Advanced CANDU Reactor® Computer-based Displays Design Process

R. Bodner[1] and R. Chatterton[1]
[1] Atomic Energy of Canada Limited (AECL), Mississauga, Ontario, Canada

Abstract

The ACR-1000® project integrates Human Factors Engineering principles and processes throughout all phases of design. The human factors engineering effort follows a structured approach to the application of human factors to the design process. Included in this approach is a tight integration with subject matter experts from the operations and maintenance team. This paper describes the structured approach followed for the control centre design, focusing in particular on soft displays and the points of integration with subject matter experts.

1. Introduction

The Advanced CANDU Reactor[1] (ACR[1]) design process integrates Human Factors Engineering (HFE) principles and processes throughout the engineering-system design phase. The primary goal of the application of these HFE principles and process within the ACR-1000[1] design process is to improve the operability and maintainability of plant systems for increased safety of plant personnel, the public, and overall plant production. This is accomplished by identifying human error inducing events and designing system interfaces to prevent such errors (prevention), reducing the likelihood of human error via human factors analysis techniques (tolerance), and providing facilities that assist in the recovery and mitigation of the consequences of such events (mitigation). The result, partly because of the application of HFE during the design phase is a plant design that supports safe, productive, efficient operating characteristics throughout all stages of plant lifecycle.

2. Background

The control centre for CANDU[2] plants has evolved since the original CANDU[2] 6 plants designed in the 1980s. These earlier plants had computer control and computer-generated "soft displays" for system monitoring and limited control (e.g., changing setpoints).

The Darlington CANDU[2] plant made extensive use of computer control and display. The control computer displays use an early form of touch sensitivity (i.e., light pen activation) as the primary means of interaction. The application of computer control has also been fully extended to the two independent Shutdown Systems, and at Darlington, they are fully computerized from reactor trip to display and alarm functions.

With improvements in computer technology and particularly in movement to digital communications and distributed systems, there is significant capability to further improve the human-system interface in the main control room. Display functions could be moved into dedicated systems, separate from the systems that provide control functions, thus allowing for added

[1] Advanced CANDU Reactor, ACR, and ACR-1000 are registered trade-marks of Atomic Energy of Canada Limited (AECL).
[2] CANDU is a registered trademark of Atomic Energy of Canada Limited (AECL).

functionality without impacting safety. Systems could be partitioned for performance and reliability.

The design of computer control and display evolved further with the CANDU[2] 9 design. Based on operations feedback a number of additions were included in the main control room:

a) Addition of a highly integrated Main Operator Console (MOC) and Shift Interrogation Console (SIC). These consoles provide work stations for monitoring safety and production functions as well as work stations for administrative functions.

b) Addition of Large Screen Displays (LSDs). Large Screen displays provide plant overview information that can be situation specific and can be easily shared amongst operating team members in the main control room (MCR) for group problem solving. These displays are ideally suited to maintain high level overall plant situational awareness, while they may be augmented with detailed displays available at the Main Operator Console (MOC).

c) Addition of computer assisted safety system testing from the Main Operator Console location. In addition to reducing operator workload and distraction in the MCR, automated testing also significantly reduces panel space requirements for the testing controls.

d) Development of the CANDU[2] Annunciation Message List System (CAMLS) to improve annunciation. This system processes the annunciation message stream to help ensure only pertinent conditions are enunciated. The processing algorithms use key information such as plant state, significance, redundancy, cause-consequence, chattering, etc, and separate 'alarm' messages from expected 'status' messages. The application of CAMLS to the ACR-1000[1] project is described in Leger *et al.* [1].

2.1 ACR-1000 Control Centre Design Description

The vision for the ACR-1000[1] main control room is a continuation of the CANDU[2] 9 development, focusing on feedback items from the CANDU[2] 9 control centre mock-up validation. One of the main recommendations was to move to a "control from the console" concept using more "soft controls" (i.e., via the Plant Display System Human-System Interface (HSI)). This improves the ability to perform some of the more complex tasks as it brings the required controls and displays (and procedures) to one location to complete the given task.

