UNIVERSIDAD POLITÉCNICA DE MADRID

ESCUELA TÉCNICA SUPERIOR DE INGENIEROS DE MINAS

Desarrollo de una metodología de simulación de secuencias de accidente en centrales nucleares de agua ligera considerando actuaciones del operador

TESIS DOCTORAL

Antonio Expósito Lorenzo
Licenciado en Ciencias Físicas por la Universidad Autónoma de Madrid

2006

DEPARTAMENTO DE SISTEMAS ENERGÉTICOS

ESCUELA TÉCNICA SUPERIOR DE INGENIEROS DE MINAS

Desarrollo de una metodología de simulación de secuencias de accidente en centrales nucleares de agua ligera considerando actuaciones del operador

TESIS DOCTORAL

Autor: Antonio Expósito Lorenzo
Licenciado en Ciencias Físicas por la Universidad Autónoma de Madrid

Director: Dr. José César Queral Salazar
Doctor en Ciencias Físicas por la Universidad Nacional de Educación a Distancia

2006

UNIVERSIDAD POLITÉCNICA DE MADRID

(D-15)

Tribunal nombrado por el Magfco. y Excmo. Sr. Rector de la Universidad Politécnica de Madrid, el día ..... de ..... de 200....

Presidente: _____

Vocal: _____

Vocal: _____

Vocal: _____

Secretario: _____

Suplente: _____

Suplente: _____

Realizado el acto de defensa y lectura de la Tesis el día ..... de ..... de 200.... en la ET-SI/Facultad.....

EL PRESIDENTE

LOS VOCALES

EL SECRETARIO

Resumen

En la presente tesis se expone el trabajo realizado para el desarrollo de un sistema de simulación para centrales nucleares, denominado simulador integral TRETA / COPMA-III, que permite la simulación tanto de los procesos termohidráulicos que tienen lugar en este tipo de instalaciones, en operación normal y de emergencia, como de las actuaciones del equipo de operación relacionadas con la gestión de las situaciones de emergencia. La simulación de los procesos termohidráulicos se lleva a cabo mediante el uso del simulador TRETA (PWR) o TIZONA (BWR), ambos desarrollados por el Consejo de Seguridad Nuclear (CSN). En lo que respecta a las actuaciones humanas, y partiendo del hecho de que en este tipo de instalaciones la gestión de las emergencias está fuertemente procedimentada, se emplea un simulador de procedimientos desarrollado por el Halden Reactor Project (HRP) denominado COPMA-III, adaptado para su uso en el simulador integral.

Esta nueva herramienta se caracteriza principalmente por su modularidad y su capacidad de interconexión con otros códigos. De forma individual, los diferentes códigos que componen el simulador presentan capacidades avanzadas en sus modelos. Por un lado, el simulador TRETA presenta gran versatilidad a la hora de definir el grado de complejidad en la simulación de los procesos, abarcando en el caso de las centrales nucleares un amplio rango de operación, tanto en operación normal como en situaciones de emergencia. En lo que respecta al simulador COPMA-III, permite la simulación automática de actuaciones humanas procedimentadas o planeadas, es decir, de todas aquellas actuaciones manuales de las cuales se pueda desarrollar un modelo determinista a priori, incluyendo aspectos de tiempos de ejecución y carga de trabajo obtenidos por estudios adicionales. Respecto al carácter modular de la herramienta, cabe destacar que hace posible incluso la sustitución de los simuladores de proceso o de procedimientos y la implementación de cualquier otro simulador que se considere más apropiado para otras necesidades.

Este sistema de simulación, del cual se presenta sus especificaciones y una primera versión prototipo, no solo permitirá validar el diseño de los procedimientos, sino que también se podrá emplear en la verificación de la consistencia de los análisis llevados a cabo durante la realización de los estudios de seguridad. Este último aspecto es de especial importancia, pues estos estudios no incluyen, salvo raras excepciones, la evaluación de forma dinámica del impacto de las acciones del operador en el análisis de las secuencias accidentales.

Summary

This thesis presents the work carried out to develop a simulation system for nuclear power plants, denominated TRETA / COPMA-III integrated simulator, which allows the simulation of the thermalhydraulic processes that take place in this type of facilities, in normal operation and emergency operation, as well as the control room crew actions related with the management of the emergency situations. The simulation of the thermalhydraulic processes is carried out by means of the TRETA (PWR) or TIZONA (BWR) simulators, both developed by the Spanish Nuclear Council (CSN). In what concerns to the simulation of the human performance, and taking into account the fact that in this type of facilities the management of the emergencies is strongly proceduralized, the COPMA-III procedures simulator is used. This simulator has been developed by the Halden Reactor Project (HRP), and it was adapted by the HRP development team for its use in the integrated simulator.

This new tool is characterized mainly by its modular structure and its interconnection ability with other codes. In an individual way, the different codes that compose the simulator present advanced capacities in its models. Firstly, the TRETA simulator presents great versatility in defining the grade of complexity in the simulation of the processes. On the other hand, regarding to the COPMA-III simulator, it enables the automatic simulation of human actions proceduralized or planned, that means, all of those manual performances of which it is possible to develop a deterministic scheme, including aspects of timing and work load. Concerning the simulator package modular structure, it makes possible even the substitution of the process or procedures simulators and the implementation of any other simulator that it is considered more appropriate for specific necessities.

This simulation system not only could be applied to validate the procedures design, but rather could be use in the verification of the consistency of the analyses made in the safety analysis. This last aspect is specially relevant, because these studies don’t include, except for seldom cases, the dynamic evaluation of the operator actions impact in the analysis of the accidental sequences.

Agradecimientos

Como es lógico, el resultado de este tipo de trabajos no es fruto de la dedicación y el esfuerzo de una única persona, sino del de muchas de ellas, tanto a nivel profesional como personal.

Primeramente, quisiera agradecer el apoyo recibido del área de Modelación y Simulación del Consejo de Seguridad Nuclear: Miguel Sanchez, Francisco Javier Hortal, Jose María Izquierdo, Enrique Meléndez y Roberto Herrero. Os estoy profundamente agradecido.

Agradecer especialmente el apoyo que me ha dado a nivel técnico y personal, tanto durante la realización de esta tesis, de la cual es director, como desde que tengo el placer de conocerle, agradecerle a César Queral todo, y con todo intento reflejar demasiado. Muchas gracias por apoyarme, animarme y soportarme. De la misma forma, quisiera dar las gracias a Juan Antonio Quiroga y Aitor Ibarra por su trabajo y humor, sobre todo por el humor y más que nada por su trabajo. Nunca había trabajado riéndome tanto.

Agradecer a todos aquellos que comparten mis buenos y malos momentos, día a día, durante mis jornadas de trabajo, en el Área de Ingeniería Nuclear del Departamento de Sistemas Energéticos de la ETSI de Minas de la UPM; a los que ya se fueron, que espero seguir viendo, y a los que están, que espero sigan mucho tiempo: Alberto, Isaac, David, José, Laura y un largo etcétera.

Finalmente, hay otro tipo de esfuerzo y dedicación mucho más importante, del cual uno es beneficiario y deudor de por vida. Por ello, cualquier oportunidad de agradecer tanto siempre será insuficiente.

Agradezco a mi madre todo lo que ha hecho por mí, y lo que sé que aún hará y lo que haría. Eres única. No te preocupes, no te haré leer este *matapersonas*. A mi padre, porque has sido ejemplo, voz en la distancia y mucho más de lo que puedas imaginar. A mis hermanos, el acicate intelectual de mi infancia, el apoyo en todas mis empresas, la tranquilidad de saber que siempre tendré a alguien para lo que sea. Que te toque la lotería es tener suerte, lo mío con teneros a vosotros va más allá de las palabras. A toda mi familia: Dori, Jose, Marta (bien sabes que tu nombre podría ser el primero de todos los que aparecen en esta página y todos los adjetivos irse detrás de él, ¡se los lleva de calle!). Abuela, serás bisabuela y lo que aún te queda, al menos por mi parte. A los que ya no están, lala y abuelo, sigo adelante pensando en vosotros, todo lo que hago lo hago pensando en vosotros.

