Work 41 (2012) 730-736
DOI: 10.3233/WOR-2012-0233-730
IOS Press

The contribution of ergonomics to risk analysis in the design process: the case of a future control room

Cecilia De la Garza*, Jean-Paul Labarthe* and Louis Graglia*
**Risk Management Department, EDF R&D - 1, Av. Général de Gaulle, 92140 Clamart, France, Tel: 0033147652920, e-mail:cecilia.de-la-garza@edf.fr, jean-paul.labarthe@edf.fr, louis.graglia@edf.fr*

Abstract. The aim of this paper is to highlight how ergonomics contributes to risk analysis and risk management in a design project for a new reactor, the French EPR (European Pressurized Reactor). An iterative ergonomics design process has been conducted over the last 10 years through a Human Factors Engineering program at the French energy company EDF. A parallel has been drawn between a risk management process and this ergonomics process based on International Organization for Standardization (ISO) publications such as ISO/IEC Guide 73, ISO Guide 51, etc. The contribution of ergonomics to risk analysis is illustrated by an example: the automatic diagnosis, which is a very important technical device for safety. Five main types of risk have been identified via ergonomic analyses during the different design stages. Counter-measures have been implemented and their efficacy tested within the scope of new campaigns to assess human factors. However, the management of risks in such a design project requires the participation both of the different design entities involved in the project and of other experts in aspects of risk management, such as human reliability. The organization of collaborative participation remains a challenge to be addressed.

Keywords: risk management, design, human reliability, nuclear power plant

1. Introduction

This article demonstrates how, in a project to design a nuclear power plant – the EPR, ergonomics contributes to anticipating and managing risks relating to the use of a new sociotechnical control system.

Through a Human Factors Engineering (HFE) program, an iterative process, standard in design ergonomics, has been followed for 10 years to design control systems suitable for the different foreseeable situations. To demonstrate how ergonomics contributes to risk management, a parallel can be drawn with a dedicated risk management process. According to the International Organization for Standardization (ISO) [10], the objective of a risk management process is to arrive at a tolerable risk, in other words one accepted by the different stakeholders, through an iterative process of regular risk assessment (identification, analysis and evaluation) and risk reduction (preventive and protective systems taken into account during the design project or implemented during operation).

After presenting the main characteristics of the sociotechnical control system studied, we will cite a range of risks taken into account by ergonomics. We will then proceed with an analysis of the guiding principles common to the process of taking ergonomics into account in design and the risk management process. Next, we will describe the methodological approach specific to ergonomics within the scope of this design project. Finally, an example linked to the introduction of a new type of controller will provide a concrete illustration of the consideration of risks during the design process.

2. Control system design

Control of the design complexity of a nuclear power plant is based, among other factors, on a division into sub-systems. Here we are interested in

the design of the reactor's sociotechnical control system.

The primary role of this system is to safely and effectively control the nuclear power plant to meet production targets relating to the demands of the electric grid. It operates 24 hours a day and must be capable of managing all types of power plant operation: normal (production and maintenance), incidental and accidental (which may lead to crisis management).

The scope is limited to that of the centralized operation conducted by the operating team from the control room. This control system is in direct interface with local (logistics support, maintenance, management, etc.) and national entities (electric grid, emergency response teams, etc.).

The design of this system refers to several design "objects" for which, in the execution of this project, different technical specialties and organizational entities are responsible: the layout of the work stations and control room, the human-machine interfaces and instrumentation and control functionalities, the operating imagery, the working procedures, the organization of the operating team and that of the training program. Within the scope of the project presented here, all of these components have been subject to significant changes compared with existing power plants.

The control system's performance will be based on the correct link between all of these design "objects". The transverse role of ergonomics in the design process is based on an overall vision of the future work situation. An analysis of the interaction between the different system components subsequently enables the expected impacts on safety and performance objectives to be highlighted.

3. Risks and risk assessment: What does ergonomics take into account?

The ISO gives several definitions of risk, all of which are applicable depending on the purpose of the study and the discipline contributing to the risk analysis.

In general, risk is defined as "the effect of uncertainty on objectives" [10]. The objectives may relate to various aspects: health, safety, environment or finance, and concern different levels: body, project, power plant, product or process. Uncertainty characterizes a lack of information on the knowledge of an event, its consequences or its likelihood.

