APPLICATION OF HFE TO THE DESIGN AND V&V OF A COMPUTERIZED PROCEDURE SYSTEM: BENEFITS AND CHALLENGES

Sara Fernandez & Cristina Corrales & Fernando Ortega
Tecnatom
1, Montes de Oca, 28703 San Sebastián de los Reyes (Spain)
sfernandez_fernandez@tecnatom.es; fortega@tecnatom.es

ABSTRACT

The application of Human Factors Engineering (HFE) practices to the Human Machine Interface design and subsequent Verification and Validation (V&V) is a widely applied practice when talking about the design of complete control rooms or important control room modernizations, but not so often applied to the design of computerized operator support systems. In order to overcome the challenges faced on designing a Computerized Operation Support System (COSS) that meets the process efficiency requirements and integrates seemingly with hybrid plant operation concept, the involvement of a HFE team early in the COSS design and implementation process along with operation, Instrumentation and Control (I&C) and cybersecurity experts will guarantee the project success.

This paper documents the HFE process applied during the design and evaluation of a Computerized Procedure System (CPS) and how final product was shaped to ensure that the transition from paper to computerized procedures will help in meeting Delivering the Nuclear Promise (DNP) goals, improving plant efficiency. The HFE program included the following activities:

1. A review of existing operating experience

2. An analysis of functions and tasks associated to the use and maintenance of CPS

3. A design verification of the system to meet guidelines prescribed in the NUREG-0700 (Rev.2), requirements of the ISG-05 and cybersecurity criteria (NEI 08-09, IEC-62646, EPRI 1015313, these among others).

4. An integrated system validation in a full scope simulator

The application of HFE practices in the design and implementation of COSS helps not only to ensure that efficiency and safety improvement requirements are met, but also to evaluate the potential return of the investment, that such tools should bring.

Key Words: HFE, Verification and Validation (V&V), Efficiency, COSS, Computerized Procedures.

1 INTRODUCTION

The biggest challenge for the aging nuclear power plants fleet is to remain competitive in an uncertain and hostile economic environment. Industry initiatives as DNP identify ways to do so. One of the building blocks of the DNP strategic plan calls for "redesign of the nuclear power plant process to improve efficiency while advancing the fundamentals of safe, reliable operation". While analysing cost drivers and opportunities to improve efficiency in plants operation, the introduction of Computerized Operation Support Systems (COSS), such as Computerized Procedure Systems (CPS) seems promising, if the system is designed to reduce the operation costs by increasing the process efficiency and the safety of the plant

while executing operating sequences. To do so the design and implementation of CPS in the nuclear power plant should suite the operation organization needs, from operating crew to administrative personnel, whose efficiency is planned to be increased.

With the increased efficiency and safety goals in mind, the design team delineated an ad-hoc HFE program to help meet the requirements. The program was also intended to provide input on the return on the investment. The HFE program included the following activities:

1. A review of existing operating experience related to the use of procedures in nuclear power plants, screening events to identify the weaknesses of paper procedures and defining requirements for CPS based on them in order to prevent recurrence of such events.

2. An analysis of functions and tasks associated to the use and maintenance of CPS. This analysis allowed the design team to identify requirements to be imposed to the system.

3. A design verification of the system to meet guidelines prescribed in the NUREG-0700 (Rev. 2). In addition to this design verification based on human factors criteria, a verification of the requirements of the ISG-05 was also conducted along with other tests to assure reliability and performance of Tecnatom CPS system. Cybersecurity criteria (NEI 08-09) as well as other standards (IEC-62646, EPRI 1015313, OWASP guides…) have been considered in the design and development process of Tecnatom CPS system.

4. An integrated system validation in a full scope simulator to determine that CPS design enables plant personnel to successfully perform their tasks and other operational goals, assuring plant safety, as well as comparing the use of paper based procedures and computer based procedures.

The Figure 1 graphically resumes the Nureg 0711 program elements and which of those were used for the CPS design and V&V project.

