and application lifecycle and (2) practically significant to quality management, a selective analysis of complex safety critical HSSs design practice has been conducted (as regards nuclear power plants).

The analysis of the potentially hazardous facilities' HSSs quality assurance practice shows that due to the increasing intellectual complexity of HSSs the conventional methods of quality assurance do not cover the wide range of various indirect safety risks that manifest themselves in practice and cannot be evaluated quantitatively. That primarily pertains to human factor-related risks during HSS design and testing. It is assumed that the conventional approach to safety critical HSS quality assurance is the stage-by-stage verification and validation along with relevant organizational methods and limited use of formal methods whose capabilities amidst the increasing HSS complexity are significantly limited.

Below is the classification of risks depending on the nature of their influence on the safety of potentially hazardous facilities during HSS operation:

- HSS operation-related obviously safety critical risks (i.e. entailing the risk of hazardous situations at the facility),
- indirect risks that do not show obvious connection with hazardous situations.

The indirect risks include:

- technical risks related to the engineering decisions taken during HSS development;
- organizational and managerial risks including those related to the

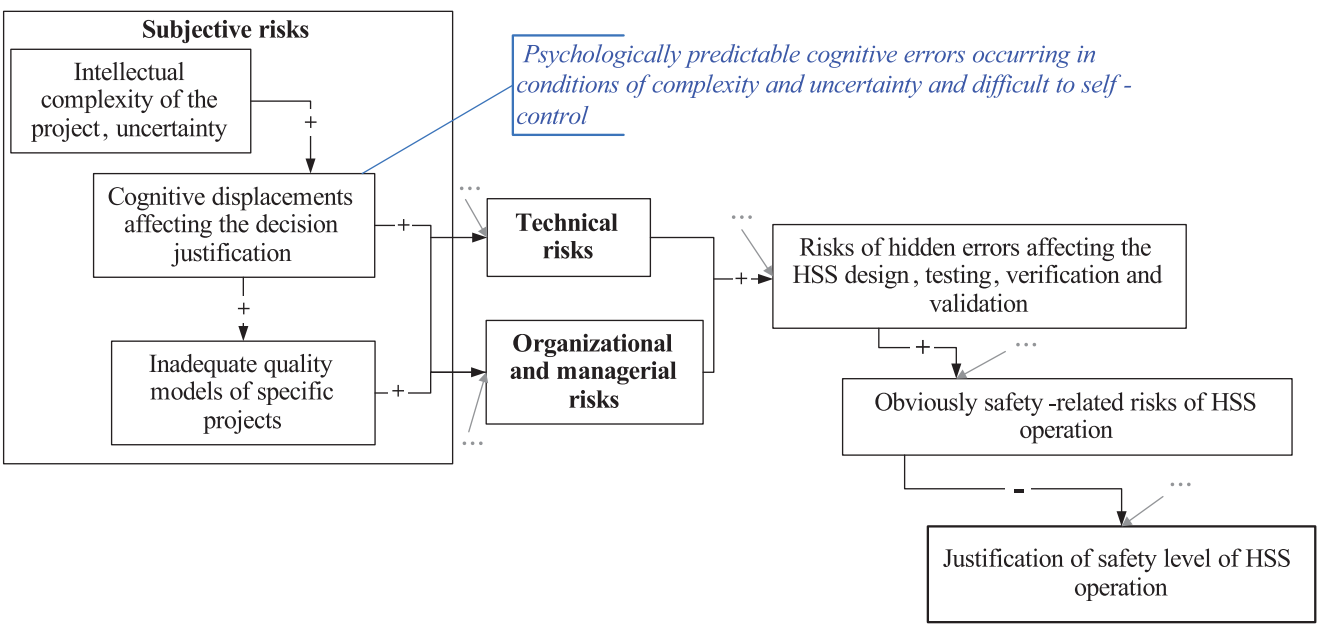

Fig. 1. Human factor-related risks during safety-critical HSS development and their causal relationships

– maturity of the HSS development process in terms of the SW-CMM maturity model [2];
– competence of the parties involved in the manufacturing and managerial processes;
• subjective risks related to cognitive and other particular properties of the parties involved in the manufacturing and managerial processes (according to present-day cognitive science knowledge).