Figure 2-1 shows a basic conceptual layout for the MCR of the ACR-1000[1]. Although the figure shows some details, the exact size, location and appearance of various components will be finalized to ensure proper sight-lines, good ergonomics and specifics of the chosen component technologies.

The basic layout shows a single unit configuration comprising of large display panels, main operator console (MOC) and shift interrogation console (SIC). Only one unit, of a two unit MCR, is shown in the figure. The second unit would be a mirror configuration of the one shown in the figure. The fuel handling configuration is also not shown in the figure. The fuel handling configuration comprises of large display panels, an MOC and a SIC all specific to fuel handling operations for the unit.

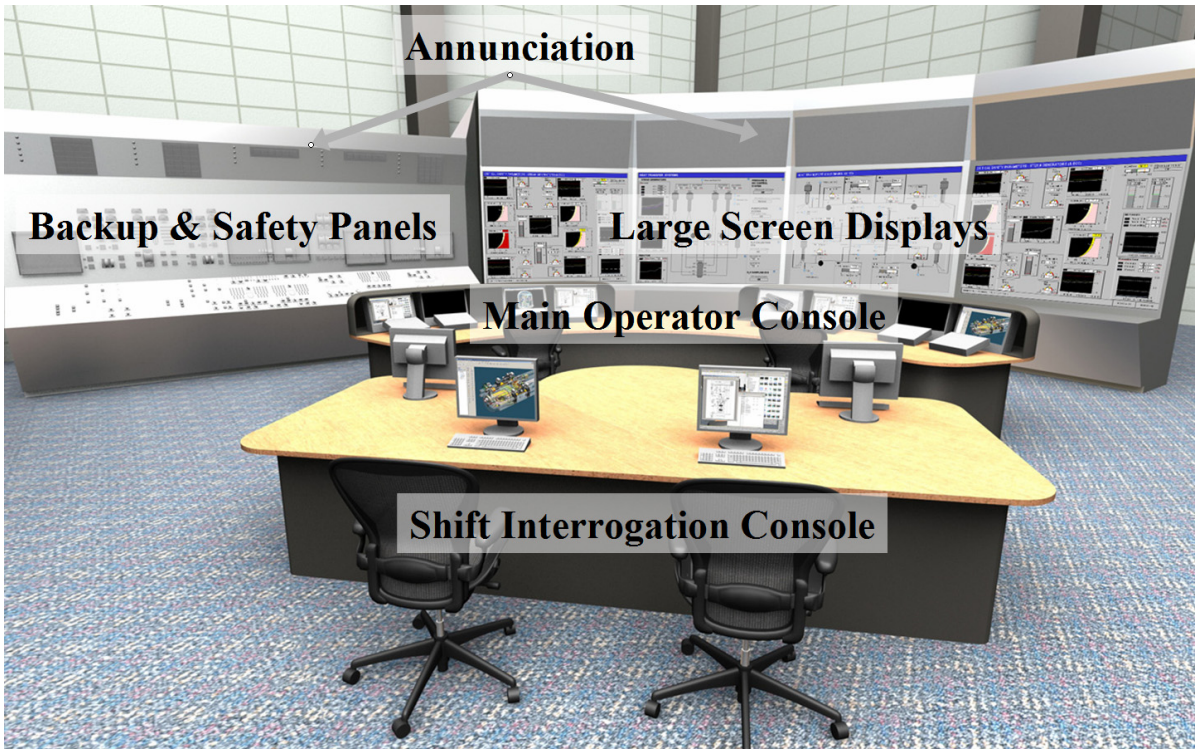

Figure 2-1 ACR-1000 Main Control Room Conceptual Layout.

