INTERFAZ HUMANO-SISTEMA PARA EL REACTOR CAREM

ABAURRE, N. F.; FLURY, C. A.; PIERINI, J. P.; ETCHEPAREBORDA, A.;
BREITEMBÜCHER, A. J.; LEMA, F. M.

Comisión Nacional de Energía Atómica – Centro Atómico Bariloche

Resumen:
Asociadas a las actividades a ser desarrolladas por nuestro grupo de trabajo respecto de la construcción del simulador de entrenamiento del reactor CAREM, se tiene planificado el diseño de la interfaz humano-sistema (HSI) de la sala principal de operación del reactor. El objetivo del presente trabajo consiste en describir la planificación y la metodología utizada para el diseño de la interfaz HSI. Los productos de este proceso es obtener las especificaciones de la disposición de la Sala de Control y las especificaciones de las pantallas para el software de control.

Abstract:
Associated with activities to be developed by our working group on the construction of the reactor training simulator for the CAREM, we have planned the design of human-system interface (HSI) of the main control room. The goal of this study is to describe the planning and methodology used for the HSI interface design. The products of this process are the layout specifications of the Control Room and the screens specifications for control software.

1. Introducción:

El diseño de la interfaz humano-sistema (HSI en sus siglas en inglés) para centrales nucleares requiere un especial cuidado, ya que el operador juega un papel importante en la seguridad. Este cuidado especial se tiene sobre todo luego del accidente de Three Mile Island. El HSI propuesto para CAREM está conformado por una interfaz que hace uso de computadoras, para el control y monitoreo de la planta mediante software. Este tipo de interfaz computarizada trae beneficios tanto en la seguridad como en la operación de la planta.

La ventaja de la computarización de la sala de control en seguridad radica en que se simplifica los paneles de comando y de instrumentación en la misma, presenta la información en forma más inteligente para que el operador pueda planear y ejecutar correctamente las acciones de control y de seguridad. La ventaja para la operación radica en la reducción de costos disminuyendo la salida de operación de la planta, permitiendo la detección temprana de fallas y la gestión integral de la planta [1].

Una de las características del uso de pantallas para la interacción con la planta, es que el operador accede solo a una porción de la información de la planta dependiendo de la pantalla en la que está. Esto requiere del operador una tarea secundaria, además de la tarea principal que es la de controlar la planta. Esta tarea secundaria es la navegación entre las distintas pantallas. La tarea de navegación requiere de trabajo mental, ya que el operador debe memorizar cierta información para pasar de pantalla en pantalla, debe conocer cómo llegar a la pantalla que desea, por lo tanto el diseño de la interfaz juega un papel importante para disminuir los requerimientos de memoria y trabajo metal por parte del operador. Otra cuestión de diseño que tiene la interfaz computarizada es que en la interfaz tradicional, con vista rápida de los paneles, se obtenía el estado del funcionamiento de los sistemas, mientras que en los sistemas computarizados se debe diseñar pantallas que muestren en alto nivel estos estados.

Para reducir el trabajo mental el objetivo es diseñar las pantallas de forma tal que requieran de poca navegación para la realización de las tareas, acompañado del diseño de

pantallas que presenten la información con un alto nivel abstracción de manera que se pueda obtener el estado de un sistema de forma rápida. También se debe tener las mismas consideraciones sobre factores humanos que se tienen en la interfaz tradicional.

Para todo esto y en paralelo con el desarrollo del simulador de entrenamiento, se irá diseñando la interfaz, con la aplicación de alguna metodología, se logrará un diseño que minimice los errores humanos, mediante un análisis sistemático.

2. Sala de Control CAREM

El reactor CAREM contará con dos salas de control: la Sala de Control Principal (SCP) y la Sala de Control de Emergencia (SCE). Ambos contarán con un sistema computarizado además de la interfaz tradicional para los casos de visualización y actuación de los sistemas de seguridad, y también de un sistema que permita la parada de reactor como respaldo al sistema computarizado.

