HFE IN THE DESIGN OF THE SOCIO-TECHNICAL SYSTEM OF THE CONTROL ROOM OF A NEW GENERATION REACTOR: ISSUES FACED DURING MULTISTAGE VALIDATION

Stanislas Couix
EDF R&D – Management des Risques Industriels – Facteurs Organisationnels et Humains
7 bd Gaspard Monge, 91120 Palaiseau, France
stanislas.couix@edf.fr

ABSTRACT

This paper deals with the contribution of Human Factors & Ergonomics (HF&E) experts to the design of the control room (CR) of a new generation reactor (NGR), our view of the multistage validation (MSV) process and the issues faced during it.

Our approach to MSV was to articulate two points of view: the designers' point of view (test and explore various design options) and the regulatory authorities' point of view (validate the performance of the socio-technical system of the CR). To perform this articulation, both tests and validation shared the same method and goals.

The main issues faced during this process were to (1) get a coherent and integrated version of the full-scope simulator when the design of the socio-technical system of the CR was still in progress, (2) determine when to stop MSVs, and (3) define a criterion for the sampling of operational conditions. The first issue led us to the conclusion that specific project milestones synchronising the design of every part of the CR have to be planned early in the project in order to mitigate the risk of delaying WSTs (Whole System Tests). Regarding the second issue, we advocate that no further WSTs are required when the last modifications brought to the CR design have no significant impact on crews' activities. Finally, concerning the last issue, we think that performing WSTs in all classes of situations a crew may face during operating the plant is necessary.

Key Words: Human Factors & Ergonomics, Design, Control Room, Multistage Validation

1 INTRODUCTION

1.1 Context

EDF is currently building a new generation reactor (NGR). This reactor has four key characteristics that have a strong impact on human activities in the control room (CR).

- The main human system interface (HSI) between CR operators and the instrumentation & control (I&C) is computerised.
- Part of the procedures used by CR operators is on paper, the other part is computerised.
- The NGR has a higher level of automation than any other French nuclear power plant (NPP).
- This high level of automation has led us to define a new operating crew concept.

To anticipate the impact of these evolutions and innovations on the activities of CR operators, and, consequently, on the performance and the safety of the plant, a Human Factors Engineering (HFE) programme has been developed. The aim of this plan was to integrate human factors and ergonomics (HF&E) experts into the design of the CR (and other parts of the plant as well).

This programme was driven and led by an HF&E expert who had strong links to the global project management. It is a very important point as it provided a human factors (HF) point of view in all the major design decisions made during the project. Another important role of the HF supervisor and coordinator was to update the programme and to decide in which plant element, some HF design inputs were needed. Thanks to this, the HF team at EDF R&D has been involved since the beginning of the detailed design phase and will stay involved after the plant commissioning, until the end of the first production cycle of the plant.

1.2 Control Room as a Socio-Technical System

Fig. 1 shows a picture of the main NGR CR, which is composed of 4 computerised workstations for the 2 operators, the deputy shift supervisor and the shift supervisor. The screens on the work station are used to control and monitor the plant and the screens in front of operators' desks are used to give operators a more global view of the state of the plant. In case of a failure or the maintenance of the main HSI, operators have to use a hardware HSI.

Figure 1. 3D view of the NGR CR.

From our point of view the CR should be considered as a socio-technical system. This system is composed of the physical layout of the CR, the people that are operating the plant, the operating procedures they use, the human machine interface they interact with, and the way the operating crews are organised to face normal, abnormal, accidental and emergency situations. Therefore, CR design means the design of all the elements of the socio-technical system of the CR.

2 DESIGN AND VALIDATION APPROACH ADOPTED BY HF&E EXPERTS

Throughout the design of the CR, we adopted an iterative, participative and user-centred approach. This means that the future crews have not only participated during the tests and validations in the full scope simulator, but also in many design workshops and reviews. Fig. 2 shows an overview of the HF&E contribution to the design of the CR.

Our design approach is strongly influenced by the French ergonomics approach of design (e.g., [1], [2], and [3]). This approach is focussed on the anticipation of future work situations. Work situations are

composed of all the elements of the socio-technical system of the CR plus the context of the operation which greatly influence operators' activities and goals.

