VERIFICATION AND VALIDATION OF NEW OPERATION SUPPORTS SYSTEMS FOR BEZNAU NPP

A. JIMÉNEZ - J. A. BURILLO

FOREWORD

This article describes the activities associated with the Verification and Validation works performed by Tecnatom on a computerised Advanced Alarm System (AAS) and a Computer Based Procedure System (CBP), for the licensing of these systems to be used in the control rooms of Beznau NPP (property of NOK).

In this process Tecnatom acted as an independent company in the evaluation of the new systems, supporting Beznau NPP to obtain the approval from the HSK (Swiss Federal Nuclear Safety Inspectorate) for the implementation of these systems into the training and operating concepts of the plant.

VERIFICATION AND VALIDATION PROCESS

The verification activities were focused on an independent evaluation of the following subjects:

- Interconnection between the plant information system and the new systems
- Detailed check of the system databases and the correspondent plant data
- Human System Interface verification

The verification activities were documented using special formats. The verification process consisted in the detailed evaluation of each element included in the databases that are needed to define the Emergency Operating Procedures (EOP's) and the alarm messages.

The verification process reached the following objectives:

- Consistency of the data structures
- Completeness
- Unambiguity
- Correctness of the data values against the emergency operating procedures and the alarm logic's of the plant (logic/sequence/ priority).
- Readability
- Protection against unauthorised changes

The validation activities were performed to demonstrate that the systems are operational and that they comply with functional and HFE requirements included in the methodology.

These activities consisted in the execution and analysis of several test cases or scenarios in a simulator with actual Beznau crews. The evaluation was achieved by assessing the use of the CBP system in relation to the operator interactions with the system, taking into account an operator/human performance model of activities when responding to abnormal or emergency conditions. The major activities represented in this model are:

- Monitoring/detection
- Situation assessment
- Response planning
- Response implementation
- Feedback

Special emphasis was placed on the following topics when evaluating the operator's actions:

- Situation awareness
- Workload
- Communications

EVOLUTION OF THE OPERATIONAL CONCEPT IN BEZNAU NPP CONTROL ROOM

This section discusses the control room operating philosophy in the current situation and how the operational concept evolve after the V&V

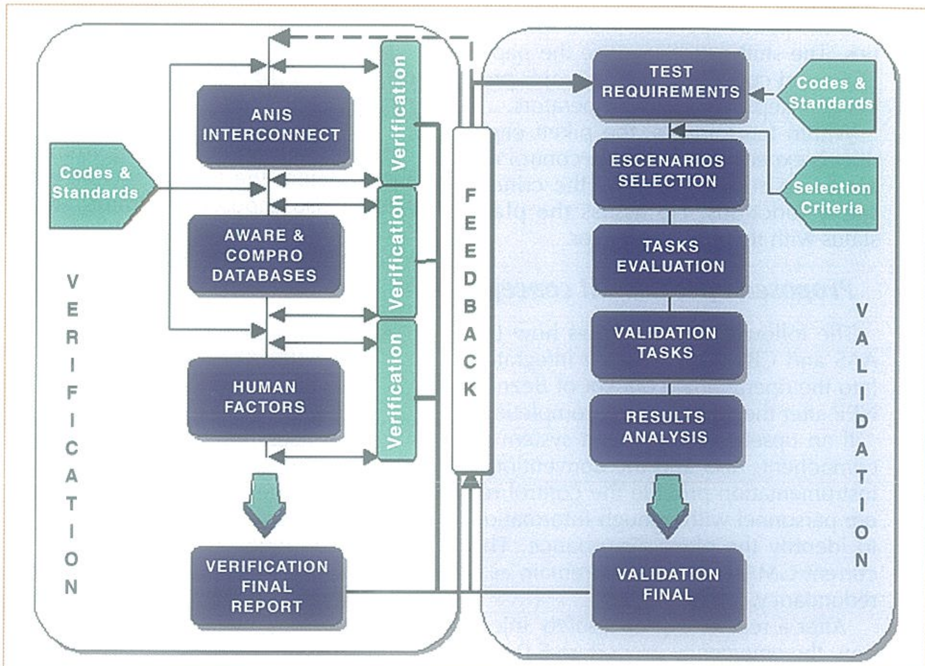

Figure 1.