With regard to industrial safety, risk is more commonly defined as the "combination of the probability of the occurrence of harm and the severity of that harm" [10]. For a nuclear power plant, specific risks need to be taken into consideration, the most serious feared event being core meltdown, which has consequences for the environment and human population. The severity of risks associated with nuclear safety [1] is often presented with reference to the eight levels on the INES[2] scale used by the media.

With regard to the design of new work situations involving significant technological innovations, ergonomics above all participates in the design of the sociotechnical control system. The aim is to best anticipate the risks in relation with the objectives of the system studied to be attained during operation (personnel health and safety, environmental safety and preservation and production performance). It is thus a case of avoiding situations detrimental to the system's effectiveness and the attainment of the safety and performance objectives.

However, unlike reliability engineers, ergonomics has not developed specific methods or tools to precisely measure the probabilities of the occurrence of a feared event. Rather it seeks to anticipate the risks and identify and characterize the factors which could engender "uncertainty on [safety and performance] objectives" in different work situations. In this case the situations of normal, incidental and accidental operation.

To this end, ergonomics structures these interventions around a methodological approach according to the phases and progress of the design project as described below.

4. Method: intervene as early as possible and throughout the project to reconsider technical and organizational choices

With the aim of anticipating risks, the analyses will focus on the interactions between the operating teams and control systems in the power plant's

[1] Nuclear safety is all of the technical dispositions and organizational measures relating to the design, construction, operation, shutdown and dismantling of basic nuclear facilities, as well as to the transportation of radioactive substances, taken with a view to preventing accidents or limiting their effects.

[2] International Nuclear Event Scale

different operating phases: normal, incidental or accidental operation. The simultaneous implementation of the design objects that make up the future operating situations enables their usefulness and appropriateness to the operating requirements to be verified and their combination to be assessed. This enables feedback to be given to the designers on any changes to be made. The ergonomic analyses will also test and analyze the effectiveness of the technical and organizational lines of defense integrated into the system by the designer.

In the FHE program for the French EPR, the identification of risks does not constitute a finality or a dedicated study activity, as in dependability with the a priori risk analysis and assessment tools (FMECA, bowtie diagram, failure tree, etc. cf. [9]), or in human reliability with studies focused on risks affecting safety, but the detailed analysis of certain "human factor missions" which will contribute to the probabilistic safety studies ([6][4]). Broadly speaking, in ergonomics, the identification of risks is integrated as of the earliest phases, on the one hand via the knowledge brought by an HFE expert or experts to the design teams and, on the other hand, through an iterative process to assess the control systems throughout the project.

However, the identification of risks linked to future operating activities is a sensitive phase, particularly at the start of the project when all the operating tasks and components of the future work situations are only very approximatively known at specifications level (introduction of new operating concepts, reuse of part of the existing power plant but within a different scope, etc.).

The first stage will consist of specifying and agreeing with the different stakeholders (future operator, engineers and ergonomist) on a model of the large families of tasks to be conducted in the control room (taking over the work station, monitoring, tracking maintenance interventions, conducting periodic tests, etc.) and on an initial operational breakdown of the control systems used to execute these tasks. Particular effort will be made in the analysis of the major changes compared with current power plants.

Risks will be identified: i) based on the opinions of experts relying on different types of knowledge; ii) according to a prospective "causes-effects" approach; iii) or even according to an iterative approach through evaluations conducted on models or simulators.

4.1. An expert opinion to contribute to risk analysis

The identification and analysis of risks based on experts' opinions primarily rely on three fields of knowledge:

- Knowledge of existing operating situations, through analyses of the operating teams' activity;
- The field of ergonomic standards (ISO 11064, ISO 9241, IEC 60964, etc.) and design reference bases specific to the nuclear industry (NUREG 0700, etc.);
- Knowledge in the field of human and social sciences. By relying in particular on models of the activity and models of the cognitive operation, we are able to anticipate situations which risk creating difficulties in understanding, processing information, etc. (cf. for instance [1], [2] or [8]).

The ergonomist is not alone but is considered to be one of the experts and is consulted either on occasion to reread a document or give an opinion on a technical choice, or within the scope of pluridisciplinary working groups. These groups have been established to break down and specify operating concepts in relation to the different design objects (work stations, HMI, imagery, documentation and organization).