Fig. 1 shows generic risks and causal relationships between those generic risks (the sign «+» indicates a positive influence («the more…, the more…»), while the sign «–» indicates a negative influence («the more…, the less…»); the grey arrows indicate other possible types of risks).

As a result of analysis and classification of risks depending on their influence on the safety of potentially hazardous facilities during HSS operation (1), confirmation was found for the hypothesis of the dependence of human factor-related risks during the design of safety-critical HSS on the functional roles of people in the HSS lifecycle; (2) a hypothesis was developed and tested of the dependence of inadequate quality model of specific projects used by executive managers from well known psychological risk factors called cognitive displacements (psychologically predictable cognitive errors occurring under conditions of complexity and uncertainty that are difficult to self-control). Those include stereotypes of obsolete technology application, systematic underestimation of the significance of unusual requirements.

The diversity of the identified practically significant risks affecting the design of complex safety critical HSS considering the significant role of the human factor along with the practical impossibility of reliable quantitative evaluation of such risks indicate the development of new theoretical approaches to the solution of the problem of complex HSS design quality management.

2. General principles of indirect quality management of safety critical hardware and software systems

The well-known principle of stage-by-stage verification during safety critical HSS development can be considered as an indirect HSS quality management principle. The standard approach involves the verification based on preventive quality criteria of intermediate design products represented in appropriate documentation.

In order to boost the capability of early identification of indirect human factor-related risks (compared to the standard approach to verification), a number of new principles were proposed:

• *wider coverage of diverse indirect risk factors and their causal relationships*, most notably human factors in situations of identification of errors or risks of inadequate technical or managerial decisions in order to improve the efficiency of HSS quality management and to extend the number of control mechanisms;

• *principles of extended verification*, including the verification of not only technical solutions, but the used evaluation methods, namely project quality models (within the available total resources);

• *limited use of formal methods of comprehensive assessment*, specific to safety critical HSS design and testing quality management in order to avoid the risk of inaccurate assessment combined with the verification of the assessment methods themselves. The principle of limited use of formal methods of comprehensive assessment combined with the verification of the methods of assessment is justified by (1) previously found by means of theoretical analysis and practically confirmed possibilities of quality assessment manipulations in conditions of impossibility of reliable quantitative evaluation of risks or other design quality indicators; (2) uncovered risks in the assessment methods themselves suggested by the theory and standards for the purpose of comprehensive assessment of safety critical HSSs;

• *reflexive method of justification analysis* of the technical and managerial decisions that takes into consideration not only the objective justifications of the decisions taken, but also the dependence of the notions of the executive managers from the subjective factors of risk, functional roles and interests. The reflexive method is justified by the existence of a number of practical situations when the identification of unjustified decisions is impossible or complicated if subjective factors are not taken into consideration (e.g. erroneous understatement of requirements to the design of HSS compared to the level of requirements based on the safety class);

• *expert verification without predefined criteria* in addition to conventional verification based on predefined criteria. The method of expert verification without predefined criteria is justified by the

– analysis of the experience of verification and cross analysis of design decisions taken by co-contractors of a specific HSS project;

– interdisciplinary research of psychological mechanisms at the foundation of expert verification, beginning with «error detector» [4], «cognitive dissonance», etc. [5].

In order to increase the quality of the error and risk identification process, verification experts have developed an original interdisciplinary model of the cognitive process of expert verification without predefined criteria. It is comparable with the well-known model of two cognitive systems reflecting the intrinsic human capability to identify errors in justifications [6].

2.1. Model of cognitive process of expert verification without predefined criteria

The fundamental difference between the conventional verification based on predefined criteria from the expert analysis as a verification method is that in the first case the selection of the criteria and the selection (identification) of the verified fragment precede the consistency assessment, while in the case of expert analysis the analyzed material is immediately identified as inconsistent with certain notions of the verification expert. «Immediately» means that the evaluation is the result of intrinsic, not necessarily conscious cognitive processes.