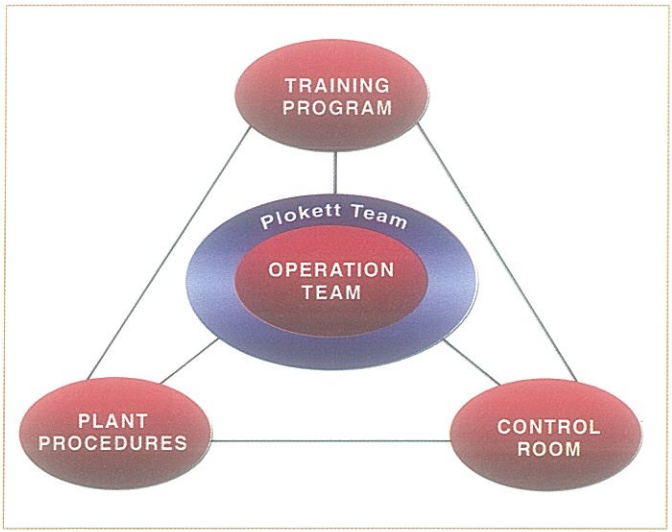

Figure 2.

process implementation with the introduction of AAS and CBP.

Current operational concept

The current operational concept can be explained as the "operating triangle" shown in the figure 2.

If an upset is caused by a system or component, the current GMA alarm system and the conventional instrumentation provide the panel operators with enough information to identify the plant disturbance.

After a reactor trip or a safety injection, the emergency procedure E-0 were executed, using the above mentioned information and the paper EOPs. During this time, the shift supervisor and the panel operators have split duties. The shift supervisor use the paper EOPs and communicate the major procedural steps to the panel operators.

Within ten minutes, the pikett engineer is expected to enter the control room to assist in monitoring the critical safety functions. He assess the plant status with the shift supervisor.

Proposed operational concept

The following figure shows how the AAS and CBP systems were integrated into the operational concept of Beznau NPP after the V&V process completion.

If an upset is caused by a system or component, AAS and the conventional instrumentation provide the control room personnel with enough information to identify the plant disturbance. The current GMA alarm system remain as a redundancy.

After a reactor trip or a safety injection, the emergency procedure E-0 were executed by using both AAS and CBP. During this time, the shift supervisor use CBP to monitor proper execution of procedures and communicate the major procedural steps to the panel operators.

Once the pikett engineer enters the control room, he use the conventional instrumentation to support the crew, monitoring the critical parameters.

These changes in the operational concept were congruent with the training that is being carried out.

FUNCTIONAL CRITERIA FOR CBP V&V PROCEDURES DEFINITION

There are some specific requirements that have to be considered when selecting the tests to be performed in the CBP V&V process.

The Westinghouse Owner Group establishes in their Emergency Response Guidelines the action steps for the development of plant specific emergency operating procedures.

The CBP V&V process include a set of verification formats and validation scenarios so that all critical safety functions and the mayor paths of E-0, E-1, E-2, and E-3 series were checked.

These are two different and complementary approaches to face the plant operation under emergency conditions.

HUMAN FACTORS CRITERIA FOR AAS AND CBP SCENARIOS DEFINITION

Besides the functional requirements above stated, the human factors engineering also imposes constraints on the AAS and CBP validation tests: a set of realistic and feasible scenarios should be selected.

- Scenarios should be realistic in the sense that they should represent what could actually happen and should require subjects to produce responses typical of what would actually be required in such situations. In general, if subjects are asked to deal with situations they do not believe could happen, or to produce responses that they would be unwilling to make in reality, there is significant risk that the scenario will not be useful for the evaluation. Further, even if subjects do comply with unrealistic requirements, the results will not be representative of eventual system performance in an operational environment. The selected scenarios should include environmental conditions such as noise and distractions that may affect human performance in an actual NPP.
- Scenarios should be feasible in the sense that they should not impose requirements that exceed the capabilities of the simulator facility being employed.