The key features of the unit operator configuration are as follows:

a) The main operator location is sitting at the MOC. This console is designed for one primary operator and an assisting operator during periods of high work load. Here the operator has access to all soft controls and any important or frequently used hardwired controls. The multiple console workstations provide access to annunciation, process, and safety system information in the various formats tailored to operator tasks. These displays are augmented by the relatively stable and unchanging Large Screen Displays (LSDs) that provide a plant wide overview. This allows the MOC displays to be used for drilling down into system and equipment status with minimal risk of losing situational awareness of plant state.

b) The MOC is also the location for the operator to launch automated test sequences for any system or plant equipment through the console workstations. The use of computerized testing significantly reduces the control panel space needed for hardwired test controls and unloads the operator from performing these routines.

c) The large screen display (LSD) panels (four large panels from the right) comprise both large computerized displays and annunciation units (at the top). These panels support operator situational awareness of overall plant state. Although the large displays are computerized providing flexibility to change, they are intended to show a fixed representation of key plant information pertinent to an operating state (e.g. full power operation, shutdown, etc.) with a limited number of selections available (the right-most LSD is intended to support specific crew tasks of the moment). The annunciation units will provide the alarm and status message lists

and fixed location representations similar to the window tiles in previous generation CANDU[2] control centres, for alarms of sufficient importance.

d) The 'Backup and Safety' panels at the left contain hardwired controls and displays required to maintain safety in accident conditions or in the event of a loss of the primary integrated computer-based HSI. These controls and displays are generally part of the safety systems. A portion of this panel will be patterned to replicate the corresponding displays and controls of the Secondary Control Area to minimize the differences from working in either area.

e) The shift interrogation console (SIC) is provided for interaction between the unit operator and shift supervisors or other staff as needed. Computer workstations are provided to allow information access by support staff without interrupting the operator. A large desk area is provided for printers/copiers/scanners, drawings and documentation. This station also doubles as a stand-up command post to direct unit operations during emergency situations.

3. ACR-1000 Design Process for Computer-based Displays

For the ACR-1000 project, Human Factors Engineering (HFE) follows the program plan outlined in Canadian Nuclear Safety Commission (CNSC) Regulatory Guide G-276 [2] and specifically the twelve elements of a human factors engineering program plan as described in NUREG-0711 [3]. These elements are further categorized into four stages: planning and analysis, design, verification and validation (V&V), and implementation and operation (see Figure 3-1). This paper will discuss elements 1 through 7 as they relate to the design of soft Human-System Interface displays. In particular the discussion will focus on the activities performed by the Control Centre (CC) design team developing soft displays and the integration of the Operations and Maintenance (O&M) team into that design process.

3.1 Human Factors Engineering Program Management

HFE program management defines the HFE activities for the ACR-1000[1] project and are documented in a Human Factors Engineering Program Plan (HFEPP). The ACR-1000[1] HFEPP and supporting design guidance documentation were prepared at the start of the project to ensure that human factors considerations are addressed throughout all project phases from conceptual design to commissioning. The application of HFE at the start, and throughout all phases, of the ACR-1000[1] project helps to ensure the following:

a) System/equipment processes of design and acquisition are provided with HFE relevant information.

b) Human-system interface (HSI) design supports operator situation awareness of plant/system states and the capability to respond appropriately.

c) Allocation of functions/tasks to human or machine in accordance with human cognitive and physical abilities.

d) Human-system interfaces are designed to minimize the likelihood of human error and to provide mechanisms, were practicable, for human error accommodation, detection, and recovery.