This approach is favored in the earliest phases of the design project but can be useful throughout the project as new problems or questions arise.

The approach consists of making forecasts based on knowledge of similar situations on existing power plants. It relates to two levels of analysis: a micro level, targeting the interaction between the user and the design object studied to identify risks relating to difficulty of use, and a macro level, targeting integration within the sociotechnical system to identify risks of interference between design objects or of ineffectiveness of the operating group and the organizational and technical lines of defense.

4.2. Top-down prospective approach to ergonomics for risk analysis

This analysis can then be complemented by a top-down prospective "causes-effects" approach to highlight the imaginable consequences on the control system's behavior: "What happens if I lose this control system or that controller?", "…if I make such and such input error?", "…if I don't detect this information?", "…if during the design process I can only present the information in this way?", "…if during the design project the product's off-the-shelf

HMI functionality only partially meets my needs?", "...if I change the organization of my team?".

This prospective approach is conducted in the working group and pluridisciplinary meetings to gather the different points of view. End users can be involved in this.

4.3. "Bottom-up" prospective approach: simulation to forecast the risks and difficulties of the future work situation

This approach is also “prospective” but is based on situational training with the future operators within the framework of evaluations conducted using models or simulators. The purpose of these experiments is to confront operators with difficulties they may encounter in their future activity. The results of these tests will constitute initial feedback allowing forewarning about the potential uncontrolled or unexpected negative effects. These simulations are then a tool for diagnosis and forecast for future operating activity. They are an essential stage of the design which, in view of the scale of the EPR industrial project, need to be updated as the project progresses. The simulations constructed throughout the project to test the different control systems are not (yet) considered definitive, but are a necessary stage for moving forward. Simulation is a basic tool for the diagnosis and forecast of future activity and even the future work situation concerning performance of the teams and the safety and reliability of the control system. Simulations suited to the requirements at the time have been carried out throughout the project. These have taken the form of static models (on paper for screenshots or instructions, on the computer screen for HMI specifications and images, on a wooden scale model for fitting out the control room, etc.), dynamic models coupled with a PWR type process for carrying out overall or targeted evaluations of control systems, and, finally, a full scale EPR simulator. These simulations are based on the construction of scenarios intended to be realistic and representative, at the time of the evaluation, of the likely future operating activity. They have involved the participation of end users whose status has changed as the project has progressed [5].

4.4. Conclusion: Assessing ergonomic risks is a qualitative approach

In a risk management process, the risk identification phase is followed by an assessment phase both to decide whether the counter-measures implemented are effective and to decide with the project team whether the residual risks are tolerable or not. This assessment phase also allows the different risks to be ranked, which then enables the priority with which they are dealt to be defined.

Ergonomics will above all concern the overall assessment of the work situation; there is no evaluation risk by risk. This concerns the risk resulting from the interactions between the operating teams and control systems. The situational training constructed by the ergonomist in collaboration with the different stakeholders (operator, designer and trainer) and implementing all of the design objects enables risks or difficulties not previously identified to be discerned.

Here it is often difficult for the ergonomist to define a level of criticality for each identified risk, in the sense of dependability or in the same way as the reliability engineers, giving a precise measure of the probability and severity. In other words, it is difficult to quantify the relationship between a problem with using a design object and a feared event at system level affecting security, productivity or health/safety. This is most often represented by the display of potential impacts with a ranking based on at best three to four levels to qualify severity and probability.

The risk assessment and identification of the counter-measures to be implemented, and the priority with which they are dealt, are then subject to a debate and consensus between the different stakeholders (operator, engineers and ergonomist). This risk assessment within the project is then questioned within the scope of the inquiry with the French Nuclear Safety Authority. In the next section, the case of a controller important for safety, the automatic diagnosis, will illustrate the approach.

5. Results: the case of the automatic diagnosis

In the operator's specifications, a new controller has been introduced to make reliable the choice of operating strategies to be applied in Incidental/Accidental Operation (IAO). This is the Automatic Diagnosis (AD) which has the role of

permanently analyzing the power plant's status. In the event of a change to the plant's status and following an alert of severity 4, the AD responds with a specific audible alert and recommends an operating strategy (procedure) to be applied according to whether it is a case of accidental or incidental operation. This recommendation is displayed on an image dedicated to the AD.