No me olvido de ti. Sin tu apoyo no habría podido terminar esta tesis y hacer otras tantas cosas. Espero que la vida me dé infinitas oportunidades de agradecerte y devolverte.

A todos, especialmente a los que no aparecéis, GRACIAS.

Índice general

Índice de figuras

Índice de gráficas

Índice de tablas

Introducción

La importancia del factor humano en los resultados de la evaluación de los incidentes y accidentes operacionales en centrales nucleares y los estudios de seguridad es especialmente relevante. Por una parte, la experiencia operativa muestra que, considerando los reportes realizados a instituciones tanto internacionales como nacionales, el 48 % de los sucesos registrados está relacionado con fallos humanos y que la mayoría de los incidentes de mayor gravedad podrían ser atribuidos a fallos de esta naturaleza. Teniendo en cuenta los estudios de seguridad que se realizan en este tipo de instalaciones, el porcentaje de sucesos identificados como origen de secuencias accidentales y que están relacionados de una forma u otra con actuaciones humanas asciende hasta el 65 %. Generalmente, en estos casos, se encuentra como uno de los principales orígenes del error humano intolerables violaciones de los procedimientos o fallos de diseño de los mismos. Por todo ello, la evaluación de los procedimientos de operación de las centrales nucleares y el estudio y mejora del papel del equipo de operación en la gestión de las emergencias se ha convertido, a lo largo de los últimos diez años, en una línea de investigación de especial relevancia. Las disciplinas implicadas, entres las que se encuentran la ciencia cognitiva y los estudios de ingeniería relacionados, han experimentado un desarrollo sin precedentes.

El objetivo de esta tesis ha consistido en desarrollar una herramienta que complemente los métodos tradicionales de evaluación de procedimientos, dotándolos de carácter prospectivo mediante la simulación integrada de la planta y las actuaciones humanas. Por una parte, la simulación de los procesos termohidráulicos se lleva a cabo mediante el uso del simulador TRETA, orientado a la simulación de centrales de agua a presión (PWR) y desarrollado por el Consejo de Seguridad Nuclear (CSN). En lo que respecta a la simulación de las actuaciones humanas, y partiendo del hecho de que en este tipo de instalaciones la gestión de las emergencias por parte del personal de operación de la sala de control está fuertemente procedimentada, se emplea un simulador de procedimientos desarrollado por el Halden Reactor Project (HRP) denominado COPMA-III, adaptado para su uso en el simulador integral. La realización del trabajo se ha llevado a cabo en el Departamento de Sistemas Energéticos de la Universidad Politécnica de Madrid (DSE-UPM) dentro del marco de dos proyectos de investigación financiados por el CSN (2003-2007). El grupo de investigación del DSE, del cual el autor es miembro en calidad de investigador principal, ha contado con el apoyo técnico del personal del área MOSI del CSN, la colaboración del grupo de trabajo encargado de los desarrollos informáticos de la Universidad Complutense de Madrid (UCM), y el personal de desarrollo del simulador de procedimientos COPMA-III del HRP.

La herramienta diseñada y de la cual se ha realizado un prototipo, es útil para:

- Verificar que los procedimiento de operación pueden ser entendidos y ejecutados por los operadores.
- Verificar que las respuesta de la planta en base a la ejecución de dichos procedimientos es la esperada.
- Identificar las situaciones potenciales en las que el juicio de los operadores respecto a las acciones a considerar es inconsistente con los procedimientos.
- Estudiar las consecuencias de la realización de errores de omisión o comisión y las posibilidades de realizar actuaciones de recuperación.

A lo largo de los capítulos que componen esta tesis se presenta el desarrollo del simulador integral TRETA / COPMA-III. En el capítulo primero, se realiza una introducción al tratamiento de los factores humanos en la industria nuclear, considerando principalmente los aspectos relacionados con los estudios seguridad y la gestión de las emergencias. El objetivo del capítulo es constatar que los procedimientos de operación de emergencia son el pilar fundamental, no solo de la intervención de los operadores en la gestión de emergencias, sino que también son un complemento fundamental durante el diseño de controles y sistemas de las centrales nucleares y la evaluación del riesgo en los estudios de seguridad de estas instalaciones.

A partir de las conclusiones obtenidas en este primer capítulo, en el segundo capítulo se presenta de forma resumida la herramienta desarrollada para la evaluación integrada de los procedimientos de operación de emergencia, el simulador integral TRETA / COPMA-III. En este capítulo se describen los diferentes elementos que la componen, introduciéndolos de forma somera, a saber: el código termohidráulico TRETA, el código de simulación de procedimientos COPMA-III y la interfase de comunicaciones basada en la librería SWBus.

En los capítulos siguientes, capítulos tres, cuatro y cinco, se describe de forma pormenorizada los diferentes trabajos realizados relacionados con cada uno de los elementos del simulador integral. En el capítulo tres se introduce el modelo genérico de planta PWR-W desarrollado para el código TRETA, destacando la descripción detallada de las partes del modelo y el conjunto de transitorios simulados para la verificación del mismo. De la misma forma, el capítulo cuatro trata la definición de la metodología de computerización de los procedimientos de operación de emergencia de una central PWR-W y su aplicación al desarrollo de diferentes modelos de procedimientos, mostrando resultados de su simulación sin acoplar al simulador de planta. Finalmente, el capítulo cinco presenta la solución adoptada en cuanto a la interfase de comunicaciones se refiere, la definición de la funcionalidad de la misma, la implementación física realizada en ambos simuladores y el resultado de las pruebas funcionales desarrolladas para su verificación.

Una vez se han presentado los resultados de la verificación de las comunicaciones del simulador integral TRETA / COPMA-III y los modelos de planta y procedimientos por separado, en el capítulo seis se lleva a cabo la aplicación del simulador a un conjunto de secuencias de

roturas en el secundario con el objetivo de hacer una verificación completa de la herramienta. Tras realizarse un estudio bibliográfico extenso de este tipo de transitorios, los resultados de la simulación son evaluados y se extraen conclusiones sobre los resultados obtenidos. Adicionalmente, se comentan de forma detallada las modificaciones realizadas en el modelo de planta para su integración con el modelo de bajo nivel de detalle de los procedimientos de emergencia desarrollado para la simulación de este tipo de secuencias.

Finalmente, en el capítulo siete, se detallan las conclusiones generales del trabajo. En este capítulo se incluye un estudio de las limitaciones del simulador integral y las posibles mejoras, definiendo las líneas de trabajo que se están realizando a corto plazo y aquellas a considerar en un futuro.

Capítulo 1

El factor humano en la industria nuclear

Índice

Está reconocido ampliamente que el error humano tiene gran impacto en la fiabilidad de sistemas complejos. La experiencia operativa muestra que las actuaciones humanas desempeñan un papel esencial en la seguridad de todo tipo de actividades. De hecho, se estima que que el factor humano está implicado entre en un 50 % y 90 % de los accidentes que se dan en sistemas complejos y de alta fiabilidad, dependiendo del sector considerado, demostrando que la contribución del factor humano al comportamiento de un sistema es, al menos, tan importante como la fiabilidad de los componentes.

Así, en la industria química, cerca del 27 % de los accidentes ocurridos en los Estados Unidos de América (EUA) durante el periodo de 1987 a 1996 fueron debidos a errores humanos, EPA (1999), existiendo estadísticas similares para la industria aeronáutica Mc Fadden (2003), donde se estima que el 71 % de los accidentes tienen su origen en un fallo del piloto. Se han realizado multitud de trabajos de revisión bibliográfica en cuanto al impacto del error humano en las diferentes industrias, pudiendo destacar el trabajo de Park et al. (2005) de entre los más recientes.