Se prevé que en la sala de control principal habrá en forma permanente cuatro personas que conformarán el plantel de operación (dos operadores, un supervisor y un oficial de radioprotección), alojados en distintas estaciones de trabajo. En cada estación de trabajo tendrá a disposición: VDUs (Visual Display Units = pantallas), teclado y dispositivo de puntero (mouse o track-ball). Con lo cual los operadores podrán navegar por las distintas pantallas. En particular los dos operadores tendrán a su disposición cuatro VDUs que serán altamente configurables pero una configuración típica de izquierda a derecha será: 1. acceso a información de los sistemas de seguridad, 2. pantalla de alarmas, 3. pantallas específicas para la ejecución de tareas y mímicos, 4. pantallas de apoyo a las tareas (manuales de procedimientos, diccionario de componentes, etc). Además habrá grandes paneles de pared (wall panels) que mostrarán un mímico general de la planta, lógicas de los sistemas de seguridad, configuración del núcleo, posición de las barras de control, valores del flujo neutrónico, lógica de enclavamientos de operación, sistema de visualización de parámetros de seguridad, información del sistema de monitoreo pos-accidente. Una porción de estos grandes paneles podrá ser configurada por los operadores para compartir información entre las personas del plantel de turno.

3. Metodología

En el desarrollo de la interfaz humano-sistema (HSI) para centrales nucleares se deben realizar consideraciones sobre los factores humanos. Se podría desarrollar el HSI de manera similar a la industria convencional, pero en ciertas situaciones la interfaz puede inducir a un error humano que evolucione en una situación peligrosa. Este tipo de errores puede ser debido a que el operador no tiene suficiente información de la planta (o se le brinde información incorrecta o se interprete de manera errónea) y deduzca un estado erróneo de la planta.

Es muy difícil plantear requisitos que debe tener el HSI para que la interfaz minimice los errores humanos que resulten de la operación. Por lo tanto se debe tomar una metodología de diseño para que garantice los objetivos. En la Figura 1, se muestra esquemáticamente la metodología a utilizar para llegar a los objetivos. En la misma se incluye una serie de análisis que se deben desarrollar para garantizar que el HSI no propicie el error del operador.

Lo primero que se realiza es un análisis de funciones y asignación de funciones. Dicho análisis consiste en definir cuales son las funciones para operar la planta. Se parte de los objetivos generales de la planta (seguridad, generación de electricidad, etc), se determina que funciones y sistemas son necesarios para llevar acabo esos objetivos, y que función de control es necesaria para controlarlo. Luego de identificadas las funciones de control se define, de

acuerdo a los requerimientos de esa función, si es realizada por el operador, por un automatismo o en forma mixta.

De las funciones asignadas al operador, se determinan las tareas que debe realizar para cumplir con los objetivos de las funciones. También se determinan las tareas que debe realizar los operadores para llevar la planta a distintos estados operacionales y que tareas debe realizar en el monitoreo de las funciones automáticas. Se debe describir cada tarea, que información necesita para realizarla, que decisiones debe tomar, en que tiempo debe efectuarla, con que confiabilidad debe realizarla y que actuación sobre el sistema debe realizar. Dicha descripción de las tareas, realizada por el operador, se puede utilizar para evaluar si la calificación del personal coincide con la tarea, y de este análisis se pueden obtener el manual de procedimientos.

Del análisis de funciones también se obtiene que funciones debe realizase en forma automática, esta información es útil en el diseño de los lazos de control y de los automatismos. Del proceso de diseño de la I&C se provee los diagramas donde se especifican los sensores, actuadores y lazos de control de cada sistema.

El diseño de HSI se realiza las distintas pantallas para la interfaz por computadoras, la base del interfaz es una serie de pantallas que representa los diagramas de instrumentación y tuberías (P&ID), que en ellos se representa la interrelación entre los componentes físicos del proceso para un determinado sistema con sus variables, válvulas, bombas, etc. En la Figura 2 se observa una pantalla típica de P&ID, en este caso para el sistema secundario del Open Pool Light-Water Reactor (OPAL). También otras pantallas son los diagramas eléctricos. Estos tipos de pantalla están organizados de acuerdo a una jerarquía que facilitan la navegación. La jerarquía responde a diferentes niveles de abstracción, los niveles más bajos cuenta con más detalle de las variables, los niveles superiores muestran los flujos de procesos. Para el caso de los niveles inferiores son pantallas P&ID o diagramas eléctricos en tanto que para los niveles superiores son pantallas de flujo de procesos. Las pantallas de flujo de procesos son la interrelación entre el sistema y sus componentes principales mostrados en forma cualitativa. Este tipo de diagramas sirven para obtener información rápida de los estados de cada sistema. Las pantallas intermedias van dando más detalle de cada sistema, presentado más información de parámetros relevantes.