Through joint work with the technicians and engineering units involved in the project, five types of risk have been identified during different stages of the design process concerning the automatic diagnosis.

During the initial specifications, two main risks have been identified and studied.

1) The first focused on the unavailability of the automatic diagnosis. The counter-measure consisted of guaranteeing the robustness of the automatic diagnosis from the technical standpoint and proposing an alternative in the event of automatic diagnosis failure.

2) The second risk was linked to acceptance by the team. In effect, the team is responsible for the emergency operation, but no longer decides which emergency procedure to apply. This kind of risk required an additional barrier to be raised through training.

3) The third type of risk related to the execution of the design project and referred to the inability to guarantee the robustness of the programming (or its demonstration). This risk was analyzed during the detailed specification phases and the counter-measures have led (among other benefits) to limiting the complexity of execution by reducing its scope for the identification of operating strategies to be applied in the accidental domain. For the incidental domain, which concerns the power plant's less serious impaired states from a safety point of view, the choice of strategies to be applied remains the responsibility of the operator, who uses guidance instructions on paper. This point therefore required the analysis of another type of risk linked to the introduction of a different level of guidance. In effect, in accidental operation the AD recommends the choice of strategy to be applied and permanently analyses whether it is indeed appropriate, whilst in incidental operation the AD permanently ensures it does not come under accidental operation but leaves the operator to choose the strategy to be applied and regularly ensures it is indeed appropriate. The associated counter-measures rely mainly on the AD's doctrine of use and training, ensuring during the successive assessment phases that the additional workload relating to the manual guidance phases during incidental operation do not cause the power plant to deteriorate into the accidental domain.

During the initial assessment phases in 2003 and then in 2005, two other types of risk appeared.

4) The fourth type of risk taken into account was linked to the lack of understanding of the operating procedure recommended by the AD and its relation to the power plant's status. The consequence of this may be the teams' rejection of this controller, as it is they who are responsible for the operation implemented, but application of the AD is dictated to them. As long as the latter is considered to be "valid", its application can only be brought into question on the joint decision of the operating team (issue of shared Human (operator) vs. Machine (the designer with the diagnostic help tools) responsibility). This risk is inherent in the consequences of removing previously "manual" phases in conducting the status diagnostic and the move towards an operating strategy (execution of a series of tests with search for information and identification on logic diagrams of the parameters at the origin of a given strategy). With the introduction of the AD and its initial implementation, the operators lost one of the tools in constructing a mental map of the power plant's state of impairment and the process of deciding between strategies. They submitted to the recommended operating process more than they could anticipate and manage it. The counter-measures related to redefining the content and presentation of the information on the AD's images and explaining the recommended result through images breaking down the process followed by the machine to recommend an operating strategy.

5) The fifth type of risk identified during the second assessment campaign conducted in 2005 was linked to problems of use. Questions were raised about the possible "non-detection" of a change of result from the AD or inappropriate manual activation. In effect, there are three specific situations where, subsequent to the attainment of a threshold, the AD must be manually activated by an operator (example, upon a primary leak report). The counter-measures related to changes to the HMI and technical solutions (audible alert and command with validation).

These different risks and their counter-measures were reviewed during a test campaign held in 2009 and appear to be under control.

Of the four assessment campaigns with the operating teams where the AD was used, the first two iterations in particular have led to consolidating the risk analysis and defining the counter-measures (2003 and 2005). The next campaigns (2008 and 2009) did not bring any specific changes, but enabled the AD's acceptability and the added value brought to the teams' operational activity in IAO to be reinforced. More subjectively, by progressively increasing the total volume of situational training, they enabled risks to be detected relating to phenomena that occur over a longer term, such as "diverted" uses of certain functionalities, which Leplat and Cuny refer to as catachreses [7]. These can be positive or negative depending on the situation, i.e. they may or may not increase security, safety and efficiency. These lessons must be taken on board, whether during the design phase or within the scope of the team training program.