En general, y según la fiabilidad y las técnicas de mantenimiento de sistemas y componentes va mejorando y los métodos de evaluación del factor humano se perfeccionan, en los últimos diez años se ha venido incrementando la importancia del factor humano es los incidentes registrados en todas las industrias. Para el caso de la industria nuclear, NEA (2004), se ha pasado de valores del 45 % en los primeros estudios de los años 80 a aproximadamente al 55 % de los últimos años. Hay que destacar que este incremento ha sido más drástico en otras industrias, estimándose entre el 20 % de 1960 hasta el 80 % en 1980, Hollnagel (1994), ya que no en todas ellas se consideró en factor humano en el diseño y análisis de seguridad, tal como se hizo en el sector nuclear.

Dentro de los estudios de seguridad en el sector nuclear, Rasmussen (1975) concluyó que el error humano contribuía en un 65 % de los accidentes considerados, alcanzando tanta o mayor importancia como los correspondientes a fallos de sistemas. La Comisión Reguladora Nuclear de los EUA (*Nuclear Regulatory Commission*, NRC) estima que el error humano está involucrado en cerca del 65 % de los incidentes anormales de forma directa e indirecta, Trager (1985). Según los datos del sistema de información de incidentes de la IAEA (*Incident Reporting System*, IRS), el 48 % de los sucesos registrados está relacionado con fallos en actuaciones humanas. De ellos, el 63 % fueron en operación a potencia y el 37 % restante lo fue en parada. Además, de los sucesos reportados mediante la escala internacional de sucesos nucleares (*International Nuclear Events Scale*, INES) en los últimos 10 años, la mayoría de los incidentes de nivel 2 o superiores podrían ser atribuidos a causas relacionadas con la actuación humana. De forma adicional, un estudio realizado sobre un amplio conjunto de análisis probabilistas de seguridad (*Probability Safety Assessment*, PSA) determina que entre el 15 y el 80 % de la frecuencia de daño al núcleo (*Core Damage Frecuency*, CDF) está relacionada con el fallo de alguna actuación manual por parte del operador, NEA (2004). El amplio margen de variación de esta estimación se relaciona con el grado de detalle y la atención que se haya dado al factor humano en el estudio, lo cual aumenta la importancia del resultado. Reason (1990), en un estudio de una docena de accidentes significativos ocurridos en los 15 años previos al trabajo, entre los cuales cabe destacar Three Miles Island (TMI), TChernobyl, Bhopal y el incendio del metro de Londres, concluye que al menos el 80 % de los fallos de los sistemas fueron provocados por humanos, especialmente por gestión inadecuada de la supervisión del mantenimiento. Además, determina que otros aspectos

tienen relevancia, siendo de destacar la inexactitud técnica o el entrenamiento incompleto en los procedimientos de operación. Este último aspecto es de gran importancia en multitud de sectores cuya optimización de la operación en situaciones anormales o de emergencia se fundamenta en un entorno fuertemente procedimentado. En este sentido, cabe resaltar que cuatro de las investigaciones de incidentes de importancia (*Major Incident Investigations*) llevadas a cabo por la NRC y cerca de 20 de las investigaciones adicionales realizadas desde TMI concluyeron que tuvieron como factor decisivo intolerables violaciones de los procedimientos.

La escasa interacción entre los desarrolladores de procedimientos y los operadores y supervisores de sala de control en planta, llevan a que estos últimos deban o bien reinterpretar los procedimientos, tomando acciones correctivas violando la regulación, o bien seguir los procedimientos existentes incrementando la posibilidad de un accidente, Ryan (1995). En un balance de 180 sucesos significativos realizados por Green (1991), se estimó en más de un 18 % los accidentes atribuibles de alguna manera a fallo de personal al seguir los procedimientos y un 43 % los motivados por procedimientos o documentación deficientes. Además, en un estudio posterior Green y Livingston (1992) estimaron que en un 69 % de los 1440 LERs registrados en 1990 (*Licensee Event Report*[1], LER), lo que hacen aproximadamente 700 casos, se identificaron problemas con los procedimientos como factor contribuyente al evento. Los errores más frecuentes detectados fueron, Figura 1.1:

- el uso del procedimiento equivocado en un 29.7 %,
- el uso del correcto pero en tiempo inadecuado en un 16.8 %,
- uso del procedimiento pasado el tiempo límite de aplicación en un 13.8 % y
- el fallo al ejecutar el procedimiento correctamente en un 11.2 %.

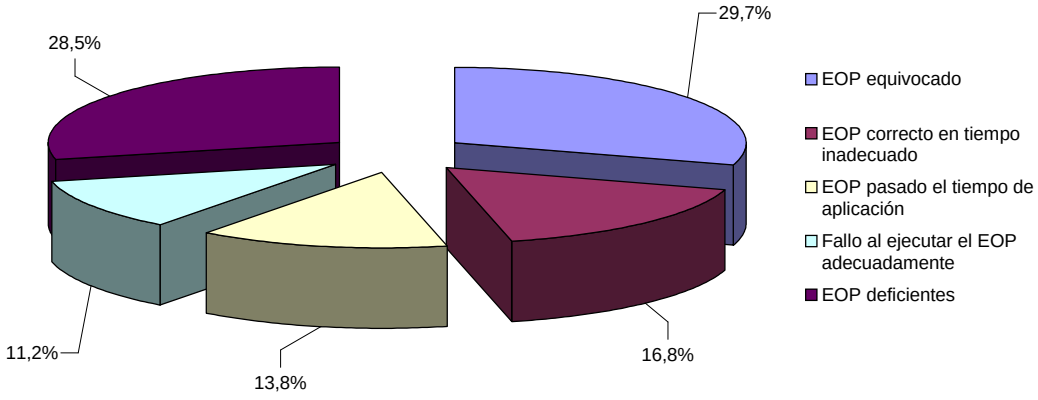


Figura 1.1: Causa de los errores humanos en el seguimiento de los EOP.

[1]Informes detallados que las compañías explotadoras deben remitir a la NRC dentro de los 60 días siguientes tras un suceso anormal en la planta tal como se considera en la 10 CFR 50.73.

En un estudio similar Marsden (1996), sobre los 180 sucesos significativos reportados en los EUA durante 1985, concluye que cerca del 48 % de los incidentes se pueden atribuir a fallos del operador y casi el 65 % se podría clasificar como relacionados con procedimientos deficientes.

En estudios más recientes, Gertman et al. (2001) realizó una clasificación por categorías de los errores registrados en el uso de los procedimientos, según la cual el 38 % de los sucesos se debe a errores en el diseño o la aplicación de los procedimientos. En este mismo estudio, se identifica como segundo problema en importancia durante la operación el fallo o la baja efectividad en el diagnóstico, debido sobre todo a falta de comprensión técnica de la situación, procedimientos deficientes u otros aspectos relacionados con los procedimientos. En otro informe, Gertman et al. (2002), el diseño y desarrollo de los procedimientos es una de las cuatro causas relacionadas con el 60 % de los eventos estudiados. Park y Jung (2003a) estimaron que de todos los incidentes relacionados con el seguimiento de los procedimientos, el 30 % implican la elección equivocada del procedimiento adecuado, teniendo como causa un error por parte del operador en la fase de diagnóstico del suceso. Es importante considerar que, tras el accidente de TMI, se estableció que los errores humanos debidos a fallos cognitivos asociados al proceso de diagnosis son los de mayor importancia por presentar mayor gravedad en las consecuencias.