Cada elemento de los diagramas anteriores conducirá a otros diagramas o tendrán asociado un ¨faceplate¨. Estos ¨faceplate¨ son pequeñas ventanas donde se puede actuar y tomar acción sobre algún componente físico. El ¨faceplate¨ de componentes debe ser diseñado tratando de imitar ciertas características de paneles de comando, para que se diferencie totalmente de un diálogo estándar, y el operario tenga más conciencia de que está realizando una acción de control. El ¨faceplate¨ tiene que proveer suficiente retroalimentación de las acciones de control que se tomen en él, para asegurar que la acción remota tuvo éxito.

De la descripción de las tareas del operador se puede diseñar pantallas que contengan la información y controles que se necesiten para desarrollarlas. Las tareas se pueden realizar interactuando tanto en los diagramas P&ID y eléctrico, o en los diagramas orientados a tareas. La dificultad de los primeros diagramas es que se requiere una determinada tarea de navegación y además, también pueden requerir memorizar parámetros y estados al pasar de un diagrama a otro. En cambio, las pantallas orientadas a tareas contiene toda la información necesaria, y todos lo enlaces a los P&ID de los sistemas que intervienen en la tarea. En estas pantallas se tendrá retroalimentación de la acción que se tome sobre los componentes físicos.

Se diseñarán además pantallas orientadas a funciones. Este tipo de pantallas servirán para el monitoreo de todos los sistemas que intervengan en determinado objetivo o meta. Por ejemplo una pantalla que muestre los parámetros de los sistemas que intervienen en la integridad de la contención. Estas funciones se determinan mediante el análisis de funciones. Las pantallas orientadas a funciones solo sirven para monitoreo, pero se le puede proveer con

enlaces a otras pantallas (P&ID, eléctricos o de tareas) para tomar alguna acción sobre el sistema.

Las consideraciones anteriores en el diseño del HSI, y ciertas recomendaciones sobre cómo incluir los factores humanos en el diseño, se obtienen de la norma de la IEEE 1289 [2].

En la etapa de verificación y validación (V&V) se prueba el sistema computarizado obtenido en el diseño. Para esto se propone varias iteraciones de V&V y el proceso de diseño. Esto permite evaluar el diseño del HSI y su desempeño en forma global, y generar modificaciones en el diseño del mismo. Ya que se tiene el HSI conjuntamente con el simulador se puede estudiar e investigar en forma concreta la aplicación de factores humanos, depurando así el diseño. También se prevé la participación de una misión de especialistas en factores humanos provenientes de Halden para verificar el diseño en estos aspectos. Otra verificación adicional será comprobar que el diseño cumpla con las normas NUREG-0700 [3] e IEC 962[4].

El último paso es el desarrollo, después de depurar y validar el diseño, de las especificaciones para la implementación del HSI con los sistemas comerciales. Las especificaciones incluyen la descripción de la pictografía de cada pantalla, el comportamiento, su orden jerárquico y la navegación.

Debido a que el desarrollo del HSI está atado al desarrollo del simulador se prevé el desarrollo en dos etapas coincidentes con las dos primeras etapas de desarrollo del simulador.

3.1. Primera Etapa:

Se realizará en conjunto con el desarrollo del primer simulador que se utilizará para ensayos de los lazos control. Dicho simulador solo contará con un número reducido de sistemas modelados y estados operacionales. Por lo tanto, se aplica la metodología propuesta solo para ese alcance del modelo y como producto de esta primera etapa se obtendrán las librerías de los elementos a utilizar en las pantallas de interfaz computarizada y solamente las pantallas preliminares de los sistemas modelados.

Se realizarán pantallas de P&ID para el manejo del simulador 1, para ello se comenzará a realizar el análisis de funciones, y se designarán las funciones al operador, al automatismo o a ambos de manera conjunta.