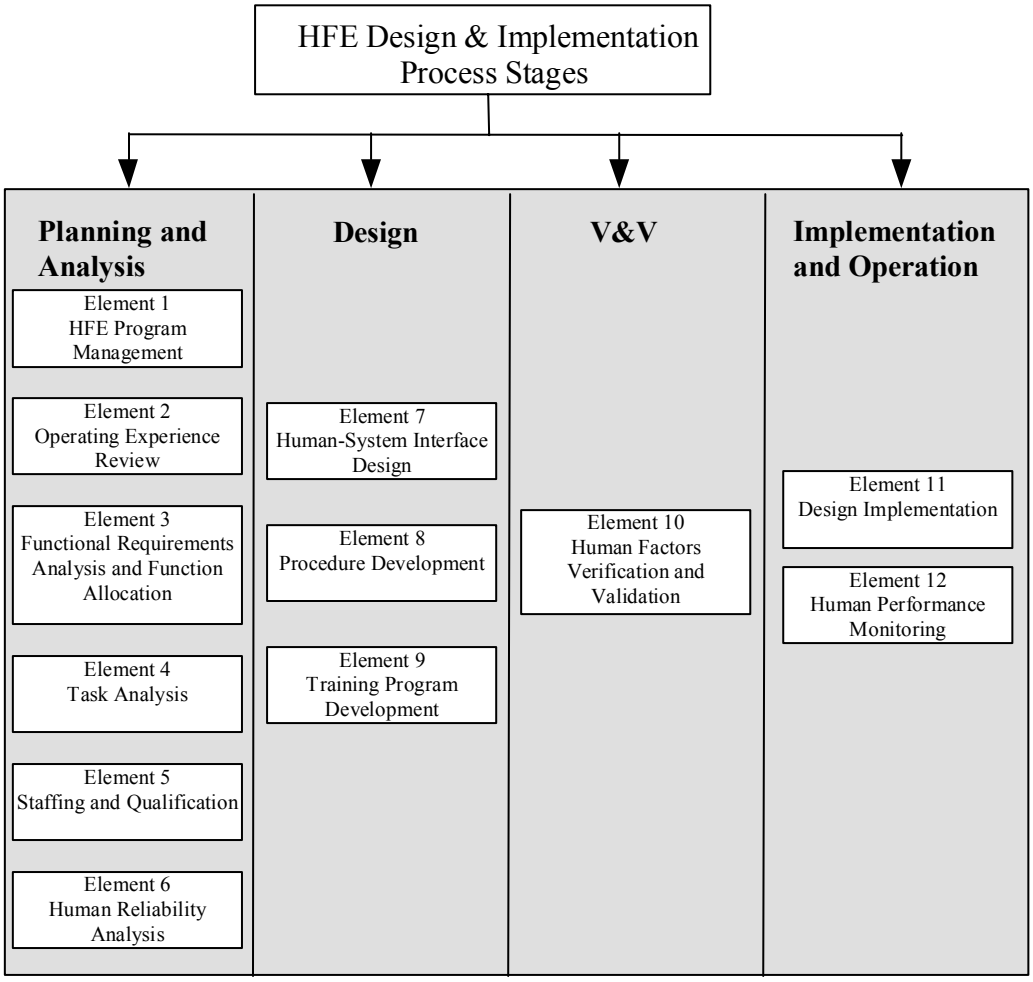

Figure 3-1 Human factors engineering program model.

3.2 Operating Experience Review

The objective of the Operating Experience Review (OER) is to identify and analyze issues from previous designs that are similar to the ACR-1000[1] reference design. Feedback issues from the OER that are relevant to the project are systematically reviewed, tracked, and recommendations recorded. The project has a procedure for managing such feedback issues.

In addition to the formal feedback process, the O&M team provides operating experience input to ACR-1000[1] designers to ensure the integration of operating and maintenance requirements into system designs.

The primary output of this element relevant to soft display design are the human error design issues related to human-system interfaces of reference systems or systems of similar functionality.

3.3 Functional Requirements Analysis and Function Allocation

The objectives of the ACR-1000[1] functional requirements analysis and function allocation (henceforth referred collectively to as "function analysis") are to:

a) Establish a description of the plant functions that are required to operate the plant to setpoints, to achieve safety and production objectives,

b) Establish the inter-relationships among plant functions, together with their performance measures and health indicators,

c) Describe the allocation of each function to the operator (human), automation, or a combination of both, and

d) Assess the adequacy of the functions against operational and human needs.

The process that the ACR-1000[1] project employs for function analysis has been previously described in a paper by Leger and Davey [4] and thus will not be described further.

Along with appropriate engineering disciplines, Operations and Maintenance provides feedback on both the functional decomposition and allocation. Human error and performance issues identified in the OER element may be explicitly acknowledged in the functional decomposition, but typically are considered in other elements.