Por todo ello se puede concluir que, independientemente del rango tecnológico en consideración, el error humano suele estar implicado en el 70 % al 80 % de los transitorios operacionales. Además, como ya se ha comentado, este aumento del impacto de la actuación humana tiene su origen en al aumento de la fiabilidad de los sistemas y componentes, la complejidad de los sistemas en aumento y el papel del operador en el lazo de control. Este último aspecto está íntimamente condicionado por el aumento de la automatización en los sistemas de producción industrial, aspecto que por su relevancia se tratará, aunque de forma sucinta al no ser el objetivo de esta tesis, en la Sección 1.1.3.4.

En lo que respecta los accidentes registrados, se puede decir que el accidente de Three Miles Island, TMI, (EUA, marzo de 1979) mostró que los factores humanos no habían sido considerados adecuadamente en los análisis de seguridad. Este hecho llevó a numerosas mejoras de diseño y prácticas operacionales en las centrales nucleares. El accidente estimuló el desarrollo de sistemas de instrumentación y de sistemas de control avanzados, alcanzándose una alto grado de innovación en los sistemas de control e información y ayuda computerizados tanto en operación normal como de accidente. La consideración de factores humanos en la etapa de diseño se hizo de forma que garantizase que la planta tolera fallos del operador, consiguiéndose mediante el uso de controles automáticos y de sistemas de protección mejorados. En la implementación actual, la intervención del operador solo se requiere en caso de que haya suficiente tiempo para realizar el diagnóstico del suceso y de diseñar un conjunto de acciones correctivas, garantizando su fiabilidad. En los reactores avanzados, se hace hincapié en las características de seguridad intrínsecas y pasivas, que no requieren actuación del operador o suministro de energía. Debido a que el papel del operador en este tipo de tecnología sigue siendo relevante, sobre todo en situaciones donde las condiciones de la planta pueden estar fuera de operación normal, se estima necesario diseñar un conjunto de procedimientos para la operación segura y proteger la instalación de posibles violaciones de los márgenes de seguridad adoptados en el diseño, tal como se considera en las tecnologías actuales.

A parte de los aspectos puramente técnicos, el accidente de TMI ilustró claramente como la interacción de éstos con los factores humanos y organizativos puede ayudar a la progresión de los sucesos. Tras el incidente, grandes esfuerzos de investigación y desarrollo se han enfocado al estudio de los factores humanos en la gestión de accidentes. La gestión de accidentes incluye las acciones que debe realizar la plantilla de operación durante un accidente más allá de la envuelta base de diseño, con el objetivo de mantener las funciones básicas de seguridad de potencia generada en el reactor, mantenimiento del combustible refrigerado y asegurar el confinamiento del material radiactivo. Se distinguen dos fases en la gestión de emergencias: la fase preventiva, en la cual las actuaciones del operador están centradas en evitar el daño al núcleo y mantener la integridad de la instalación, y la fase de mitigación, en la cual, una vez producido el daño al núcleo, las actuaciones del operador están orientadas a reducir la cantidad de radioisótopos que se pudiesen liberar. La gestión de accidentes se lleva a cabo mediante el uso de los procedimientos de operación de emergencia (*Emergency Operational Procedures*, EOP) y las guías de gestión de accidentes severo (*Severe Accident Management Guides,* SAMG), y su mejora fue otra de las actividades desempeñadas tras el accidente.

De forma similar al accidente de TMI, el accidente de la unidad 4 de la central nuclear de TChernobyl (Ucrania, abril de 1986) tuvo gran repercusión en el sector nuclear. Sin embargo, debido a las características de diseño del reactor y al gran conjunto de deficiencias detectado durante la gestión del accidente, ambos aspectos muy diferentes en la industrial nuclear de occidente, el impacto en las tecnologías occidentales fue prácticamente nulo. El efecto fue el contrario, produciéndose un aumento de la preocupación de los países occidentales por las condiciones de seguridad de las instalaciones soviéticas, y el nacimiento de una fuerza de presión en estos países con la intención de exportar el enfoque de ingeniería aplicado en el diseño y durante la operación de este tipo de instalaciones a los países herederos de esta tecnología tras la extinción de la Unión de Repúblicas Socialistas Soviéticas, URSS.

Cabe destacar que un conjunto considerable de incidentes operacionales, en cuyo desarrollo la actuación humana podría haber dado lugar a accidentes de consecuencias impredecibles, pasa desapercibido a la opinión pública y disimulado como parte de las estadísticas globales al no tener impacto económico o humano. Como ejemplo ilustrativo de lo expuesto, se puede citar el incidente ocurrido en septiembre de 1988 en la central nuclear de Stade, en la Alemania occidental. En dicho incidente, un fallo eléctrico causó el cierre de una de las cuatro válvulas de aislamiento de las líneas de vapor principal (*Main Steam Isolation Valves*, MSIV), cerrándose las otras tres posteriormente. En un incidente de este tipo, el sistema automático de protección del reactor debería haber disparado el reactor y la turbina. En contra de los procedimientos, los operadores anularon dicha actuación y abrieron las MSIV en un intento de continuar operando el reactor a potencia. Éstas volvieron a cerrar rápidamente por segunda vez y el sistema disparó. El cierre y la apertura rápida de las válvulas provocó una onda de presión que hizo oscilar las líneas de vapor unos 20 cm entorno a su posición de reposo. Este desplazamiento es más del doble del límite de diseño y, según los investigadores, las acciones llevadas por los operadores estuvieron a punto de provocar un fallo en las líneas difícilmente cuantificable, Marsden y Green (1996). Es evidente que no se puede diseñar con la intención de erradicar cierto tipo de comportamientos humanos, pero dentro de la ingeniería se están estableciendo un conjunto de disciplinas orientadas a la mitigación y prevención de este tipo conductas. En este sentido,

tenemos los criterios de diseño de sistemas de automatización centrados en el hombre y los sistemas tolerantes a fallos. En la sección 1.1.3, dedicada a los estudios de ingeniería, se trata de forma somera este aspecto sin ánimo de profundizar, ya que no es el objetivo de este trabajo.

Como se argumentará a lo largo de este capítulo, la presencia del operador como parte del sistema, considerando el control y la gestión del mismo, no es cuestionable, siendo el objetivo de la ingeniería obtener el mayor grado de fiabilidad posible de las actuaciones humanas consideradas como posibles. Uno de los aspectos claves de este objetivo es realizar una evaluación de los medios de que dispone el operador para gestionar las emergencias, es decir, los procedimientos de operación. En este sentido, este capítulo pretende desarrollar y respaldar esta idea, justificando la necesidad de la realización del trabajo que se ha llevado a cabo.

1.1 El error humano. Estudio, definición y taxonomía

A lo largo de la introducción del capítulo se ha hecho un uso extensivo del término **error humano** pero ¿qué se entiende por error humano? ¿que alcance tiene la justificación de un hecho a partir de esa definición? Dentro del enfoque fenomenológico, ¿es causa o efecto? Muchos expertos se manifiestan ante estas tres preguntas de forma dispar, pudiéndose determinar dos motivos como origen de la variedad de criterios.

El primero, y más importante, el relacionado con la complejidad del fenómeno a estudio, que no es otro sino el comportamiento humano en una de sus materializaciones y, en segundo lugar, la variedad de disciplinas en que se considera esta problemática. A estos dos aspectos hay que añadir un tercero, la naturaleza de su tratamiento, fuertemente condicionado por el objeto del estudio que se realice. Quedando lejos de estar unificado, la naturaleza de su tratamiento pasa de la definición y comprensión de la problemática, objetivos propios de los estudios de filosofía, hasta su estructuración, simulación y aplicación práctica directa al diseño y estudio de sistemas de control, que se realiza en ingeniería. Esta disparidad hace que el objeto de estudio se convierta no solo en el establecimiento de un punto de partida, como en filosofía, sino también en sí mismo como una justificación de otros objetivos completamente ajenos a la naturaleza del problema, tratamiento propio de la ingeniería. Evidentemente la disparidad de criterios roza el antagonismo, lo que lleva incluso a veces a la inconsistencia.