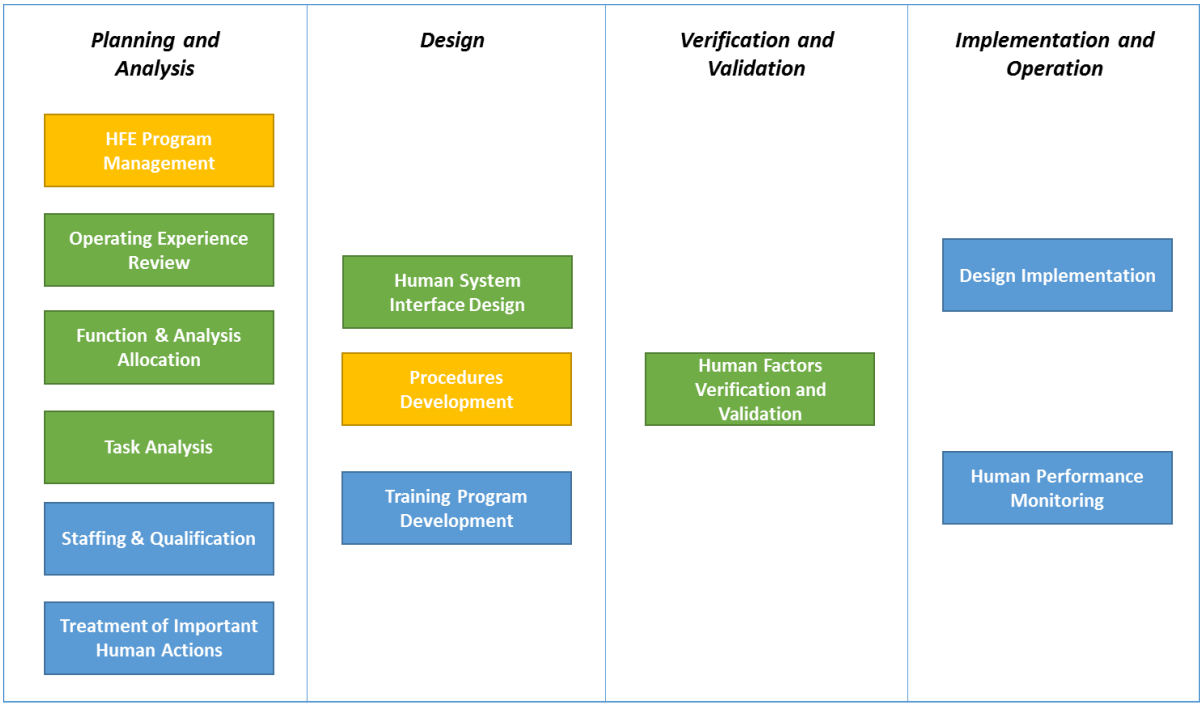

Figure 1. Nureg 0711 program elements and those applied to CPS design and V&V project.

*Colour Code: green-element fully applied in the analysis, yellow-partially applied and blue-only applied in a timely manner.

A review of the plant operation experience (searching for current difficulties and potential improvements); a functions and task analysis to identify all the workers affected by the change and how it will impact them maximizing the benefit; the verification of the system design in accordance to NUREG-0700 guidelines and other standards; and a validation of the CPS in the full scope simulator to evaluate the performance in an very close to real environment; all these key HFE activities were essential to ensure the CPS meets the efficiency and safety improvement requirements, build the arguments that will help the plant to make an informed decision about the project and prepare future implementations of the system with minimum cost and risk.

2 HFE PROGRAM TO COSS DESIGN

The CPS project was framed in a similar way to human factors engineering program, scaling the resources, focusing the HFE activities on those providing value to the product.

The team in charge of the project had a project manager with experience in digital I&C projects and included I&C and IT engineers, experts in plant operation, human factors engineers, procedures writers and software developers. The experts in plant operation, human factors engineers and procedures writers compiled a set of user oriented requirements, while the I&C and IT expert delineated the architecture and determined the plant I&C potential and constrains. All those requirements were documented in the system specification. The adoption of agile methodologies for the software development allowed the team to test the system in very early stages and to ensure that the product never lost the desired user focus.

The team also carried out some sessions or workshops with plant operators in different stages of the project. The results of those sessions informed significantly the design.

The human factors program management activities were integrated with the project management ones, applying a systematic process to document and resolve any issues that arisen as a result of HF activities or software development tests.

The major HF activities mentioned above are explained in depth in the following sections.

2.1 Revision of existing operating experience

An analysis of the existing operating experience related to the use of procedures in nuclear power plants was performed. The goal of this analysis was to identify the common underlying problems that the operators faced while using paper procedures. Then, those issues were used to formulate some of the requirements for CPS in order to prevent recurrence of such events.