The primary outputs of this element relevant to soft display design are the functional decomposition and function allocation. The function allocation assists in identifying the format of information required by an operator to perform a given function. The functional decomposition is used to identify goals that can be associated with goals for a display or set of displays. In addition to identifying display goals, the functional decomposition describes performance and health measures, control devices and feedback details, supporting functions, and initiating/terminating conditions.

Performance measures are concerned with the ability of a function to achieve its intended purpose. For example, if a function were to supply a flow, a measured flowrate would be a performance measure. Health measures are concerned with challenges to the ongoing availability of the function and in many cases related to supporting functions. Both of these measure categories provide the actual measure (e.g., l/m, mA, %) and the quality criteria associated with the parameter (e.g., engineering range, high/low alarm setpoints). These measures and criteria are a starting point for identifying the instrumentation parameters that are associated with a display or set of displays. Task analysis defines the detailed signals and their characteristics.

The functional decomposition also describes the control devices associated with a particular function, thus the controls required for a given display can be identified. Additionally, since the feedback information is identified, this information can be added to either a control dialog window or the display to provide an operator with the required information to identify whether or not a requested control action had the envisioned affect. Again, task analysis defines the details of how a given device is controlled.

Finally, identifying the functional detail helps illustrate the 'collective view' of the function - the starting point for identifying information overviews that might appear on large screen displays.

3.4 Task Analysis

The objective of task analysis is to identify the performance demands on plant personnel and the task requirements for accomplishing functions allocated to them. The primary task analysis technique employed is scenario-based tabular analysis. Scenarios are selected to cover a full range of plant operating modes (e.g., normal operations, disturbance operations such as upsets, transit conditions, and plant start-up and shutdown). A sampling strategy is employed to guide the selection of scenarios for the operating modes. For example, the following factors are considered when selecting scenarios:

- Critical tasks related to safety,
- Frequently performed tasks,
- Tasks with known or suspected performance issues,
- Range of task behaviours common to many operations, and
- Areas of significant HSI design change.

Task analysis scenarios contain the following details:

- Initiating conditions, such as imposed plant/system events or human actions/errors,
- Operation region and system state conditions, and
- Scenario ending conditions.

The primary input into the above scenario selection process is obtained, in part, from the details of the Functional Decomposition. The Operations and Maintenance team is involved in the selection of scenarios and providing subject matter expertise that will be employed during task identification, task breakdown, and task sequencing.

One output of the task analysis is a description of the information and control requirements. The description consists of:

- List of instrumentation required/used, and
- When/how these instruments/controls are used.

The first point identifies the information needed, information relationships as required to accomplish a task, and their relation to a function. These details are used to identify the instrumentation parameters to be displayed on a given screen.

The second point is of primary interest in the design of HSIs. The usage context, along with the control devices/feedback details identified in the functional decomposition and the human-machine allocation of the function related to a task, are then used to identify the control requirements for a given display. For example, the format of the information may differ if an operator is required to monitor a parameter and perform tasks based on its value, versus monitoring the status of a system that does both the monitoring and responds to changes in a parameter's value (e.g., a shutdown system).

Thus, the "how" question in regards to the instrumentation parameters usage is of great importance. Addressing this question helps to identify the appropriate graphical element (e.g., bar chart, trend, scatter plot) for presenting a single or set of parameters to an operator. For example, a task may request an operator to correlate information, thus suggesting that the information be easily accessible from one another and that the level of detail be provided (e.g., displaying the relationship on a single visual element such as a trend, displaying two digital readouts side-by-side).

The following information usage categories (extended from [5]) have been defined and are used to select appropriate graphical display elements:

- Single Variable Visual Element
    - A variable within limits
    - A variable with a constraint
    - A variable with a normal value
    - A variable that changes slowly over time
    - A variable where the rate of change is of interest
- Multivariate Visual Element
    - Multiple balanced or equivalent variables
    - Additive variables
    - Multiplicative variables
    - Multiple variables that determine system state
    - Multiple variables with interactions

These information usage categories are mapped to a set of graphical display elements, ordered by preference, which can satisfy the information need. An element from the set is selected by a designer in the implementation of a soft display. The selection process is affected by the element preference ordering, consistency in the application of an element to an information usage category, and physical space requirements for a given display.