El comportamiento humano es una cuestión abierta en todas las ramas del conocimiento, desde la filosofía, la psicología y la ingeniería. En ninguna de ellas se ha alcanzado la madurez suficiente como para sentar una base sobre la que construir un conocimiento teórico estructurado y esto lleva a que cualquier intento de unificación de las diferentes líneas de trabajo fracase. Muchos estudios concluyen tras un análisis exhaustivo que es un campo de conocimiento inmaduro y que deberá evolucionar algunos años para concretar sus bases. En los últimos diez años los expertos han comenzado ha encontrar las raíces de su trabajo en la denominada ciencia cognitiva y, a partir de ella, se está empezando a definir los objetivos de una rama de la técnica, la ingeniería de los factores humanos, que deben cubrir una necesidad acuciante: el estudio y la evaluación del factor humano en la ingeniería. La importancia de esta necesidad se ha puesto de manifiesto en la introducción del capítulo.

Analizando la situación actual de las diferentes áreas de conocimiento implicadas, podemos distinguir entre el estudio científico del error, principalmente preocupado por estudiar los aspectos psicológicos y sociales del error, y la aproximación de la ingeniería a las acciones erróneas, trabajo relacionado con el desarrollo de técnicas que permitan apoyar las actividades de diseño y evaluación de sistemas con participación humana.

En este trabajo nos centraremos en la aplicación técnica de los trabajos científicos, y nuestro objetivo principal será presentar las principales líneas de trabajo en las distintas ramas del conocimiento citadas, exponer las diferentes metodologías técnicas desarrolladas para determinar la importancia de los factores humanos en la ingeniería y como beben éstas de las definiciones conceptuales establecidas en las primeras. Posteriormente, y tras haber revisado las diferentes implicaciones de los estudios previos, se procederá a establecer una definición del error humano y una taxonomía del mismo.

1.1.1 El estudio del error humano en la filosofía

En la **filosofía**, el error humano adquiere una dimensión especial al considerársele claramente como prueba de los límites de la capacidad del sujeto dentro de la teoría de la cognición, donde representa un objetivo dentro de las líneas de investigación.

Aristóteles describe el error humano como una subordinación y concatenación falsa de los datos aportados por nuestros sentidos mediante el proceso del pensamiento. Descartes, por contra, lo define como una expresión de la intención, entendida como la capacidad de asumir por ciertas unas ideas y rechazar otras. Así, el error nace de la intención y no propiamente de las ideas. Hume, sin embargo, ve el error como un juego de ideas e impresiones, produciéndose todos los errores como resultado de la aplicación de ideas falsas a impresiones correctas o a la interconexión de impresiones falsas con ideas correctas, Störig (1995). Kant observa, considerando el error humano en la forma de los prejuicios, que el origen de los prejuicios se encuentra en la novedad, mala interpretación, imitación, hábito, inclinación y egoísmo, Keller (1988).

Sträter (2000), tras realizar una revisión histórica considerando las similitudes y diferencias de las acepciones filosóficas del término, extrajo como conclusiones que los aspectos importantes para el estudio del error humano son:

- El procedimiento de procesado de información por el hombre; reflejado en los conceptos de Concatenación de Aristóteles y Hume, la Actividad de la Voluntad en Descartes y la Mala interpretación y el Hábito en Kant.
- El objetivo escogido por la acción del hombre; la Voluntad en Descartes, la aplicación de las falsas ideas en Hume y la inclinación por los instintos y el egoísmo en Kant.
- La información disponible vía los sentidos o los procesos de pensamiento; como los datos proporcionados por los sentidos en el caso de Aristóteles, la Idea en el caso de Descartes, las Impresiones en Hume o la Imitación y la Novedad en Kant.

Dos de los tres puntos considerados, el objetivo escogido y la información disponible, están relacionados con la forma en que se realiza el procesado de la información, lo que confiere a este aspecto una papel central en la materialización del error humano. Estos dos mecanismos se pueden ejecutar de forma consciente o inconsciente. El tratamiento de la información de forma inconsciente ocurre automáticamente y activa modos habituales de comportamiento. Sin embargo, el tratamiento de la información de forma consciente presupone siempre que un proceso habitual presenta una alteración, por lo que los aspectos desapercibidos de una situación llegan a ser conscientes solamente una vez se produce la alteración en el proceso. Una vez se produce un tratamiento consciente de la información, la tentativa entonces consiste en integrar los contrastes en un mayor nivel de abstracción vía procesos de pensamiento, intentando identificar el nuevo estado con alguno de los ya conocidos o habituales. Este modo compensatorio del comportamiento se describe de forma completa en la teoría cognitiva de la disonancia de Festinger (1957).

Resumiendo, se puede decir que el error humano viene del hábito o modos de acción aprendidos y, por otra parte, presupone cierto el objetivo escogido o la información subyacente. De esto podemos además concluir que cualquier acción del ser humano conlleva un error potencial, porque el mismo individuo nunca puede tener certeza sobre la corrección de una intención generada a partir de sus mecanismos de razonamiento. Además, tras lo expuesto, el error humano debe ser visto como un hecho positivo desde el punto de vista filosófico, ya que solamente en virtud de la duda sobre la corrección de declaraciones y de actividades de pensamiento se puede progresar en la mejora de la calidad del tratamiento de la información disponible.

Este aspecto es resaltado también por Sträter (2000), quien extrae de este positivismo dos características que exigen la existencia de supervisión humana en los sistemas técnicos y abandonar la idea de que su función se puede sustituir mediante esfuerzos de automatización:

- Un progreso cognitivo constante por medio de la mejora independiente y la capacidad de adaptación humana a nuevas situaciones.
- Capacidad de recapacitar y profundizar en la corrección de una medida en ciertas situaciones extremas, donde no son tan eficaces los sistemas automáticos.

Estas consideraciones serán referidas de nuevo en la Sección 1.1.3.4, donde se trata en detalle el papel del individuo en los sistemas altamente automatizados.

1.1.2 El estudio del error humano en la psicología

En lo que respecta a la **psicología**, el tratamiento ha evolucionado sustancialmente. El primer caso relevante del estudio del error lo tenemos en Freud (1940), quien estudiaba el error extensivamente, particularmente los lapsus de memoria y los deslices de la lengua, pero poco interesado en los mecanismos, causas y efectos de las acciones erróneas, y más interesado en lo que revelan del individuo que las comete. De hecho, Reason (1990) sugiere que durante un periodo amplio de la historia de la psicología, la misma existencia del error, o al menos la legitimidad del estudio del error como una desviación de la acción desde la intención, era discutible.

Así, las fuerzas en disputa en psicología eran, por un lado los psicoanalistas seguidores de la tradición freudiana, que sostenían que las acciones son producto siempre de la expresión de alguna intención del subconsciente, y los conductistas, que parten de la intención como objetivo de su estudio.

Actualmente, las diferentes vías de tratamiento que presenta la psicología en el estudio de las acciones erróneas se pueden clasificar en los modelos conductistas y los modelos cognitivos, careciendo de interés para este trabajo cualquier enfoque basado en el psicoanálisis.

1.1.2.1 Modelos conductistas

Estas aproximaciones se construyen sobre paradigmas que usan la observación para hacer predicciones del comportamiento humano. Las típicas aproximaciones conductistas son la neuropsicología, la percepción psicológica, así como los paradigmas relacionados con la psicología de la acción o la actividad psicológica, como por ejemplo, los modelos de reacciones a los estímulos. Las aplicaciones de modelos conductistas son muy limitadas, pudiéndose encontrar algunos usos prácticos de los modelos de la psicología de la acción.