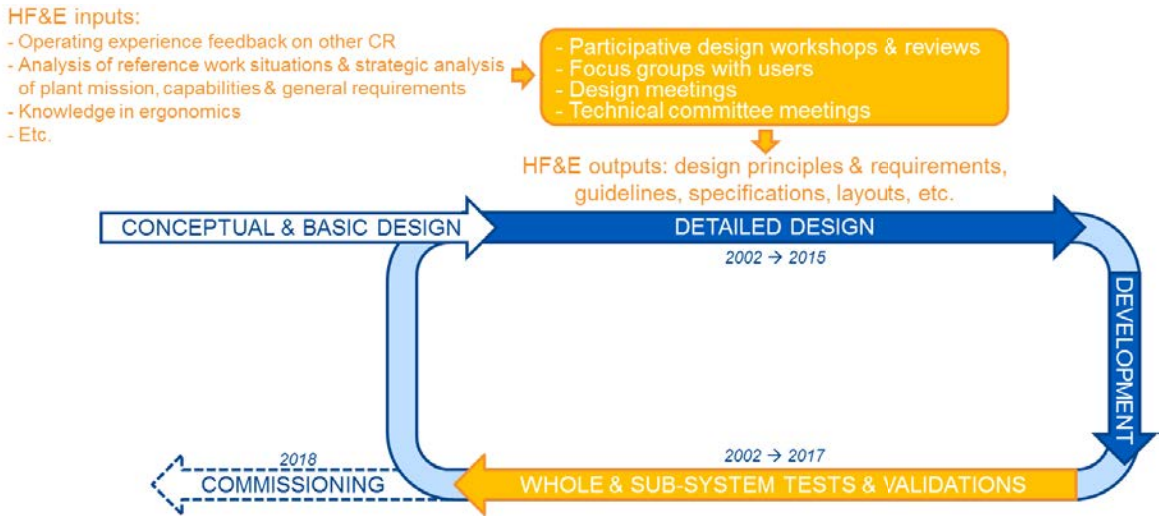

Figure 2. Overview of the HF&E contribution (in orange) to the design process.

We consider that human activity is "situated", meaning that humans are acting according to the characteristics of situations [1, 3]. Therefore, if the characteristics of the situation change, the human activity will change accordingly. From this perspective, designing means the building and forecasting of all the elements of the future work situations (the HSI, operating procedures, etc.) to ensure that the future operating crews will be able to cope with normal, abnormal, accidental and emergency contexts in an efficient way. Building and forecasting the future work situations are strongly linked but they will be presented separately.

2.1 HF&E Approach during Detailed Design

During the design phase, HF&E experts organised many participative design workshops and reviews, as well as focus groups with crews where design options where constructed and debated. We also participated in design and technical committee meetings where requirements and specifications were validated and prioritised.

Our work during these meetings was based on the crews' needs identified in reference work situations (RWS, [4]). An RWS is a work situation that shares many characteristics with the future situation. To identify all RWSs, it is first needed to identify the future work situations associated with the operation of the future system (the NGR in our case). This is the purpose of what we call a strategic analysis. This analysis is based on a review of documents describing the future plant's mission, functions, and requirements. For example, Automate Diagnosis (AD) is a new NGR function designed to help operators decide which operating strategy and operating documents have to be applied according to the situation in case of an accident. The use of AD and its possible malfunction or loss during operation were identified as possible work situations.

After determining the possible work situations, it is required to identify the associated RWSs. Based on our knowledge of operation in other French NPPs, we concluded that many future possible work situations shared similar characteristics with existing work situations in these NPPs. These existing work situations were then considered as RWSs. For instance, the main HSI of the NGR is computerised. The use of this HSI during normal, abnormal, accidental and emergency contexts was then identified as future

possible work situations. Some existing French NPPs are equipped with a computerised HSI as well. The use of this HSI in various contexts in these NPPs was then considered as RWSs. Nonetheless, some future possible situations do not exist in other French NPPs. The use of AD and its possible malfunction or loss during operation are examples of these kind of situations. Associated RWSs have to be found elsewhere. For instance, systems like AD exist in some other industries or work settings. The use of AD in these industries was then considered as RWSs.