The source of the Operating Experience Report (OER) was found in the INPO databases and the events considered were extracted from operating experience dating from 1994 to 2015. The analysis phase of this operating experience required a discrimination between those events related with the quality[1] of the procedures (how they were written and out of the scope of the project) and the actual use/execution of the procedures (which constituted the focus of our study).

After this analysis nineteen events were classified as significant for the design of a CPS and they were classified in the following categories of procedures' related issues:

- Adherence
- Precaution and caution messages
- Procedure revision

[1] Quality refers in this case to the intrinsic characteristics of the procedure content, that must be "complete, accurate, consistent, and easy to understand and follow" (Nureg –0711 Rev.3)

- Placekeeping

2.2 Analysis of functions and tasks

The purpose of this activity was to systematically identify and characterize the generic[2] functions performed by the operators and other plant personnel while using the procedures. The following Generic Functions (GF) were identified:

GF-1. Execution of operation sequences in accordance with the procedures.

GF-2. Surveillance of plant and system conditions.

GF-3. Supervision of functions GF-1 and GF-2.

GF-4. Identification, implementation and approval of procedures modifications and/or needs for new procedures.

GF-5. Distribution and archival of procedures (controlled copies and quality records of completed executions).

The plant personnel (control room operators, auxiliar operators, plant engineering, administrative personnel …) involved in each of these functions were determined. The functions were broken on more particular ones per role. The generic tasks that allowed the personnel to accomplish their allocated functions were defined and analysed to formulate the CPS requirements. The CPS design process thus ensured the translation of the function and task requirements into the system characteristics and functions. The following diagram details the methodology that was implemented to obtain the Specific Requirements included in the Design Specification of the CPS

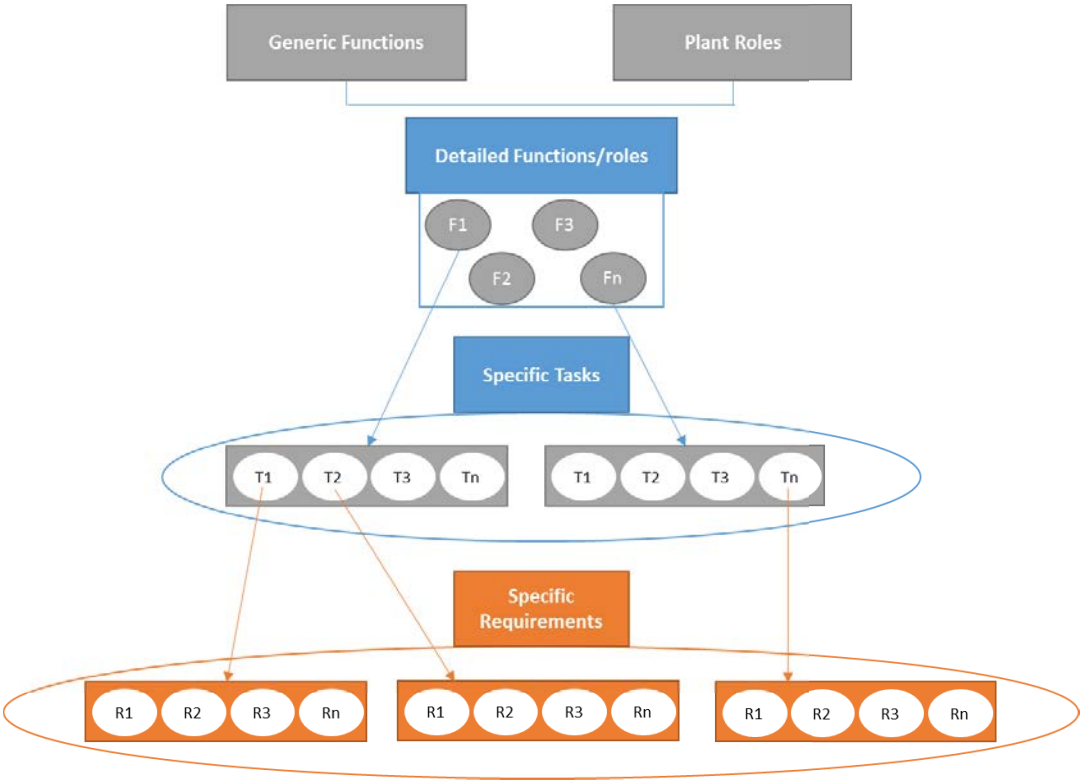

Figure 2. Specific Requirements generation process

[2] The term generic is used here to denote functions and tasks that apply to any procedure, no matter its content.