The proposed model of expert verification without predefined criteria is based on a fundamental property of spontaneous identification (localization) if inconsistencies. Furthermore, it is taken into account that, as observations have shown, there are two typical kinds of inconsistence identification. In some cases a fragment of analyzed material (or its property) identified by a verification expert may be immediately assessed as inconsistent with a declared (but not chosen in advance) criterion or requirement. In other cases the assessment is given in the most general expressions like «incorrect», «it can't be», «questionable», «something is wrong», «unclear», «strange» or «anomaly».

By means of subsequent «self-extraction of knowledge» the assessment is explained in such a way that, ultimately, either the inconsistent criterion is identified, or the necessity of further analysis in order to explain the identified irregularity or anomaly is established. In the latter case it is safe to say that we deal with the identification of a risky fragment or general property.

The explanation of cognitive processes resulting in such reaction of the verification expert can be given using the knowledge of cognitive sciences in terms of «cognitive dissonance», «cognitive control», «error detector», «functional body».

However, a more clear and comprehensive notion can result from the use of the computational metaphor and the terms «interrupt system» and related concepts such as «interrupt source», «primary (interrupted) process», «interrupt mechanism», «interrupt service discipline» for connection. The structural organization of expert knowledge processing with interruptions in case of identification of errors and anomalies is shown in Fig. 2.

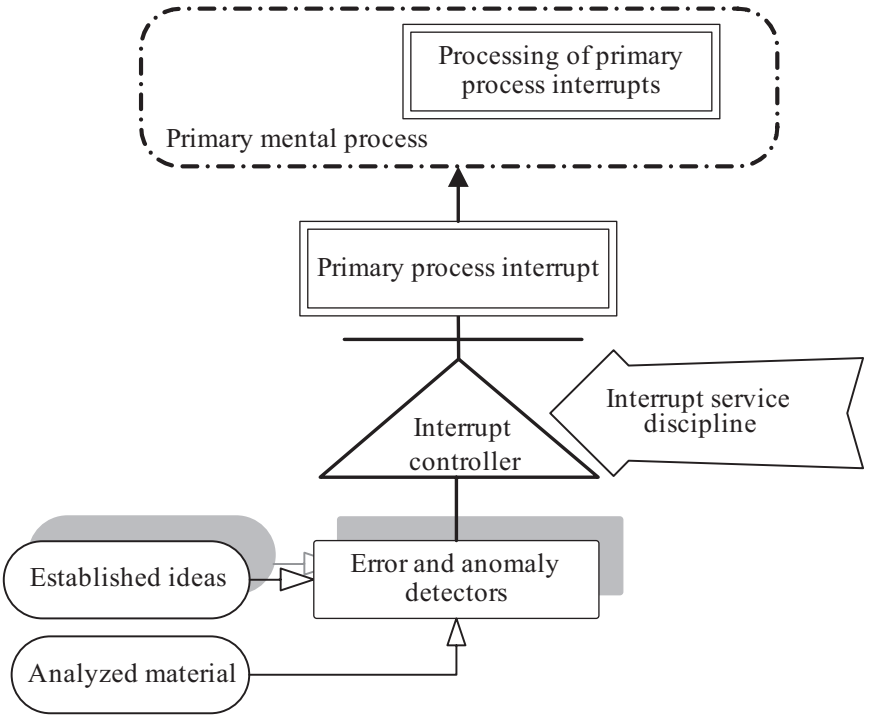

Fig. 2. Structural organization of expert knowledge processing with interruptions in case of identification of errors and anomalies

It appears to be reasonable to consider the identification of inconsistencies as a special case of cognitive dissonance, a psychological discomfort that according to L. Festinger [5] may be caused by the contradiction between the established notions and new information, facts.

The act of inconsistency identification can be interpreted as an operation of an «interrupt system» that carries out cognitive control of the knowledge extracted by the expert from the verification object.