3.5 Staffing and Qualification

An analysis of staffing qualification examines the organization and distribution of job responsibilities among the control centre operations staff and associated support staff. A prerequisite for successful ACR-1000[1] plant operation is having sufficient staff trained in the roles and responsibilities required for operating the station. The definition of crew member numbers, and their roles and responsibilities, are considered the basis for a license applicant to develop more complete definitions of the crew member expectations, to support staff training development programs and successful station operation.

The design of the soft displays may impact both the number of crew members required and the training program. Conversely, the personnel make-up of the minimum crew compliment may also impact the design of the soft displays. The Operations and Maintenance group is also responsible for defining the training program and thus will have feedback on the design of the HSI not only from an operations prospective but also from a training one as well.

3.6 Human Reliability Analysis

For the ACR-1000[1] project, Human Reliability Analysis (HRA) is performed as part of the Probabilistic Safety Assessment (PSA). From a HFE perspective, risk-important human actions identified in the PSA are used as input to the HFE design effort. The risk-important human actions are addressed during function/task analyses, HSI design, and procedure/training development. This ensures that these actions are well supported by the design and within acceptable human performance capabilities, thus reducing the likelihood of operator error and/or potential consequence of an error.

Depending on the actions and design barriers credited in the HRA, the design of a soft display may be affected. For example, additional barriers may be added in order to access a control dialogue or to execute a control request, to avoid an undesired action.

3.7 Human-System Interface Design

The human-system interface (HSI) design process represents the translation of function and task requirements into HSI characteristics and functions. This translation process uses a structured methodology to help ensure standardization and consistency in applying HFE principles as defined in NUREG-0711 [3].

Although HSI design encompasses both hardware and software interfaces, the focus of this paper is on the design of soft displays. As discussed previously, the inputs to the HSI design process include the outputs of the OER, function analysis and task analyses as discussed above. Other inputs include HFE design guidance on the following topic areas:

- Acronyms and Abbreviations
- Annunciation
- Colour Usage
- Computerized Display and Navigation

- HSI Symbology
- Parameter Display Information

The outputs of the OER, functional decomposition, function allocation, and task analyses are aggregated together by a Human Factors Specialist in a display functional specification document. This document allocates information and controls to displays and defines the use cases for each piece of information such that the optimal format for presentation can be chosen in the subsequent display design. The allocation and the information use cases are reviewed by the Operations and Maintenance team to confirm that the information and controls content of the displays will meet the function / task needs.

The display functional specification is then used by the designer to produce a soft display. The resulting displays are further verified and validated in an iterative fashion as system designs are finalized. Additionally, high-level overview displays can be generated when a sufficient number of information and control requirements have been identified for a number of related systems, by analyzing the instrumentation parameters and information usage requirements across multiple scenarios. The usability of such overview displays is tested with operations and maintenance subject matter experts. These subject matter experts may also provide alternative configurations for overview displays, either based on experiential knowledge or from relevant OER issues.