6. Discussion

The reflection conducted as part of the EPR design project demonstrates that the contribution of ergonomics to the identification and management of risks has not been clearly identified by the different entities involved in the project. There are several reasons for this:

- Ergonomics does not specifically target the analysis and management of risks. The role of ergonomics encapsulates risk analysis in an overall approach, the purpose of which is to take human factors into account in the design process. This is a case of guiding the design choices by taking account of feedback on existing situations, reference bases and knowledge gained from literature relating to human performance (cognitive and physiological performance). Risk analysis within the ergonomic approach consists of relying on different iteration levels to identify other risks likely to arise in future situations subsequent to technological and/or organizational changes. It is here that the assessment of the design choices via successive simulation campaigns makes perfect sense.
- The contributions of ergonomics constitute a "continual process" throughout the project and change as it progresses. There is no phase dedicated to risk analysis, but it is an objective continually present in the different ergonomic interventions throughout the design project: during the very early phases to define the important design principles, during the establishment and rereads of specifications, during the phases to analyze the needs of future users, during the phases to assess the different choices and changes to them, and so on.

In conclusion, ergonomics combines *a priori* and *a posteriori* risk approaches throughout the design project during which the risks may change. Some risks are identified earlier than others and this largely depends on the information available at a given time during the project. In effect, a specific feature of ergonomics consists of seeking to anticipate risks by reproducing probable future situations during simulations [3]. The simulation resources and scenarios become increasingly complex as the design project progresses [5]. At the same time, room for maneuver in the design reduces as technical and organizational changes become increasingly difficult to implement. In addition, ergonomics does not enable every possible risk to be identified; it is just one competency among others than can contribute to risk management.

Thus, with a view to a more exhaustive and integrated approach to risks, this "continual" risk analysis process, specific to ergonomics, must be combined with other areas of knowledge and expertise.

Throughout the project, the ergonomists have collaborated with the engineers coordinating the project execution, the designers from the different entities involved for the various control systems (HMI, imagery, set points, etc.) and the future operator. And for some time, reliability engineers have been participating to model the control system, clarify the impact of certain design choices and contribute to a probabilistic assessment of human reliability. However, the different approaches that contribute to the control of risks relating to human activities (ergonomics, human reliability, probabilistic studies and safety studies), although essential, are often conducted in parallel or sequentially and would benefit from being more integrated with each other in the design project. Consequently, methodological developments are to be made in this direction if we wish to improve and enrich the risk analysis and management process. It is certainly desirable to explain the participation of each of the competencies within the Human Factors Engineering process, attempting to associate them

with the major phases and the different iterations of the design project.

References

[1] Amalberti, R., Montmollin, M. de, & Theureau, J. (Eds.) (1995). Modèles en analyse du travail. Mardaga : Liège.
[2] Amalberti, R. (1996). La conduite des systèmes à risques. Paris : PUF.
[3] Daniellou, F., & Garrigou, A. (1992). Human factors in design: sociotechnics or ergonomics? In M. Helander & M. Nagamashi (Ed.), Design for manufacturability and process planning (pp. 55-63). London: Taylor and Francis.
[4] Gallet, M., Deriot, S., Le Bot, P., Primet, J.(2003). Les données des EPS : fiabilité des matériels ; défaillances de cause commune, facteurs humains. Revue générale nucléaire, n°1, 30–35.
[5] Labarthe, J-P, De la Garza, C. (2011). The human factors evaluation program of a control room: the French EPR approach. Human Factors and Ergonomics in Manufacturing, 21 (4), 331-349.
[6] Le Bot, P., Desmares, E., Bieder, C., Cara, F., &, Bonnet, J.L. (1998). Mermos: an EDF project for updating probabilistic human reliability assessment. Revue générale nucléaire. International edition, vol. A, 32–39.
[7] Leplat, J., Cuny, X. 1977. Introduction à la psychologie du travail. PUF, Paris.
[8] Rasmussen, J. (1986). Information Processing and Human-Machine Interaction. Editions North Holland Publisher: Amsterdam.
[9] Villemeur, A. (1988). Sûreté de fonctionnement des systèmes industriels. Eyrolles: Paris. p. 744.
[10] ISO Guide 51 Safety aspects – Guidelines for their inclusion in standards. 1999.
[11] ISO Guide 73 Risk management — Vocabulary. 2009.
[12] ISO 11064 Ergonomic design of control centres. 2004 (7 parts).
[13] ISO 9241 Ergonomics of human-system interaction (different parts, including part 210: Human-centred design for interactive systems). 1998.
[14] US NRC (Nuclear Regulatory Commission) NUREG 0700 (Rev. 2). Human-system interface design review guidelines. 2002.