Then, it is required to analyse operators' needs. We postulated that operators' needs depend notably on the characteristics of work situations. Thus, operators' needs associated with the operation of the future system can be partly derived from the needs analysis identified in RWSs. The method used to analyse them depends notably on the ease of access to these situations. To identify the operators' needs in RWSs associated with the operation of French NPPs, several observations, interviews, and an analysis of the relevant operating experience feedback (OEF) from other French NPPs were conducted. For instance, OEF and observations of CR operators' activity in some French NPPs pointed out that the way computerised procedures were designed may influence the way operators understand the effects of the actions they are carrying out. Therefore, for the NGR, it has been decided to change radically the design concept of computerised procedures.

To analyse needs associated with RWSs in other industries, direct observations and interviews with operators or an OEF analysis were not possible. Other techniques have been used. For instance, to analyse the needs associated with the use of the AD, a review of scientific literature on cooperation between humans and systems like AD was performed. This analysis was completed by a "Wizard of Oz" technique [5] where the functioning of the AD was simulated by an experimenter.

Of course, the needs identified and the design decisions made were also strongly influenced by other technical constraints imposed by plant mission and system requirements. They were also strongly influenced by our general knowledge in HF&E. We also took into account the results of the iterative tests and the validations we performed throughout the project.

2.2 Iterative Testing of the Future Control Room

If the aim of the design phase is to build the future work situations, the aim of the test phase is to explore the performance of future crews in the work situations designed or that will be designed. This allows us to gain access to the future activity of the crew. In this way, we can easily identify HF issues and human engineering discrepancies (HED), and solve these issues before plant commissioning. The point here is to check that the various design guidelines, principles and rules used or that will be used during the design of the whole socio-technical system of the CR will allow efficacy and efficiency of the system.

Two types of tests can be distinguished: sub-system tests[1] (SST) and whole system tests (WST). SST are performed on parts or elements of the future CR associated with one or more classes of situation. For example, we performed an SST on the operating documents used by operators in emergency situations. We also explored the HSI look and feel with future users using paper mock-ups. These kind of tests are ideal to explore and evaluate various and new designs of some elements of the CR. The issue associated is that elements are tested separately. On the contrary, in real work situations, all the elements are used in conjunction with one another.

The point of WSTs is to overcome this limit. These tests are performed in a full scale simulator in every class of situation the crews may face. This kind of test is used to evaluate the coupling between all the elements of the CR and explore various designs. For instance, during the NGR design, two WSTs were led to test two crew concepts.

[1] The term refers to sub-system validation by [6]. We prefer to speak of test instead of validation as we consider that validation can only be performed using the whole socio-technical system of the CR.

In the case of NGR design, the SSTs were only led by HF&E experts. On the contrary, a multidisciplinary team composed of HF&E experts as well as safety experts led the WSTs. These experts have also been helped by operating experts, training experts, and designers to analyse the results of the tests.

During the NGR design, 17 HF tests were performed (5 WSTs and 12 SSTs) from the end of the basic design. The first test was a WST aiming at determining if the design orientations decided during the basic design were viable. Many SSTs followed to improve the design of each part of the socio-technical system of the CR. Since the end of the detailed design, only WSTs have been performed. The representativeness of what was observed during all these tests was closer each time to the future system. In this way, we were more and more confident in the ability of the socio-technical system of the CR to operate the plant safely. Nonetheless, the HFE programme will not end at plant commissioning. HF evaluation will be performed during the try-out and start-up phases as well as the first operating cycle.

2.3 Whole System Tests as Part of the Verification & Validation Process: Our View of Multistage Validation

The workforce and time associated with WSTs is significant. During the NGR design, it took 1 year to plan each WST, to build the testing scenarios and to design the test protocol. The WSTs were usually performed in 2 months and involved 3 trainers, 15 operators, 5 HF and safety experts, and 3 other experts on a full time basis. Each WST generated more than two hundred hours of video on each of the thirty cameras used to record the test and the same amount of audio records from the debriefing organised after the simulation. It required 3 months for 4 HF&E and safety experts to analyse the results and another 6 months to process the results into design inputs. Therefore, there is a need to rationalize the economic effort associated with the Verification and Validation process (V&V).

Many approaches to multistage validation (MSV) have been proposed and used (see [6] for a short review). The way we did this during the NGR design was to integrate the WST and the validation process into what is our vision of MSV. This was made possible because we unified the WST method and the validation of the socio-technical system of the CR.