Las librerías definidas en esta etapa consistirán en los diagramas de los componentes físicos de los sistemas para realizar P&ID, también poseerá un conjunto de ¨faceplates¨ que permitirán la acción o monitoreo de los componentes. Se definirá además la barra de herramientas, la barra de navegación, la barra de estado y los menúes.

El desarrollo de las librerías se realizará con el programa ProcSee[5], dibujando las distintas clases de objetos que se utilizan en las distintas pantallas. El ProcSee posee un lenguaje orientado a objetos. Cada objeto está definido por una clase, posee atributos -variables que son sus propiedades o definen su estado-, y tiene funciones, que al ser llamadas actúan sobre los atributos. Existen también los diálogos, que son funciones que se activan por determinados eventos. Para generar una clase, se utiliza el editor de gráfico del ProcSee (GED). Se comienza a dibujar en el editor mediante figuras geométricas (líneas, rectángulos, círculos. etc.), y cada figura generada es un objeto en el lenguaje. Luego se programa las funciones y los diálogos de cada objeto gráfico. Para esto se usa el lenguaje pTALK de ProcSee, que es similar al lenguaje C++. Dicho lenguaje tiene la ventaja que permite la asignación dinámica de variables, permitiendo tener un conjunto de variables compartido con otros programas: la modificación de una de las variables modifica todos los atributos en el que intervenga dicha variable. Por ejemplo, si se quiere generar un gráfico de barra, se realiza mediante un rectángulo cuya altura se asigna dinámicamente a la variable que se quiera representar. Los diálogos permiten que al producirse un evento, por ejemplo, doble click sobre un elemento gráfico, se ejecute un código configurado en pTALK.

Las pantallas en ProcSee se crean igual que una clase, mediante figuras geométricas y la inserción de objetos de las clases definidas en las librerías. Como ejemplo, en la Figura 2 se observa una pantalla creada por ProcSee para el circuito secundario del OPAL, donde se muestra un diagrama P&ID conformados por distintos elementos: bombas, torres de enfriamiento y las variables de los instrumento del sistema. Cada elemento anterior es un objeto que se define a través de una clase, y el conjunto de dichas clases conforma una biblioteca.

El desarrollo del software para esta etapa, es la realización de la arquitectura de software mostrada en la Figura 3, que deberá resolver la comunicación entre los modelos de los sistemas realizados en Relap y Simulink con el ProcSee. El ProcSee comparte ciertas variables con otras aplicaciones mediante el protocolo SWBus, y provee de una biblioteca para C, para crear programas que se comuniquen con el ProcSee. Por lo tanto, se creará un programa que maneje el flujo de datos entre los modelos y el ProcSee. El programa también debe permitir modularidad, o sea permitir de forma fácil de configurar la inclusión de nuevos modelos o nuevas pantallas.

El Model Manager (M.M.) cumple la función de sincronismo entre los distinos procesos (modelos, ProcSee, S.M.), y es el encargado de manejar en forma sincrónica las variables que comparten cada proceso. El M.M. debe permitir modularidad, o sea que se pueda conectar cualquier proceso que requiera las variables compartidas. Se definirá un protocolo para dicha conexión.

La interfaz ProcSee recibe en forma síncrona del M.M los parámetros de los modelos, e implementa un servidor para que se conecte en éste todas las estaciones de trabajo del operador. En este servidor se ejecuta el API (interfaz de programación de aplicación) del ProcSee, por el cual enlazará los vectores de M.M. con las estaciones de trabajo. También en el servidor se proveerá la funcionalidad del histórico de variables y eventos.

Una vez enlazado, se validará el diseño de cada elemento de la librería de acuerdo a las normas [3] y [4], y se realizará diferentes estudios sobre ellas. Un punto a tener en cuenta en el diseño, es evaluar que el operador tenga información de que la acción producida en un elemento cualquiera, produzca la acción remota correspondiente. Por ejemplo, si se actúa en un ¨faceplate¨ de una válvula mediante la acción de abrir, el ¨faceplate¨ debe contener información del éxito de la operación.