1.1.2.2 Modelos cognitivos

A finales de los años 50 la psicología sufrió una de sus revoluciones más significativas. Noan Chomsky, en un artículo publicado en el momento del surgimiento de la aproximación cognitiva al comportamiento humano, Chomsky (1957), escribió:

> *«Definir la psicología como la ciencia del comportamiento (conductismo) es como definir la física como la ciencia de la lectura del metro.»*

A posteriori, esta aproximación cognitiva al comportamiento humano se vino a denominar como la ciencia cognitiva. Esta nueva concepción del comportamiento humano construye sus paradigmas basándose en una idea o modelo acerca del procesado humano de la información. Típicamente, las aproximaciones cognitivas se suelen denominar como psicología de la memoria, teoría de las decisiones así como psicología del pensamiento. Los resultados de las investigaciones conducidas en esta corriente representan hoy en día asunciones centrales en la investigación del error. Entre ellas se pueden destacar:

- Los trabajos de Miller (1956), sobre las limitaciones del ser humano al procesar información fueron los de mayor impacto. A través de modelos íntimamente relacionados con la teoría de la información, estableció los mecanismos de procesado de información en humanos y definió modelos de decisión unidimensionales o multidimensionales basados en la naturaleza de la información considerada en el razonamiento. Una de sus conclusiones con mayor resonancia es que todo razonamiento unidimensional se basa como máximo en

siete categorías[2], mientras que los multidimensionales pueden llegar a contemplar hasta nueve. La conclusión del trabajo es que aumentando la dimensión del razonamiento hacemos mejor juicio y tenemos mejor percepción del entorno, pero empeoramos la precisión en alguna categoría en particular. Además, resalta la importancia de la recodificación, como un proceso de reestructuración de la información y de optimización de la memoria basado, principalmente, en procesos de reconocimiento de patrones. En resumen, establece un límite para el razonamiento unidimensional y la memoria inmediata, que se puede mejorar realizando razonamientos multidimensionales y somentiendo a la información a procesos de recodificación.

- El modelo de memoria de trabajo de Baddeley y Hitch (1974) y Baddeley (2001 1990), posteriormente denominado como de memoria a corto plazo. Es un modelo ampliamente citado y utilizado como referencia, tanto para comprender el funcionamiento de la memoria operacional como para comprender los fallos asociados a la misma. Según este modelo, existen los siguientes componentes:

  – Un sistema maestro de procesamiento: el sistema ejecutivo central que controla la atención, coordina los subsistemas y registra las rutinas automáticas,

  – y varios subsistemas o bucles: el bucle fonológico o verbal, que se encarga de estructurar la información auditiva de forma secuencial con cierta capacidad de memoria, el bucle articulatorio, que se encarga del recuento y almacenaje de la información del bucle fonológico, y el bucle de esquemas viso-espaciales que puede ser dividido en dos, uno para la información estrictamente visual (el qué) y otro para la información espacial (el donde).

  Se comprende que esta memoria operacional desempeña un papel central y extraordinariamente importante en casi toda la actividad cognitiva consciente. Si la memoria operacional se encuentra limitada de modo severo, es lógico que el proceso de comprensión se desmorone, sobre todo si los mensajes son largos, considerando el modelo de limitaciones en el manejo de información de Miller (1956). Este modelo tiene amplias aplicaciones en las herramientas de simulación del comportamiento humano, y un buen ejemplo de ello es la herramienta MIDAS desarrolla por la NASA y cuyas aplicaciones van desde la de la industrial aeroespacial hasta la gestión del tráfico aéreo (*Air Traffic Management*, ATM)[3].

- El modelo de máquina falible de Norman (1990), que establece que los dos tipos de procesos que gobiernan la memoria a largo plazo son la identificación por similitud y la apuesta por sucesos más frecuentes. Tiene amplias aplicaciones en las herramientas de simulación del comportamiento humano. Un ejemplo de ello es la herramienta COSIMO[4], basada en la adaptación de esta aproximación por Reason (1990).

[2]Recientemente se han publicado correcciones al modelo de Miller de tratamiento de información que parecen limitar aún más las capacidades de tratamiento de información del ser humano, Cowan (2001). En este sentido, el *número mágico* pasa de ser siete a cuatro.

[3]MIDAS es una herramienta basada en un modelo predictivo del comportamiento humano para su aplicación al diseño de interfases hombre-máquina.

[4]COSIMO se emplea como extensión a la herramienta DYLAM, Cacciabue et al. (1992).

- El modelo del efecto de la estructura de la tarea y limitaciones de la memoria de trabajo de Byrne y Bovair (1997), que tiene como objetivo determinar el efecto que tienen ambos aspectos en la ejecución del trabajo. El ejemplo más claro es el típico error de omisión de la última acción considerada dentro de una tarea. Este comportamiento se da, por ejemplo, en el realizado manual de copias en una fotocopiadora. Una vez recogida la copia, objetivo de la tarea, se omite una de las acciones secundarias, recoger el original[5].

1.1.3 El estudio del error humano en la ingeniería

Dentro de la ingeniería, las definiciones del error humano son diversas, pudiéndose destacar:

- Rigby (1970), establece que una actuación humana debe ser considerada como un error si, como resultado de ella, no se alcanzan los requerimientos establecidos por el sistema o no se hace de la forma adecuada.
- Swain y Guttman (1983), considera el término error humano como aquel que cubre todas las actividades u omisiones de una persona causando algo no deseable o que propician que algo no deseable ocurra. Esta definición fue ampliada posteriormente considerando que estaba realizada en el contexto del sistema, e incluso pensando en los principales factores que pueden contribuir al error, por ejemplo, la ausencia de un diseño ergonómico, procedimientos, entrenamiento o la combinación de todos ellos. Establece además, que no se debe asociar a este término ninguna intención de culpabilidad.
- Norman (1986) estable el fallo en la interpretación o en el entendimiento por parte del hombre de la información que recibe del sistema.
- Reason (1990), define el error como un término genérico para referirse a todas las ocasiones en las que un conjunto planificado de actividades mentales y físicas fallan en alcanzar su objetivo establecido, considerando que esos fallos no se pueden atribuir a la intervención de otro agente posible.
- Hollnagel (1998), establece una nueva idea de error humano, atribuyendo el protagonismo al contexto en vez de al sujeto. El error humano pasa a ser la acción errónea, que en un contexto específico puede llevar a un resultado no deseado. Este autor nunca ha presentado una definición a la usanza del error en lo relativo a los factores humanos, sino que se ha limitado a dar tres posibles acepciones del mismo, cada una de ellas orientada a satisfacer las necesidades de los diferentes estudios del campo:

    1. Una acción que no se corresponde con una forma o criterio de actuación estándar, en el sentido que una acción puede ser medida y comparada.
    2. Una acción que desencadena un suceso u otra acción que conlleva un resultado indeseado. Puede identificarse como un mecanismo erróneo en la forma de procesar la información del hombre, permitiendo la identificación de los mecanismos que llevan al error.

[5]Este ejemplo es un error típico de omisión de acción (*Error of omission*, EoO).

3. Las acciones erróneas, para poder definirse como tales, deben presentar un grado de volición tal que el agente tiene la oportunidad de actuar de una manera que no sea considerada errónea, independientemente del resultado. Así, si algo no es evitable por una cierta acción, no es ni razonable ni aceptable hablar de error para definir esa acción. Los factores que concurren fuera del control del individuo se definen mejor, por lo tanto, como accidentes.