Indeed, the method for both purposes includes the same:

- Goal: make sure that the performance of the socio-technical system of the CR met the expectations in terms of performance;
- Setting: a full-scope simulator representative of the future CR, including operating documents and HSI;
- Users: trained[2] users representative of future crews;
- Classes of situations: tests and validations need to ensure that the performance of the system met the expectations in a collection of representative situations;
- Independent evaluation team;
- Data collection technique (observation, debriefing, interviews, audio and video records);
- Data analysis technique (quantitative and qualitative techniques were used).

Thus, we consider that the successful test of any part of the system in a WST setting can be part of the MSV process. For example, if we test 3 crew concepts (C1, C2, C3) in 4 key situations (S1, S2, S3, S4) and we conclude that the best option is C2, then the C2 is considered validated in the given situations, and the test could be part of the MSV process. Of course, as only 4 situations have been used during this

[2] Of course, as the entire training for a licenced operators is a process lasting 2 years, it is not possible to have fully trained and licenced operators for the first WST.

first phase, other validations in different situations (S5, S6, etc.) will be needed to strengthen the validation, hence the term MSV. However, if any part of the socio-technical system of the CR (like HSI) changes significantly after the first C2 test, the test cannot be fully integrated into the MSV process. If C2 is still considered validated, a validation of the new HSI with C2 in S1, S2, S3 and S4 will be needed.

Another aim of the test phase is to tackle problems during development. Sometimes, HF requirements, guidelines or specifications are not always sufficiently detailed or can be contradictory to other design rules. Moreover, design guidelines, requirements and specifications are not always perfectly applied by developers (e.g., [7] & [8]). This can result in HED that will be tackled when preparing or during the tests.

Therefore, in the same manner as for validation, part of the verification process was performed during the preparation of WSTs. Indeed, during the preparation of any WST, we need to make sure that the operating documents and HSIs used during the test respected the HF design guidelines, rules and specifications. Many HEDs were found during this process.

3 SOME ISSUES FACED DURING THE MSV PROCESS

The HFE programme we applied during the NGR CR design led us to single out and address many issues. In this section, only some are detailed.

3.1 WSTs as a way to integrate early the various parts of the CR

The first of these issues, is linked with the requirements that have to be met before starting a WST. As shown in Fig. 3, several elements are needed to perform a WST: trained operators, operating documents, scenarios, a process as well as an instrumentation and control simulator, a simulated HSI, crew's organisation. To get all of these, other requirements have to be met. For instance, to have scenarios, a process and I&C simulator, information on crews'organisation, and operating documents are needed as well as the work situations (identified in the HFE programme) to validate. In the same manner, to get a process and I&C simulator, other requirements have to be met, and so on. The main requirements to get others elements needed to perform a WST are described in Fig. 3, but they will not be described further as this is not the point of this communication.

Despite the fact that the design of each element is still in progress, these elements have to be coherent before a test can be started. For instance, if the plant's process and I&C is at version 2.1.2, the process simulator, the operating documents and rules, and the simulated HSI have to be compliant with this version of the process. Otherwise, for instance, the operating documents will not work on the simulator.

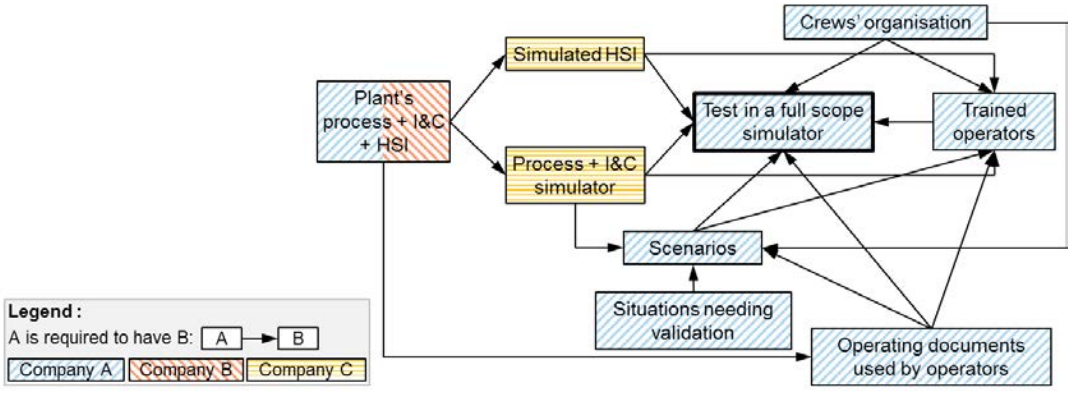

Figure 3. Elements required to perform a WST in a full-scale simulator.