3.2. Segunda Etapa:

En esta etapa se dispondrá el diseño completo de I&C y bien definido los estados de operación y el equipamiento para la sala del simulador. Esto permitirá realizar el análisis de tareas y aplicar en forma entera la metodología explicada. Con la librería validada en la primer etapa se diseñará las pantallas P&IC y eléctricos de todos los sistemas, se realizarán las pantallas orientadas a tareas y las pantallas orientadas a funciones. La navegación entre distintas pantallas estará de acuerdo al análisis de las tareas que se realicen en cada pantalla. En esta etapa se realizará varias iteraciones entre V&V y el diseño para validar contra normas, y con diferentes estudios sobre factores humanos.

Para el diseño de las pantallas se seguirá utilizando el ProcSee, y la arquitectura de software desarrollada en la primera etapa para la comunicación, con lo cual se editará mediante GED cada pantalla prevista, en análisis de funciones y tareas. En las pantallas P&ID y diagramas eléctricos, se tendrán consideración cuando se las diseñe sobre las tareas que se hagan sobre ellos para optimizar la navegación entre pantallas.

Una de las tareas de esta segunda etapa es la definición de cada alarma y la presentación en las pantallas de alarmas. La tarea es definir cada alarma, que variable la dispara, cual es la lógica de disparo y los límites de disparo. Para presentación en pantalla se dispondrá de la lógica de supresión y de priorización, para organizar la presentación y suprimir aquellas

alarmas, que no sean relevantes para el modo de operación de la planta o para el interés del operador en ese momento. Esta tarea consiste en relevar y cargar todas las alarmas en una base de datos. Dicha base de datos contiene la definición de cada alarma, las lógicas de disparo y de supresión. Se utilizará COAST, un programa de software desarrollado en Halden para el desarrollo de sistemas avanzados de alarmas, que posee un lenguaje lógico orientado a objeto, diseñado especialmente para el tratamiento de alarmas.

COAST funciona de la siguiente forma: se crea un objeto para cada una de las alarmas, en cada objeto se define las propiedades de la alarma, y las lógicas de disparo, supresión, etc. COAST contiene una interfaz programación en C que permite introducirle las variables de las alarmas y otra para introducir comandos de lenguaje COAST para extraer información sobre los estados de los objetos y presentarla en una pantalla del ProcSee.

La programación consiste en generar las clases de los objetos para cada tipo de alarma, se define las variables de estado de alarma y todas las lógicas asociadas a los cambios estados. Para facilitar la programación desde la base de datos de todas las alarmas, se configurará el tipo de clase de alarma, y se realizará un programa que genere los códigos en COAST desde la base de datos.

En el desarrollo del software en esta etapa consistirá en la realización del Simulator Manager (S.M). Éste módulo, como se muestra en la Figura 2, incluye la consola del instructor y permite al instructor generar los eventos sobre la simulación.

4. Conclusión:

La aplicación de una metodología en el diseño de la interfaz humano-sistema (HSI) y la sala principal de control, junto con el desarrollo del simulador de entrenamiento para operadores, permite validar y verificar el diseño antes de su implementación. El simulador servirá para realizar estudios sobre factores humanos, y evaluar el desempeño del operador en operación normal y anormal.

El tener una metodología permite demostrar que en el diseño del HSI, se utilizaron criterios para una mejor desempeño y minimizar la posibilidad de errores humanos.

En dividir en dos etapas el desarrollo del simulador, se puede aprovechar, que la primera etapa, sirva para la aplicación parcial de la metodología propuesta, el desarrollo del software y herramientas necesarias para aplicarla. Esto permite agilizar la aplicación de la metodología en la segundo etapa, ya con un modelo completo de la planta y realizar el diseño final.

5. Referencias

[1] Sun, Bill K.H., Kossilov Andrei N.. ¨THE COMPUTERIZATION OF NUCLEAR POWER PLANT CONTROL ROOMS¨(Advances in Nuclear Science and Technology, Volume 25, Edited by Lewins and Becker, Plenum Press, New York, 1997)

[2] IEEE - ¨Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations¨ (Institute of Electrical and Electronics Engineers, 1998).

[3] NUREG 0700 – rev. 2 ¨Human-System Interface Design Review Guidelines¨ (U.S. Nuclear Regulatory Commission, 2002)

[4] IEC 964 - ¨Design for Control Rooms of Nuclear Power Plants¨ (International Electrochemical Commission, 1989).