Una característica común a todas ellas, exceptuando la aportada por Hollnagel, es que establecen la definición del error humano en términos de los requerimientos derivados del sistema, es decir, el sistema determina cuando el individuo se comporta erróneamente. Esta orientación sesgada es criticada fuertemente por Hollnagel. Sin embargo, hay que comentar que las definiciones aportadas por Swain, Norman y Reason y sus taxonomías son empleadas de forma usual en las diferentes técnicas de HRA aplicadas actualmente en los estudios de seguridad y el análisis de accidentes, y la definición aportada por Norman es la base de las herramientas de evaluación de interacción de hombre-máquina (*Human Computer Interaction*, HCI)[6].

La aproximación técnica al estudio del error humano se ha realizado, principalmente, de forma que solo se pretenden categorizar y clasificar las formas manifiestas y no las causas internas de las acciones erróneas. Son los que se han venido a denominar modelos de brocha gorda o *Broad brush models*. Son modelos detallados en el sentido que explican algunos de los mecanismos que subyacen en el fenómeno cognitivo, orientados al comportamiento erróneo de forma particular, pudiéndose desarrollar implementaciones computacionales basadas en los mismos. Se distinguen dos corrientes principales, la fenomenológica y la causal, con cierto paralelismo con las corrientes de estudios psicológicos tratados anteriormente, y una adicional que surgió como necesidad para los estudios de factores humanos en el diseño de interfases hombre-máquina y de diseño de sistemas automáticos con interacción humana, denominada de estructura de acciones[7].

Cabe comentar que algunas de estas taxonomías del error humano, empleadas en conjunto con las aproximaciones fenomenológicas, son las más empleadas en las metodologías para cuantificar el error humano en las centrales nucleares. Sin embargo, ciertos estudios tienden a criticar la falta del tratamiento de los aspectos cognitivos del error humano, Karin (2002).

Finalmente, y antes de dar paso a la descripción de los diferentes tipos de estudios, se ha considerado de interés destacar un conjunto de ideas extraídas del trabajo de Woods et al. (1994):

- Los errores son heterogéneos, es decir, ocurren en diversidad de entornos de dispar naturaleza. Por ello, el determinar una de las categorías dentro de las posibles no sirve de ayuda, además de carecer de rigor. Se define así la necesidad de desarrollar una metodología global menos ambiciosa y más orientada a resolver el conjunto de problemas existentes, Hollnagel (1994).

[6]Las HCI son técnicas que sirven como tareas de apoyo al diseño en ingeniería y últimamente se presenta como un elemento clave para el desarrollo de metodologías prospectivas y retrospectivas consistentes.

[7]Esta clasificación se incluye por completitud, careciendo de interés para el trabajo desarrollado.

- Las acciones y los juicios técnicos erróneos deben considerarse como el punto de partida y no la conclusión a la hora de buscar respuestas.

- Las acciones o juicios erróneos son el síntoma y no la causa, son el síntoma de otros procesos cognitivos, sociales, organizativos o técnicos que se manifiestan en las acciones erróneas. Este aspecto, relacionado con las preguntas ¿dónde empieza y termina la justificación de un hecho a partir de esa definición? y, dentro del enfoque fenomenológico, ¿es causa o efecto? fueron ya expuestas por Rasmussen (1987), especificando que el factor humano siempre será causa, pues en todo sistema la implicación humana afecta a todas sus dimensiones. Por ello, Rassmunsen observa que la búsqueda de causas debe finalizar cuando se pueda definir las acciones correctivas necesarias para que el efecto no se vuelva a repetir, es decir, la regla de corte debe ser sencillamente aquella que proporcione una causa para la cual se tenga una solución.

- En el estudio retrospectivo de accidentes hay una pérdida de relación entre los procesos y los resultados, perdiéndose a su vez la relación causa-efecto entre un accidente y el proceso que ha propiciado el mismo.

- El conocimiento del resultado provoca un juicio sesgado del proceso, llevando a la definición de acciones erróneas, heroicas o cualquier otra categoría intermedia en función de los resultados obtenidos más que por las circunstancias en que fueron realizadas. En este sentido, y tal como se ha comentado en los anteriores puntos respecto a las observaciones de Rassmunsen en cuanto a la búsqueda de causas, las estadísticas sobre la importancia del factor humano no pierden su valor cualitativo, aunque se podría poner en duda que reflejasen cuantitativamente la evolución del impacto del factor humano en la industria en los últimos años, debido a la tendencia actual de adjudicar al hombre toda la responsabilidad de los sucesos.

- Los incidentes evolucionan como la conjunción de varios fallos o factores, siendo inútil cualquier intento de determinar la causa de un determinado suceso. Otros autores enfatizan esta idea en sus trabajos, Reason (1990) y Rasmussen (1987), existiendo estudios sobre este hecho que ratifican que más del 50 % de los incidentes estudiados presentaban más de cinco errores latentes, Gertman et al. (2001).

- Algunos de los factores que contribuyen a un accidente se encuentran latentes en el sistema, tal como se ha comentado en el punto anterior, pudiéndose incluso definir los accidentes como latentes, manifestándose cuando un conjunto particular de circunstancias lo propician. Esta aproximación, tratada en detalle por Reason (1990), se corresponde con la idea de que las actuaciones humanas pueden abrir camino hacia el accidente. Bajo ciertas condiciones, precursores psicológicos de la acción errónea en el sistema cognitivo humano se manifiestan de forma que dan lugar a actuaciones no seguras. Para que estos actos tengan consecuencias se tienen que dar ciertas condiciones en el entorno, capas de defensa en profundidad deben fallar al prevenir que estas actuaciones no seguras den lugar a una situación de accidente. Siguiendo la trayectoria de los posibles accidentes, se pueden presuponer actuaciones no seguras y diseñar medios contra ellas. Una de las

líneas más importantes del trabajo de investigación que intenta proporcionar medios para determinar la suficiencia de tales mecanismos defensivos se conoce como el análisis de fiabilidad humana (*Human Reliability Analysis*, HRA), que se tratará en detalle en la Sección 1.2.2.

- Los mismos factores gobiernan la expresión de la maestría y del error, por ello se requiere no solo un estudio de los mecanismos del fallo cognitivo y de ejecución, sino un estudio global de los mecanismos que rigen el comportamiento humano. Para ello es necesario que los métodos de ingeniería adquieran conocimiento de las ciencias cognitivas, tal como está ocurriendo en el desarrollo de las HRA de segunda generación.

- Las acciones y juicios erróneos tienen una fuerte dependencia del contexto. Este aspecto del comportamiento humano es resaltado insistentemente en los trabajos de Hollnagel (2005b).

- El diseño orientado a la tolerancia, detección y la recuperación del error es aún más importante que cualquier actuación preventiva del mismo. Idea extraída de Rasmussen (1986), y compartida por Woods, entre otros.

1.1.3.1 Clasificación fenomenológica

Las metodologías dentro de esta clasificación se caracterizan por atender a la observación de efectos, y no a causas, entendidas como las funciones cognitivas, o los errores definidos a partir del mecanismo mental que los propicia. Las aproximaciones al error humano desde el punto de vista fenomenológico, suelen ir acompañadas en la mayoría de los estudios por una estructura causal, que se desarrollan en la clasificación causal o conceptual. Aquí, se hace un resumen de los diferentes modos de error definidos por autores como Swain, Norman, Reason y Hollnagel, entre otros.

Algunas de las primeras clasificaciones fenomenológicas son las debidas a Norman (1981) y Swain y Guttman (1983), según las cuales, los errores se pueden clasificar como:

- Errores de omisión, como los errores que se manifiestan por la ausencia de actividad cuando es requerida.

- Errores de comisión, los errores provocados por acciones no requeridas, pudiéndose distinguir:

  – Error de secuencia: alteración del orden de las acciones prescritas o planeadas.

  – Error de sustitución: ejecución de una acción en lugar de otra.

  – Error de tiempo inadecuado de ejecución.