The issue is that different companies and different units within the same company are involved in the design of the elements required to perform a WST in a full-scale simulator. For example, the process simulator is built by company C from the process that has been designed by companies A and B which are responsible for different parts of the plant. Therefore, any delay in any element needed to perform a test in a full-scale simulator may delay a WST.

From an HF&E point of view, this has led to the conclusion that the HFE programme is extremely dependent on the project planning and management. Indeed, WSTs imply that every part of the system is coherent and integrated early, and this has to be done when the design is still in progress. Therefore, specific project milestones synchronising the design of every part of the CR have to be planned early in the project in order to mitigate the delays of WSTs.

3.2 When to Stop MSV

The second issue we faced during the NGR design was to find a relevant criterion to indicate when no further validation is required. From an economical point of view, this question is of great importance. The plant has to start production. However, we have to be confident that it will be very safe from an HF point of view.

The decision process we followed to determine if new WSTs were required is described hereinafter. This is a social process as many experts from different domains are involved. During each WST, some HF issues or HEDs may be identified by HF&E experts and safety experts on each part of the socio-technical system of the CR. If no HED or HF issue is identified on a part of the CR, this part is validated. HED and HF issues identified are then further analysed by a multidisciplinary team composed of HF&E experts, safety experts, designers, operating experts and trainers. The goal of this team is to determine if a modification of any component of the CR is required before commissioning the plant. If no modification is required, the component is considered as validated. If the answer is that a modification is required, a solution is sought. When the solution is found and approved by everyone, another group composed of HF&E experts, operating experts and trainers have to determine if the modification will have a significant impact on crews' activities. If the group cannot be very confident in the answer, a new WST in the same kind of situation where the problem was identified has to be led. Otherwise, the modification can be integrated into the design and no further WST is required. To sum up, no further WSTs are required when the last modifications brought to the CR design have no significant impact on crews' activities. The whole process is summarised in Fig. 4.

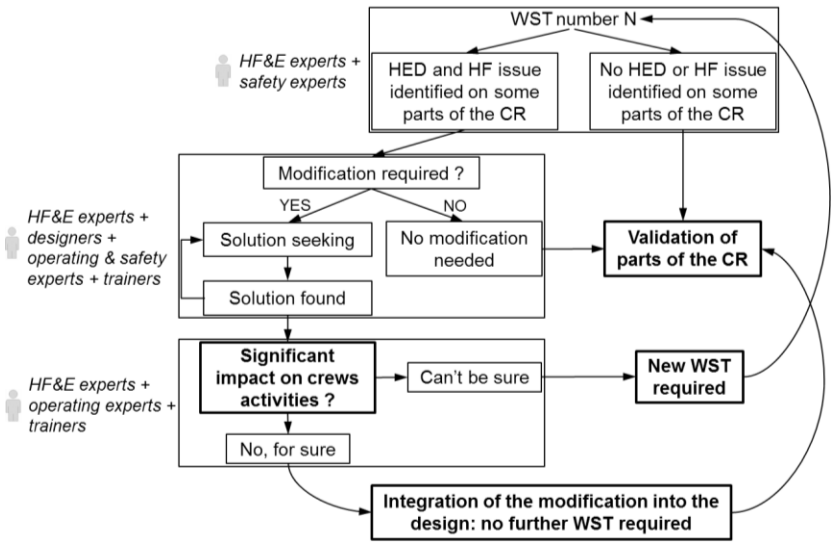

Figure 4. Decision process followed to determine the necessity of new validation in a WST setting.

To make this process work, two issues have been addressed:

1. In which kind of situation the new WST has to be performed?
2. How much is a significant impact of crews' activities?

Regarding issue 1, from our point of view, and contrary to what we think is advocated by [9], the best situation in which the new WST should be performed is not necessarily the same situation as where the problem arose. Using exactly the same situation may lead to a bias in the WST. At the end of the design process, the only operators that can participate in WSTs are the ones who will start up the plant. In the NGR, for instance, 6 teams of licensed operators will contribute to it. To be representative, 4 teams have always participated in each WST[3]. Therefore, if the same situation is used for the new WST, at least one team will know the exact scenario which will bias the results. Moreover, people talk, and operators are people too. It is very difficult to be sure that no information about the scenario used during the last WST did not leak. Therefore, when a new WST was required to validate a design modification, we used an equivalent situation. Situations A and B are considered comparable if they belong to the same class of situation. A situation belongs to a class of situation if they share the same characteristics. Two situations do not belong to the same class of situation when their characteristics are different to the point where crews' activities differ significantly in the two situations. This point led to issue 2.