The table I identifies some of the tasks analysed and how those were translated into system requirements.

Table I. Example of Designs Requirements driven from the Task Analysis

Task	Requirements
Accessing/Selecting applicable procedure	The system shall allow the user to access the procedures collection and select the applicable procedure.
Verification that the procedure used is the correct one	Title and identifying information such as number, revision and date shall be always visible.
Evaluation of the equipment and component status	The system shall provide a minimum set of information that will allow the user to know the status of the plant equipment before signing a step.
Steps signing	The system shall enable user to sign steps in real time and that signature shall be permanent and not revocable.
Procedures modification, new revisions	The system shall allow procedure modifications and enhance the traceability of those changes.
Independent Verification. Procedure restrictions	The system shall permit interactions between different users, setting restrictions to avoid steps signing without special permissions when needed.

The result of this analysis helps to build the foundations for the Design Specification of the CPS.

2.3 Design verification

A design verification of the system was performed to ensure it meets the guidelines prescribed in the NUREG-0700 (Rev. 2). The methodology applied to implement the Design Verification is explained in the steps below:

- STEP 1: Revision of the applicable Nureg Guidelines and establishment of the verification process, that has been documented as a verification procedure.
- STEP 2: Identify the NUREG-0700 sections that are applicable to CPS. This is in fact an iterative process that allows the practitioner, no matter his expertise level to start by identifying sections and to refine the selection at guideline level as the process goes on. The HF V&V team has tools to record and select the guidelines and that provide aids for their interpretation. Specifically, for this system design verification, the first iteration deemed the following NUREG-0700 sections as applicable:
    - Section 1: Information Visualization
    - Section 2: User-System management and interaction
    - Section 7: Software Control System
    - Section 8: Computerized Procedures Systems

The iterative process continued by determining for each applicable guideline, whether it was fulfilled or not and in the latest was the case, a discrepancy was generated.

In the sections cited above, more than eight hundred guidelines were considered, of them, around five hundred were selected as applicable to the CPS; 75% of them were properly fulfilled. The rest were pending waiting to specific test to be performed or not fulfilled. In the case of the not fulfilled guidelines, corrections were made in order to meet those requirements except from a few of them where the design team provided a justification not to take action.

The Nureg 711 Rev. 3 requires compliance between the CPS and the requirements of the ISG-05. This verification was also conducted to assure reliability and performance of Tecnatom CPS system.

In addition, cybersecurity criteria (NEI 08-09) as well as other standards (IEC-62646, EPRI 1015313, OWASP guides…) have been taken into account in the design and development process of Tecnatom CPS system.

2.4 An Integrated System Validation (ISV) in a full scope simulator

The objective of the CPS HFE Integrated System Validation (ISV) is to demonstrate that the design system, when integrated in a control room, allows operators to perform the tasks that have been entrusted to him in an optimal way. Therefore, the CPS evaluation aims to validate that the interface allows operators to correctly follow the operating procedures, minimizing the possibility of human error, improving the human performance and thus contributing to the safe operation of the plant.

As previously mentioned, it is also a goal of the integrated system validation to gather data that allowed the team to evaluate the human performance improvements associated to the use of computer based procedures. In order to do this, the validation scenarios will be executed using both, the paper procedures and the CPS.

The validation team is also interested on evaluating how much the age of the operators, if at all, influenced the assimilation of the system. To do so, different crews will participate (profiles, age, experience, etc) in the tests and the validation questionnaires are focused on characterizing the impact of the age in the usage of the CPS.

The ISV Observers are experts trained to collect the appropriate information in an orderly manner for to conduct the analysis required to evaluate the goals mentioned above. This table provides an example of the data that will be collected during the ISV.

Table II. Example of data collected during the execution of the CPS ISV

Number	Features
1	Annotations of compliance with expected actions, actions taken (time), panels and displays used and information exchanged in relation to the issues to be evaluated and following the measures defined
2	Simulator Parameter Summaries
3	The action measures taken into account, are the following (depending on each observed situation):
3.a	**Time**: Annotation of the time allows to measure the time that the operator needed to perform his tasks (examples: reaction time, time to complete actions, duration of the task, time of search of the devices, etc.)
3.b	**Accuracy**: It is a measure of the correctness of the actions of the operator according to the expected actions (examples: errors using the system, following procedures with the system, managing system alarms or performing control actions, etc.)