AAS AND CBP VALIDATION

The purpose of the AAS and CBP validation were to demonstrate that the systems perform the functions expected, and that operators and systems interact properly to perform the required functions and to support safe operation of the plant.

The validation tests cover the system functions in a fully representative manner. The validation tests were performed through dynamic task performance evaluation using evaluations tools which are appropriate to the accomplishment of this objective under a range of operational conditions, including normal and upset conditions.

PREPARATION FOR THE EVALUATION

This phase includes:

- Selection of scenarios
- Task evaluation
- Data collection methods

Selection of scenarios

The scenario selection began with the determination of the operational events that were used to develop the validation tests. Special emphasis were placed on abnormal and emergency conditions to better test AAS and CBP. The operational events should address the main plant systems and safety functions (the actions to maintain plant safety). Each safety function is associated with plant processes (plant system configurations or success paths) which are responsible for or capable of carrying out the function.

The scenarios contain critical tasks, as identified in the task evaluation. They describe the initial conditions, the proper sequence of plant responses and applicable symptoms.

Task evaluation

The task evaluation must adequately define the personnel task requirements

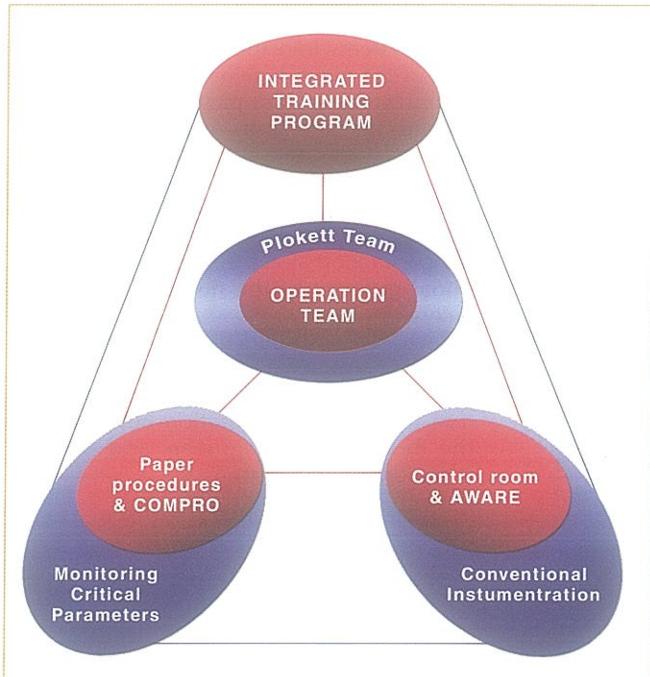

Figure 3.

that were used during the validation phase to evaluate the adequacy of the systems HSI, to guide the application of HFE guidelines and support the development of safety performance criteria for the system validation.

The information that constitutes the basis for the task evaluation includes documentation of procedures, training, existing task allocations, system design objectives, and often, interviews with operators.

Data collection

The data collection methods that were employed during the test sessions include both online and offline methods. While the online methods assess the variables of interest during the course of a trial, the offline methods involve assessment after the trial is completed. In general, online methods tend to provide finer grained data and, hence, are more useful. However, there is usually a limit to how much online assessment can be performed before measurement becomes obtrusive in the sense of distracting operators from their tasks. That is the reason to employ a mixture of online and offline methods. The nature of this mixture depend on the evaluation objectives.

Online methods that were used during the tests are, for instance, the recording of the event logs from the simulator, the recording of the interactions of the operators with the systems, and the evaluations of the observers. The sequence of crew's thoughts and actions, and the key steps in the reasoning process should be observed: the diagnoses, the various identified phases, and the resulting actions.

- **Test sessions**

A preliminary talk to explain the experiments to the crew take place before the test sessions. Tests were executed on simulators. During these tests, each operator play his usual part while the evaluation team observe the exercise and document the crew/systems performance.

- **Debriefing sessions**

A debrief session were carried out after each test session, containing interviews and questionnaires, that allow to go through the problems experienced by the crew and to supplement the real time observations.