Regarding issue 2, no quantifiable criteria have been identified to assess the significance of an impact on crews' activities. This is the reason why this significance is evaluated by a group of experts in crews' activities: HF&E experts, operating experts and trainers. As it has already been said, we assume that the activity depends on the characteristics of the situation. Therefore, if the design modification changes significantly a characteristic of the situation, the crews' activity will change significantly. A class of situation is characterised by:

- Type of HSI, e.g. hardwired HSI vs. computerised HSI;
- Functions of I&C software;
- Roles or tasks assigned to crew members;

[3] One team will participate in order to test if the scenarios go technically well and to assess the difficulty of each scenario.

- Type and structuration of operating document used by CR operators, e.g. computerised vs. paper procedures, or emergency procedure vs. normal conditions procedures, etc.;
- Operational condition, e.g. normal vs. emergency condition[4].

For example, if the role assigned to one or more crew member is modified, then we assume that their activity will change significantly and a new WST will be required. On the contrary, a change in the wording of an instruction in a procedure will not change significantly the kind of crews' activities.

3.3 Sampling of Operational Conditions Used during WST/MSV

It is widely acknowledged that testing all situations a CR crew will face is not possible. Therefore, a sampling of the operational conditions is required. The second issue we faced during NGR CR design was to define a criterion for the sampling of operational conditions. The criterion we used was based on the concepts of the class of the situation and the crews' activities.

As it has already been said, the purpose of the tests is to verify that the various design guidelines, principles and rules used (or that will be used) during the design of the whole socio-technical system of the CR will allow efficacy and efficiency of the system. During the NGR CR design, we assessed the efficiency and efficacy through qualitative and quantitative techniques. The quantitative techniques were notably based on the evaluation of human actions that are considered important for safety and/or availability of production. The qualitative techniques were based on the analysis of crews' activities[5].

So, from our point of view, it is necessary to evaluate the performance of all the various types of activities performed by the crews. As it has already been said, these activities depend on the characteristics of the class of situations. Therefore, we need to perform tests in all classes of situations a crew may face while operating the plant. In each class of situation, at least one situation must be used during a WST. Ideally, two situations of the same class of situation must be seen.

For example, during the 4th WST of the NGR CR, the performance of the socio-technical system of the CR was validated in 17 classes of situations[6]. The class of situation named "operating of sensitive transient in normal condition using the main computerised HSI" was instantiated in two situations, namely the seeking for the reactor's criticality (reactor's divergence) and the collapsing of the pressurizer's steam-bubble. The selection of a situation among all the possible situations belonging to a class of situation was supported by operating experience feedback, feedback from trainers, and the strategic analysis of NGR innovations (see § 2.1). The purpose was to select various levels of difficulty. Thus, if only one situation was to be selected, the most challenging one was preferred.

4 CONCLUSION

This communication presented the HF&E contributions to the design of the socio-technical system of the NGR CR. More specifically the aim was to present the framework we propose to clarify the links between the tests and the validation process and the issues faced during this phase of the NGR CR design.

Our approach to the HF&E contribution to design and validation was based on the concept of the class of the situations and the crews' activities. These concepts have been used throughout the design:

[4] In France, emergency procedures and normal condition procedures are different as they rely on a different operating philosophy.

[5] In French ergonomics (e.g., [1], [3]), human activity is considered as an integrated and meaningful whole that depends on the characteristics of the working situation and the characteristics of the actors. The working situation is composed of the operational conditions and the various CR components (HSIs, operational documents, roles assigned to operators, etc.). Thus, the analysis of crews' activities allows us to access the joint use of the various CR components, and all the needs, HED and HF issues associated.

[6] It is important not to confuse classes of situations and testing scenarios. Testing scenarios are composed of various classes of situations. For instance, 7 scenarios have been built to be able to analyse the 17 classes of situations.