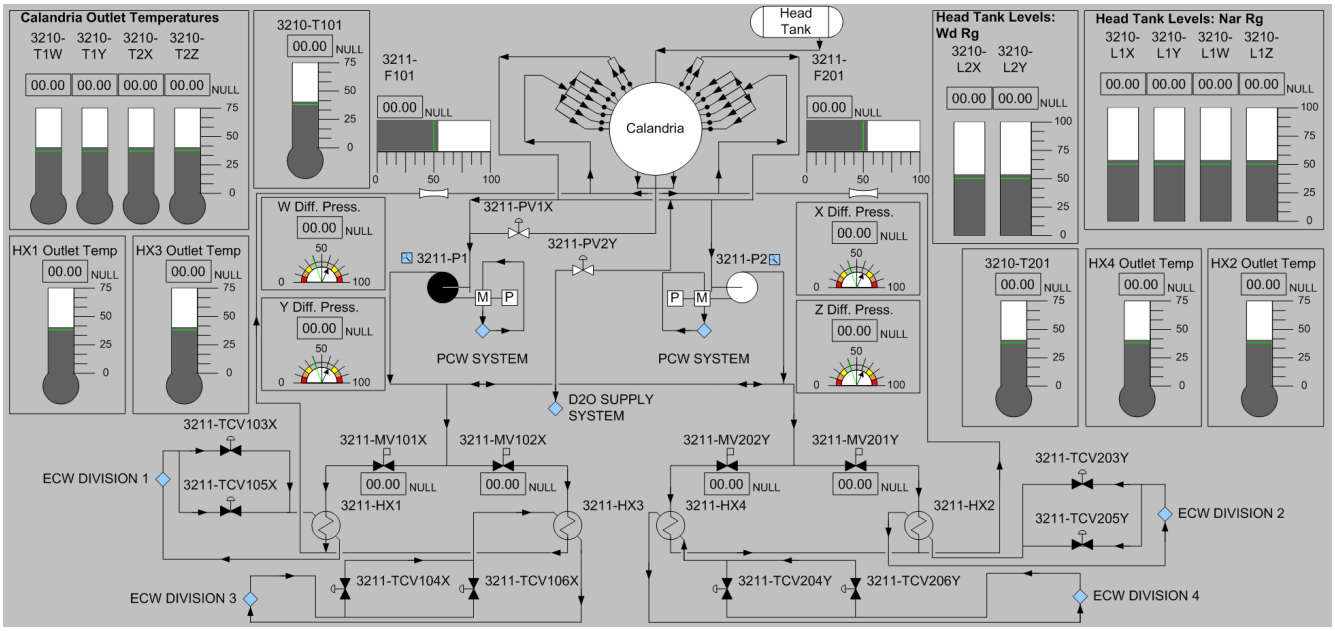

Figure 3-2 Main Moderator Circuit Display Example.

4. ACR-1000[1] Computer Based Display Example

The ACR-1000[1] Moderator System displays (see example display in Figure 3-2) are being developed using the process described in this paper. Following the Human Factors Engineering program described in Section 3.1 has formed the foundation for the process of developing the

displays and the resultant content. Operating Experience (Section 3.2) from AECL and industry databases and O&M staff inputs have been incorporated. The Functional Requirements Analysis and Function Allocation (Section 3.3) for the Moderator System and associated sub-systems have been completed and are reflected in the displays. The Task Analysis (Section 3.4) and Staffing and Training (Section 3.5), including normal, abnormal and emergency operating conditions are in progress. The remainder of the design steps and implementation for operation are to occur in the future and will follow the protocol outlined in this paper.

5. Conclusions

In following a rigorous process for the ACR-1000[1] soft display design, human factors engineering plays an integral role in ensuring the man-machine interface presents the right information to support safe and productive operation. The feedback from databases capturing CANDU operating experience, plus the input to the design process from experienced operations and maintenance personnel, along with systematic human factors engineering analysis are encapsulated in the soft Human-System Interface displays found in the main control room. In addition to strengthening design barriers to undesired events, the ACR-1000 design process helps to ensure improvements in: event recognition, recovery via the human-system interface, and utilization of station staff and plant resources.

6. References

[1] R. Leger, S. Malcolm, and E. Davey, "The Advanced CANDU Reactor Annunciation System – Compliance with IEC Standard and US NRC Guidelines", Proceedings of the 5th International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology (NPIC & HMIT), 2006, November 12-16.

[2] CNSC G-276, "Regulatory Guide, Human Factors Engineering Program Plans", Canadian Nuclear Safety Commission, June 2003.

[3] NUREG-0711, "Human Factors Engineering Program Review Model", Revision 2, U.S. Nuclear Regulatory Commission, February 2004.

[4] R. Leger and E. Davey, "The Role of Function Analysis in the ACR Control Centre Design", Proceedings of the 27th Annual Conference of the Canadian Nuclear Society, Toronto, Ontario, Canada, 2006 June 11-14.

[5] C. Burns and J. Hajdukiewicz, Ecological Interface Design, New York, New York: CRC Press, 2004.