[5] ProcSee, www.ife.no/departments/visual_interface_technologies/products/procsee/

6. Figuras

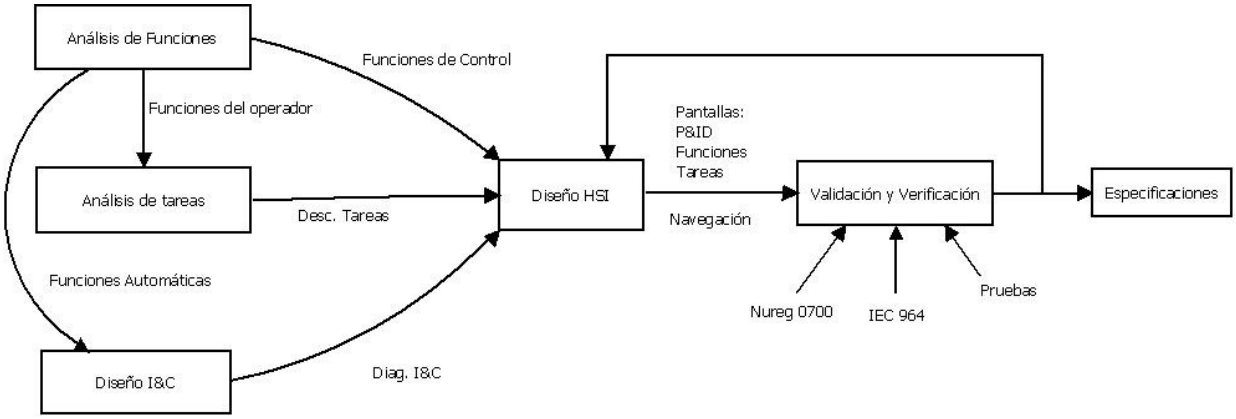

Figura 1. Metodología de desiño de HSI