In these sessions, the data collection were performed by using offline methods. While the HFE specialist should attempt to collect objective data whenever possible, in some aspects of the evaluation the objective data are not sufficient to enable a complete analysis of a system or test item.

The offline methods that were used in the debrief sessions are questionnaires and interviews:

- Structured questionnaires (debriefing questionnaires) administered to the test participants. The test subject questionnaires were examined and tabulated to determine the range of test subject opinions regarding the experiment.

- Debriefing interviews with the participants to obtain comments in a less structured, more interactive manner. An interview at the end of the test to note downs the crew's comments, to go through the problems experienced and to supplement the real time observations.

- **Data analysis and results evaluation**

The data analysis and results evaluation process consist of four basic phases or steps: transformation, organisation, identification and interpretation.

The first step involves transformation of the raw data into dependent measures of interest. The second step is the organisation of these measures into a form suitable for further analysis. (These steps of transformation and organisation can be expedited by having all raw data in computer-readable files). The third step involves identification of significant main effects and interactions, and if the systems do or not meet the objective criteria defined during the evaluation process. The final step is interpretation of results. This step must be performed by someone with knowledge of the context and situations to which the evaluation is relevant.

The test results were evaluated against the acceptance criteria defined in the validation procedures.

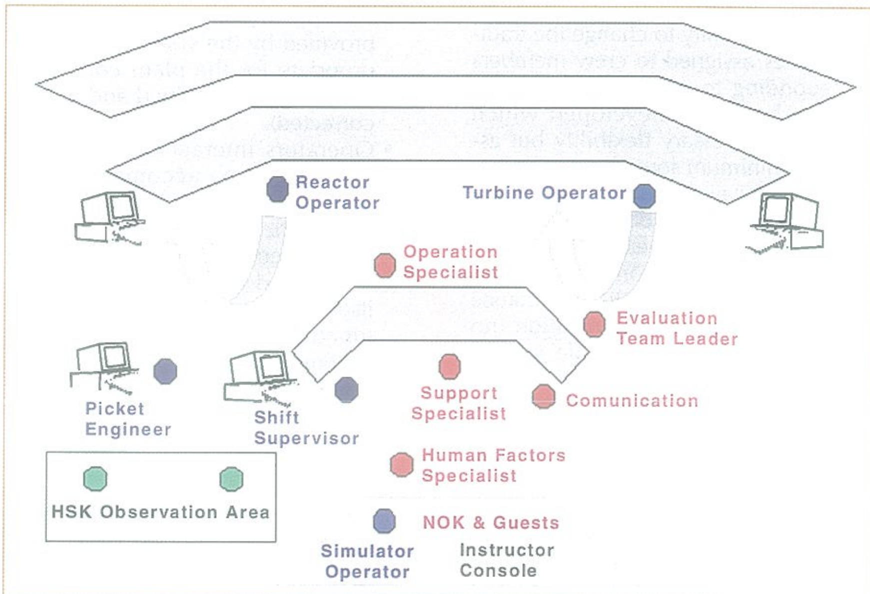

Figure 4.