The interrupt system identifies inconsistencies by means of the total of relevant error detectors. Those detectors reflect the stereotypical or at least well assimilated active knowledge in the analyzed area. The identification of an inconsistency by a detector may cause an interruption of the primary process in accordance with an «interrupt service discipline», thus the inconsistency is at least registered by the verification expert and an initial analysis is probably conducted (interruption of the «service»). Given the observation of the identification of risky fragments it is assumed that the detectors can detect not only errors, but also risky and controversial situations.

According to neurophysiologic experiments of N.P. Bekhtereva [4], the action of the mechanism that she called the «error detector» is exercised through emotions that may be considered to be the «interrupt mechanism».

The proposed model of expert verification with two types of knowledge causing a cognitive dissonance allows us to make quite an uncommon conclusion. For the theoretical knowledge to operate as an element of dissonance, the verification expert must have well formed error detectors or at least risk or risky properties detectors that due to their high activity may cause cognitive dissonance and spontaneous interruptions of the primary cognitive process in case of inconsistencies.

The analysis of the practice of safety critical HSS verification in the area of nuclear energy has shown that the proposed model does not only have comparatively significant explanatory capabilities, but also enables the improvement of errors and risks detection process by verification experts, as well as its computer support.

2.2. Modified model of safety critical hardware and software systems quality management

Using the proposed principles, a modified HSS quality management model has been developed that includes, in addition to conventional quality management model with stage-by-stage verification, the identification and assessment within a specific process of HSS design, verification and testing of diverse indirect risk factors active within the HSS lifecycle and their causal relationships with the quality control operations. The general diagram of the modified safety critical HSS quality management model is shown in Fig. 3.