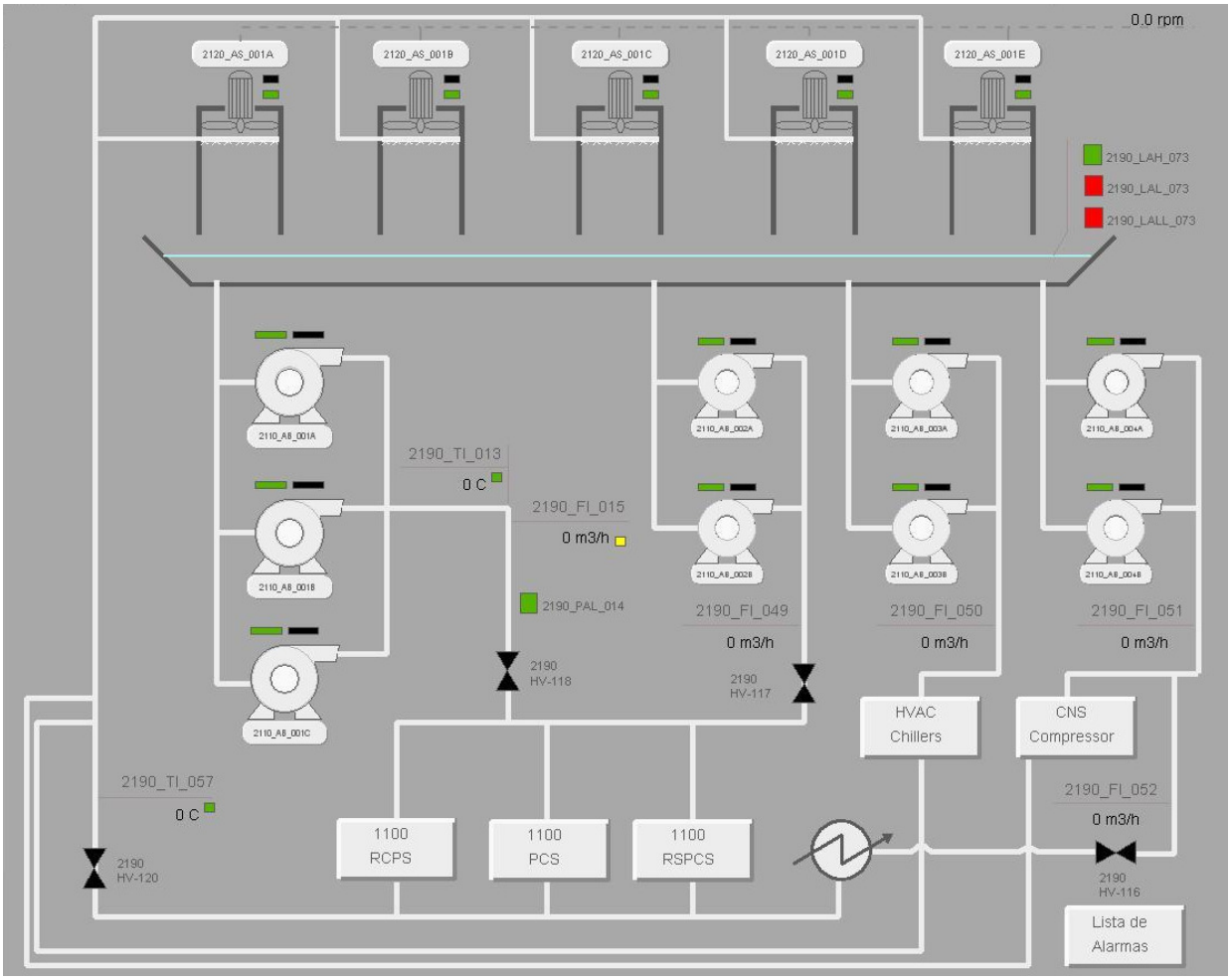

Figura 2. Pantalla P&ID del sistema secundario del OPAL

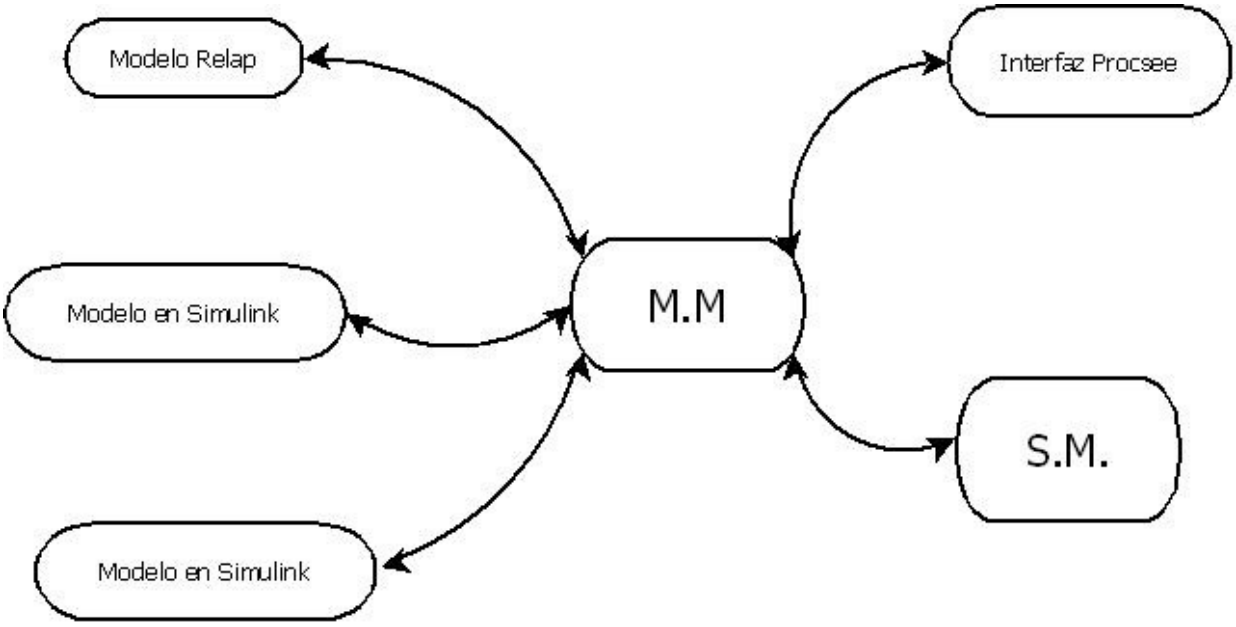

Figura 3. Arquitectura de Software del Simulador.