Table II. Example of data collected during the execution of the CPS ISV

Number	Features
3.c	**Precision**: It is a measure of how precise the same actions are even though they are far from the exact or expected result.
3.d	**Frequency of actions**: It is a measure of the number of times you have had to use or do something to complete a task (examples: information search, execution of a step, checking the status of a team, communication with the rest of the members of the shift, etc.)
3.e	**Resources employed**. (Examples: Devices used, etc.)
3.f	**Actions carried out**. Control and / or verification actions
3.g	**Communications**: It is the identification of the information exchanged by the operation crew with special emphasis on the CPS (examples: completed actions, actions to be performed, observations made, data obtained, situation assessment, etc.)
3.h	**Dynamic anthropometry and operator movement**: It is a measure of the operator's physical interactions with the new system and its position

3 RESULTS FROM THE ANALYSIS

Relevant results are driven from the HFE Program applied. Analysis. However, is even more important to understand the type of requirements that were included in the CPS Design Specification due to this analysis.

The Operating Experience Review results, provided key design features based on previously reported issues by the plants when using paper procedures. Those key design features tried to corrector avoid occurrence of human errors related to procedure adherence, placekeeping and disregarding of precaution messages.

Continuing with the application of the HF program, the Functions and Tasks analyses provided a great amount of new User Interface Requirements, identified all the system stakeholders and integrated early at the conceptual design phase, the Software and Cibersecurity Requirements.

The Verification of the EPRI, IEC, NRC, NEI and OWASP Guidelines compliance along with the specific HFE Guidelines (NUREG-0700) ensure that not only the HFE design of the CPS is appropriate but also that this system is operable and usable under the operating conditions in which it will be used. Concretely, these guidelines were taken into consideration before the Design Specification development and afterwards, there was an analysis to check that the obtained Design Specification complied with them. Moreover, for this final checkout, the ISG-05 was also considered.

Finally, the aim of the Integrated System Validation is to, once the CPS was developed and tested, ensure that the design of the system interface and its implementation in a control room allow operators to perform their tasks regarding the execution and maintenance of operating procedures.

4 CONCLUSIONS

Counting on a multidisciplinary team since the beginning of the project enabled an CPS integrated design including different points of view which reduced subsequent rework along the CPS design and development process. Integrating HFE activities since the beginning helped to identify conflicting requirements and to make quick decisions to solve that misalignments. Moreover, this CPS design process provided an integrated and orderly CPS Design Specification.

Human Factor experts provided a user-oriented vision, specifically for main control room operators, ensuring at the same time the compliance along with the specific HFE Guidelines (NUREG-0700).

Although, a priori from the project planning point of view, including HFE activities may increase the number of activities and stress the project schedule, final project review confirmed that both, the CPS Design Specification and the subsequent CPS development process, were optimized as less or even null design modifications were implemented afterwards.

To conclude, the application of HFE practices in the design and implementation of COSS helps not only to ensure that efficiency and safety improvement requirements are met, but also to evaluate the potential return of the investment while transitioning from paper to computerized tools.

5 ACKNOWLEDGMENTS

The preparation of this paper has involved the invaluable contributions of the R&D, specially, my colleagues Cristina Corrales and Idoia Aguirregabiria; and Simulation and HFE personnel.

6 REFERENCES

1. U.S. Nuclear Regulatory Commission , “Human-System Interface Design Review Guidelines”,. NUREG-0700, 2004.
2. U.S. Nuclear Regulatory Commission, “Human Factors Engineering Program Review Model”, NUREG-0711, 2004.
3. U.S. Nuclear Regulatory Commission, “Highly-Integrated Control Rooms-Human Factors Issues”, DI&C-ISG-05, 2008.
4. Nuclear Energy Institute , “Cyber Security Plan for Nuclear Reactors”, NEI 08-09, 2010.
5. Electric Power Research Institute, “Computerized Procedures. Design and Implementation Guidance for Procedures, Associated Automation and Soft Controls”, EPRI 1015313, 2007.
6. International Electrotechnical Commission, “Nuclear power plants. Control rooms. Computer-based procedures”, IEC 62646, 2016.