- During the CR basic design, classes of situation have been used to define the concept of the operation and the HFE programme to check that each class of situation will be validated during at least one WST.
- During the CR detailed design, classes of situations were used to identify many needs and define many CR components like HSIs (HSIs considered as a support to the task and activities of the crew in all classes of situations).
- During the MSV process, classes of situation and associated crews' activities were the basis used: (1) for the sampling of operational conditions, (2) to build the scenarios used for WSTs, and (3) to stop MSV.

Our approach to MSV is to articulate two points of view: the designers' point of view and the regulatory authorities' point of view. From the designers' point of view it is necessary to test and explore various designs of some sub-systems of the CR (during SSTs) as well as the whole CR (during WSTs). In order to tackle and correct as early as possible the performance issues identified, these tests have to be performed during the whole detailed design phase in an iterative manner and have to be more and more representative. From the regulatory authorities' point of view, the validation of the socio-technical system of the CR should demonstrate its high performance in various and representative operational conditions.

The way we articulated both points of view was in the use of the same method for both the WST and the validation of the socio-technical system of the NGR CR. Indeed, both purposes have the same goals, use the same settings, data collection techniques and data analysis techniques, and are performed by the same actors with the same users in the same classes of situations. Thus, we consider that the successful test of any part of the system in a WST setting can be part of the MSV process. However, if between two WSTs, significant changes have been brought to any part of the CR, this part has to be tested again in the same classes of situation to be validated. In other words, the situation to be used for the new WST must belong to the same classes of situation used during the tests that have shown the inadequacy of the CR part to support the high performance of the whole socio-technical system of the CR.

The main issues faced during this process were to (1) get a coherent and integrated version of the full-scope simulator when the design of the socio-technical system of the CR was still in progress, (2) determine when to stop MSV, and (3) define a criterion for the sampling of operational conditions. The first issue led us to the conclusion that specific project milestones synchronising the design of every part of the CR have to be planned early in the project in order to mitigate the delays of WSTs. Regarding the second issue, we advocate that no further WSTs are required when the last modifications brought to the CR design have no significant impact on crews' activities. Finally, concerning the last issue, and considering our definition of the concept of the class of the situation, we think that it is necessary to perform WSTs in all classes of situations a crew may face while operating the plant.

5 REFERENCES

1. P. Falzon, *Constructive ergonomics*, CRC Press, Boca Raton, U.S.A (2014).
2. F. Daniellou and P. Rabardel, "Activity-oriented approaches to ergonomics: some traditions and communities", *Theoretical Issues in Ergonomics Science*, **vol. 6**, no. 5, pp. 353–357 (2005).
3. F. Daniellou, "'The French-speaking ergonomists' approach to work activity: cross-influences of field intervention and conceptual models", *Theoretical Issues in Ergonomics Science*, **vol. 6**, no. 5, pp. 409–427 (2005).
4. F. Daniellou, "L'ergonomie dans la conduite de projets de conception de systèmes de travail", in *Ergonomie*, P. Falzon (Ed.), Presses Universitaires de France, Paris, France (2004).

5. J. F. Kelley, ‘An iterative design methodology for user-friendly natural language office information applications’, *ACM Transactions on Office Information Systems*, **vol. 2**, no. 1, pp. 26–41 (1984).
6. J. Laarni, P. Savioja, L. Norros, M. Liinasuo, H. Karvonen, and L. Salo, “Conducting Multistage HFE Validations – Constructing Systems Usability Case”, *Proceedings of the ISOFIC/ISSNP 2014*, Jeju, Korea (2014).
7. I. A. Wulff, R. H. Westgaard, and B. Rasmussen, “Ergonomic criteria in large-scale engineering design–I Management by documentation only? Formal organization vs. designers’ perceptions”, *Applied Ergonomics*, **vol. 30**, no. 3, pp. 191 – 205 (1999).
8. I. A. Wulff, R. H. Westgaard, and B. Rasmussen, “Ergonomic criteria in large-scale engineering design–II Evaluating and applying requirements in the real world of design”, *Applied Ergonomics*, **vol. 30**, no. 3, pp. 207 – 221 (1999).
9. J. M. O’Hara, J. C. Higgins, S. A. Fleger, and P. A. Pieringer, *Human Factors Engineering Program Review Model (NUREG-0711, Revision 3)*, U.S. Nuclear Regulatory Commission, Washington DC, U.S.A (2012).