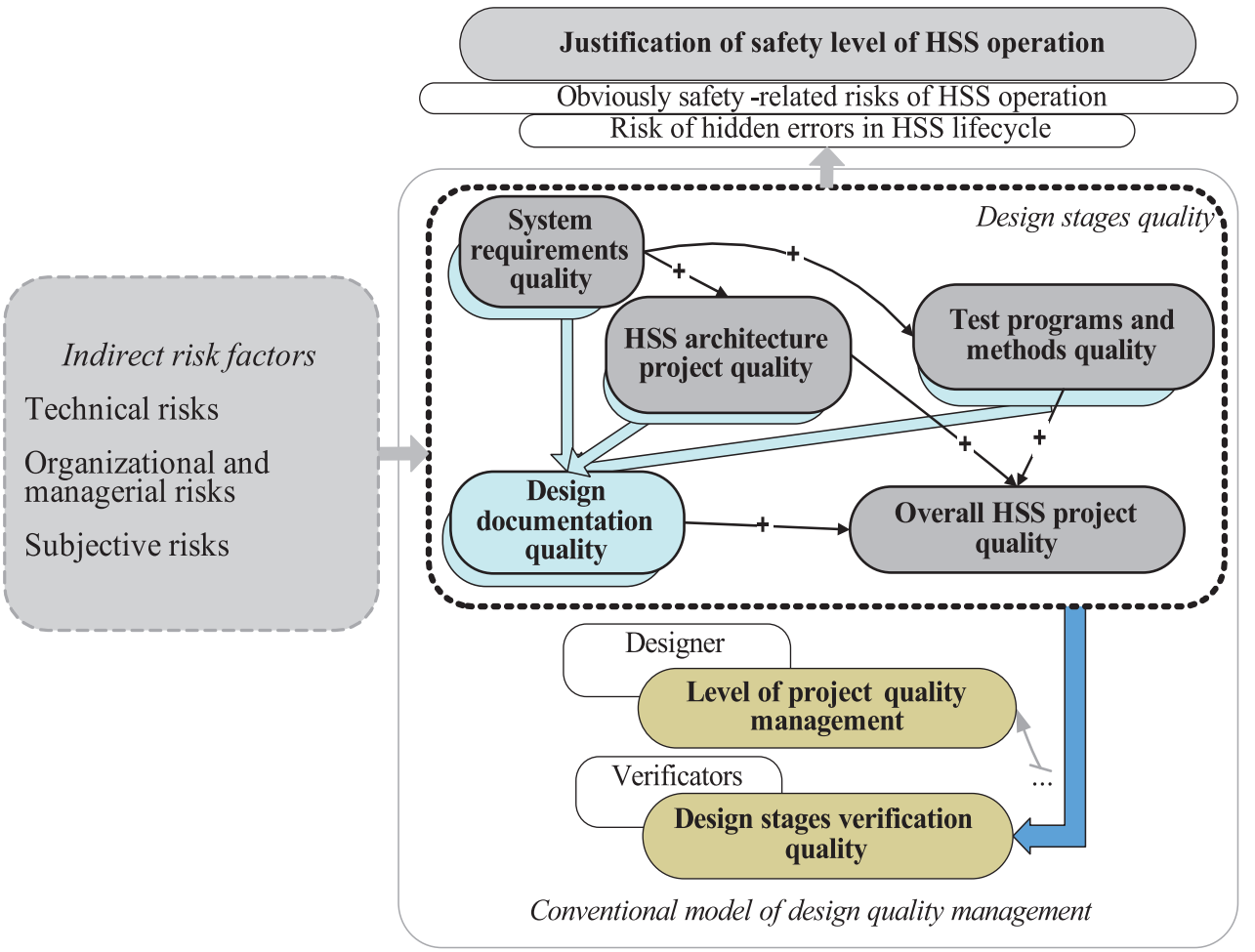

Fig. 3. General diagram of the modified safety critical HSS quality management model

The proposed method that involves the extension of the conventional design quality management model has undergone partial empirical verification as part of the development of a specific safety critical HSS for the Kudankulam nuclear power plant. As part of the HSS project verification a number of significant diverse risk factors were identified beyond erroneous or risky technical decisions (e.g. inconsistency of the system of concepts in the diverse team of an international project, complexity (non-transparency) of the role structure of relationships among project participants, insufficient experience of the developers in the creation of safety critical HSSs). That allowed us to refine the initial quality management model of the project in the form of a cause and effect diagram of indirect influence of the identified factors on the risk of hidden design errors and consequently on the safety level of HSS operation. The modification

enabled the identification of additional control points in order to improve the quality of design. Among other things, it has been confirmed that its application helps coordinate and justify various concepts and notions within a complex role structure of an international project team.

Conclusion

The practical significance of the proposed new principles of indirect HSS quality management consists in the improved capability to manage the quality of such systems' design through identification and recording of human factor-related risks as part of the development of facilities with increased safety and reliability requirements.

The efficiency of the modified model of HSS quality management has been confirmed during the development of a specific safety critical HSS for the Kudankulam nuclear power plant, thus defining the requirement to develop procedural guidelines for its practical application in potentially hazardous facilities design quality management.

The original interdisciplinary model of the cognitive process of expert verification enables

– dedicated management of errors and anomalies identification process management not covered by the conventional method of stage-by-stage verification based on predefined criteria;

– integrated development of theoretical facilities and tools in order to support expert analysis involving more active use of cognitive resources of verification experts at various stages of HSS design.

References

1. **Doerner D.** The logic of failure Strategic thinking in complex situations. Moscow, Smysl, 1997. – 243 p.

2. **Paulk M. and others.** Capability Maturity Model for Software. (CMU/SEI-93-TR-24). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1993.

3. **Abramova N.A.** On some of the myths regarding the quality assessment of software // Dependability, No. 1, 2004. − P. 38-63.

4. **Bekhtereva N.P.** Human brain. Superpowers and Prohibitions. Proceedings of World Congress "Results of the Millennium". – Saint-Petersburg, 2000.

5. **Festinger L.** A Theory of Cognitive Dissonance: Translated from English. Saint-Petersburg: Yuventa, 1999. – 318 p.

6. **Kahneman D., Frederick S.** Representativeness revisited: Attribute substitution in intuitive judgment. In T. Gilovich, D. Griffin & D. Kahneman (Eds.), Heuristics and Biases Heuristics and biases: The psychology of intuitive judgment (pp. 49-81). New York: Cambridge University Press, 2002.