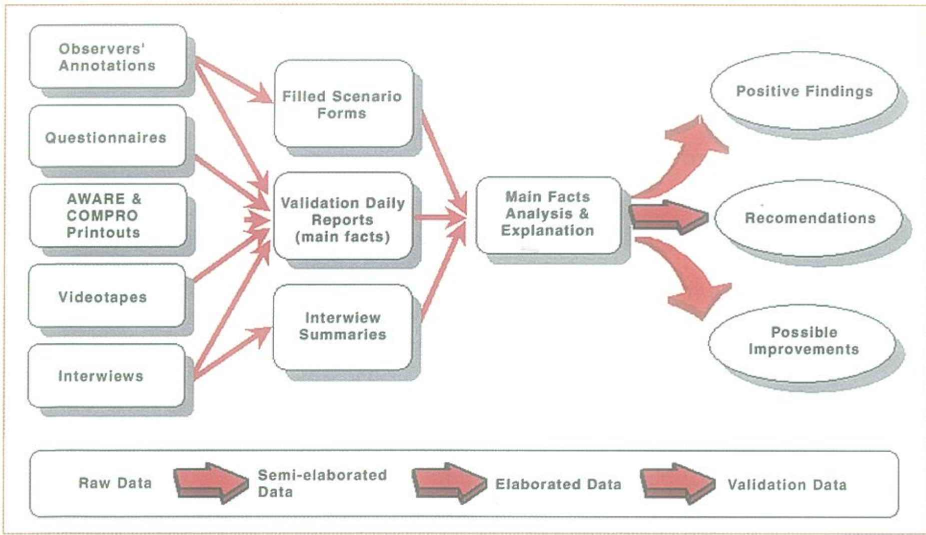

Figure 5.

OPERATION PHILOSOPHY AND USER CONCEPT OF ADVANCED HSI SYSTEMS

The introduction of computer-based HSI systems into the control room changes the amount of plant state information available to operators. It also changes the accessibility of the information to different members of the crew. In particular, CBP provides the shift supervisor with the plant state information required to work through the procedural steps. It is no longer necessary for the shift supervisor to ask the board operators to read plant parameter indications off the control board and talk them loud in order for the shift supervisor to determine whether a procedural step is satisfied or not. The CBP provides that information directly.

This change in technology introduces the opportunity to change the traditional roles assigned to crew members in responding to emergencies. A user concept has to be developed which allows the necessary flexibility but assure the minimum forced communication for safety awareness.

A study, based on observations and questionnaires in the early stage of simulator training sessions, has shown large dependency in crew performance on effective crew communication (no specific communication rule was in force at that time).

The new systems allow different levels of use by the operators (large variation from forced rules for communication as with paper procedures to situations with no specific rule for communication as in the NRC study). This has large impact on crew performance: CBP could shift the content of communication to a higher level that more directly addresses the status of the plant relative to the goals of the procedures and achievement and maintenance of safety functions. It is also possible that by removing the forcing function to communicate, CBP results in reduced communication and, as a consequence, the situation awareness among crew members might also be reduced.

FINAL CONCLUSIONS

The results of the validation process show that the objectives of the verification and validation process have been met:

- The systems performed their expected functions, displaying adequately and correctly the plant conditions. (The very specific situations in which the information provided by the systems is not appropriate for the plant conditions are precisely identified and will be corrected).
- Operators interact properly with the systems to accomplish their tasks and to support a safe plant operation.
- The systems do not perform any unintended function that either by itself or in combination with other functions can degrade the entire systems. All the scenarios ended in a safe plant condition.
- Shift supervisors are able to execute the emergency operating procedures using a computerise system.

Therefore, once the recommendations identified during the verification and validation process are implemented, Tecnatom considers that the systems will be appropriate for their use at Beznau NPP control room. The use of these systems into the operating concept of the plant, together with the supervising role of the pickett engineer, has the capability to increase the safety and reliability on managing normal and accident situations in Beznau NPP.

This V&V process is an important step towards the effective introduction of new support systems into the operational concept of the nuclear power plants.

Tecnatom is proud of the practical experience obtained during the execution of this project and wants to mention the close collaboration between the Beznau NPP engineers and the Tecnatom project team.

Alfonso JIMENEZ FERNANDEZ-SESMA, has a master degree in Electrical Engineering from the ICAI (Madrid). He started working at Tecnatom in 1981, and is currently manager of the Operation Engineering Division. He has been certified as an Operation Supervisor for PWR's Plants and has participated and co-ordinated numerous projects and studies for domestic and overseas NPP's. He worked for the Institute of Nuclear Power Operations INPO (USA), as evaluation engineer in the Operation and Technical Support areas.

Juan A. BURILLO CASTAÑO has a master degree in Electrical & Electronics Engineering from the ETSII of Madrid. He started his professional activity as a field engineer working for Schlumberger and Welex-Halliburton in the oilfields of the North Sea and Libya.
He works for Tecnatom since 1986, developing himself as simulator instructor on the Training Department being responsible for Zorita NPP formal crew's qualification. Since 1997 has worked on the Operation Engineering Division, for the past three years he's been the project manager of the V&V Beznau Project.