  – Error cuantitativo.

  – Error de selección: selección del control erróneo, elección de procedimientos de forma incorrecta.

Posteriormente, Reason (1990) añadió los denomiandos errores latentes y activos[8], definidos como:

- latentes, aquellos que se materializan a raíz de ciertas circunstancias siendo una característica existente en el sistema de forma previa. Surgen de decisiones realizadas por diseñadores, constructores, redactores de procedimientos, etc. Pueden ser decisiones erróneas pero no tienen porqué serlo. En comparación con los errores activos, que son difíciles de diagnosticar, los errores latentes pueden ser identificados y corregidos antes de que se materialicen.

- activos, como los errores provocados en el sistema por una causa ajena al mismo, no queriendo decir que estos errores siempre tengan su origen en el sujeto que los produce, pues como se puede interpretar, todos estos actos tienen una historia causal que se extiende atrás en el tiempo y a niveles superiores del sistema en que se integra el sujeto.

Una de las taxonomía fenomenológicas del error más completas es la realizada por Hollnagel (1991). Debido al interés que presenta en el presente trabajo se discute en detalle en la Sección 1.1.4. Sin embargo, cabe comentar que tuvo serios detractores al carecer de estructura causal en su planteamiento inicial. Por ejemplo, Reason (1990) comenta que la taxonomía propuesta por Hollnagel es puramente fenomenológica, y tiene como único objetivo diseñar sistemas que puedan implementar acciones correctivas tras el error. No hay intención de estudiar la causa, no hay intención de corrección y mejora. Esta idea ya fue expuesta por Rasmussen (1987), quien observó que si el análisis se centra solo en la consideración del error humano en términos de sus efectos, la identificación del mismo queda prohibitivamente obstaculizada por una explosión combinatoria. Por ello, la taxonomía de Hollnagel carece de aplicación potencial en los estudios retrospectivos.

1.1.3.2 Clasificación causal o conceptual

La base de estas aproximaciones radica en la determinación del mecanismo cognitivo involucrado en la producción del error. Se pueden distinguir cuatro enfoques como los más importantes: la teoría de la acción y el error de Norman, la aproximación de Rouse, la relación de los niveles cognitivos y el error humano de Rasmussen, la aproximación de cognición primitiva, sesgos cognitivos y error humano de Reason y el modelo simple de cognición de Hollnagel.

La teoría de la acción y el error

Basado en la psicología de la memoria, Norman desarrolló el denominado modelo de los siete estadios de acción o modelo de las fases de ejecución de tareas, Norman (1986 1981 1988)[9].

[8] Es común definirlos también como condiciones de errores latentes y activos.

[9] Los orígenes de este modelo también se adjudican en algunas referencias a Neisser.

En este modelo se definen siete estadios cíclicos de todo proceso cognitivo, Figura 1.2, estableciendo los tipos de error en cada estadio empleando la teoría de esquemas para describir estos errores. Cabe comentar que dentro de esta teoría, un esquema es una estructura de conocimiento preconcevida, con ciertos atributos que se pueden asociar con magnitudes. Estos bloques estandarizados de conocimiento se emplean para almacenar cursos o acciones. En los estados de acción se distinguiéndose dos regiones, una de evaluación y otra de ejecución, marcando el tamaño de estas regiones la distancia entre el comportamiento aparente del mundo y los deseos y objetivos del individuo, aumentando por tanto la posibilidad de incomprensión, fallo en la comunicación y error. Partiendo de esta base, establece dos tipos de errores, los deslices (*slips*) y los errores (*mistakes*). Los deslices conciernen a la ejecución de una acción que no es la que uno se proponía realizar. Pueden suceder cuando un esquema de acción sufre un defecto de activación o un defecto en su desarrollo. Así, una activación defectuosa de un esquema puede corresponder a una activación no intencional, un fallo de captación de atención, una activación asociativa o una pérdida o falta de activación. Los deslices derivados de un defecto en el desarrollo de los esquemas de acción activados, se darán por una inversión de los componentes del esquema, una combinación de los componentes de dos esquemas, un desencadenamiento prematuro o un defecto en el desencadenamiento. Los errores corresponden a fallos en la formación de la intención y/o en la determinación de objetivos, producto de una mala comprensión, dando lugar a un planteamiento inapropiado. Son acciones realizadas como se proponían, cuyos efectos inmediatos o en una etapa posterior no está en concordancia con el logro del objetivo que pretendía la persona.

Este modelo ha sido empleado como base teórica para la realización de herramientas de apoyo en la ingeniería. Un ejemplo de ello es la técnica de evaluación del error humano (*Technique for Human Error Assessment*, THEA)[10].

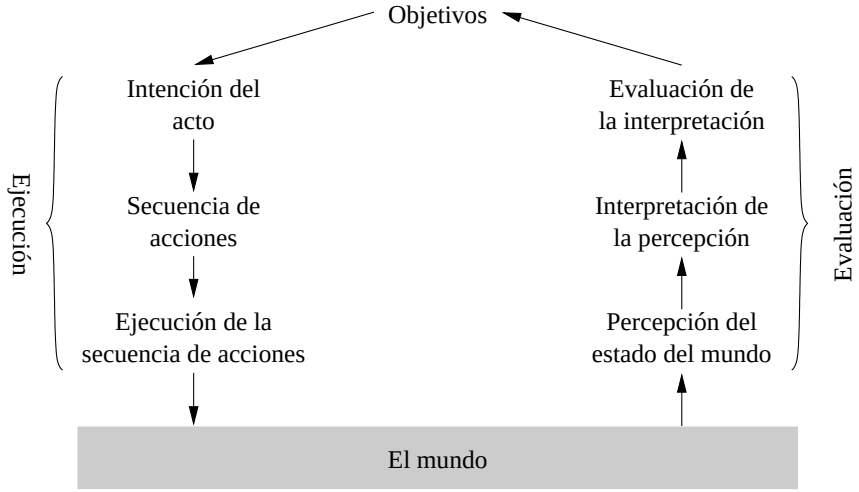


Figura 1.2: Modelo de los siete estadios de una acción de Norman (1988).

[10]THEA es una técnica basada en una ampliación el modelo de Norman desarrollada para ayudar a los diseñadores de sistemas interactivos a anticipar errores humanos antes de que los diseños se hagan operacionales.

El tratamiento de Rouse basado en la teoría de la toma de decisiones

Define tres periodos para la realización de toma de decisiones, Figura 1.3, Rouse y Rouse (1983):

- la formación de un supuesto de lo que está pasando,
- la selección del estado deseado como objetivo y
- la elección de los procedimientos por los cuales se va a alcanzar el objetivo.

Este modelo asume que durante la operación normal el operador cicla a través de los estadios relacionados con la observación del estado del sistema, y la elección y ejecución de los procedimientos. Cuando una variable del sistema se va fuera del rango normal o cuando los avisos o alarmas se activan, el operador establece que la situación es anormal e inicia el proceso de búsqueda de una solución para el problema. Si la desviación observada es frecuente, los patrones son reconocidos, y la solución es inmediata y obvia, por lo que el operador ejecuta de forma inmediata el procedimiento correctivo. Si, por contra, el patrón de las entradas del sistema es poco familiar, se inicia un proceso de resolución del problema basado en la búsqueda de estrategias. La generación de la hipótesis y la prueba en el modelo de Rouse dan lugar a una tentativa en la identificación de la fuente del problema. Durante la realización del proceso de resolución del problema puede darse un conflicto de objetivos ante el cual el operador debe discriminar, estableciendo el objetivo que considere como dominante desde su juicio de la situación. Las categorías de error relevantes para cada etapa del modelo de Rouse se muestran en la Tabla 1.1. Para algunas clases de tareas las categorías puede ser inaplicables, pudiendo ser omitidas.

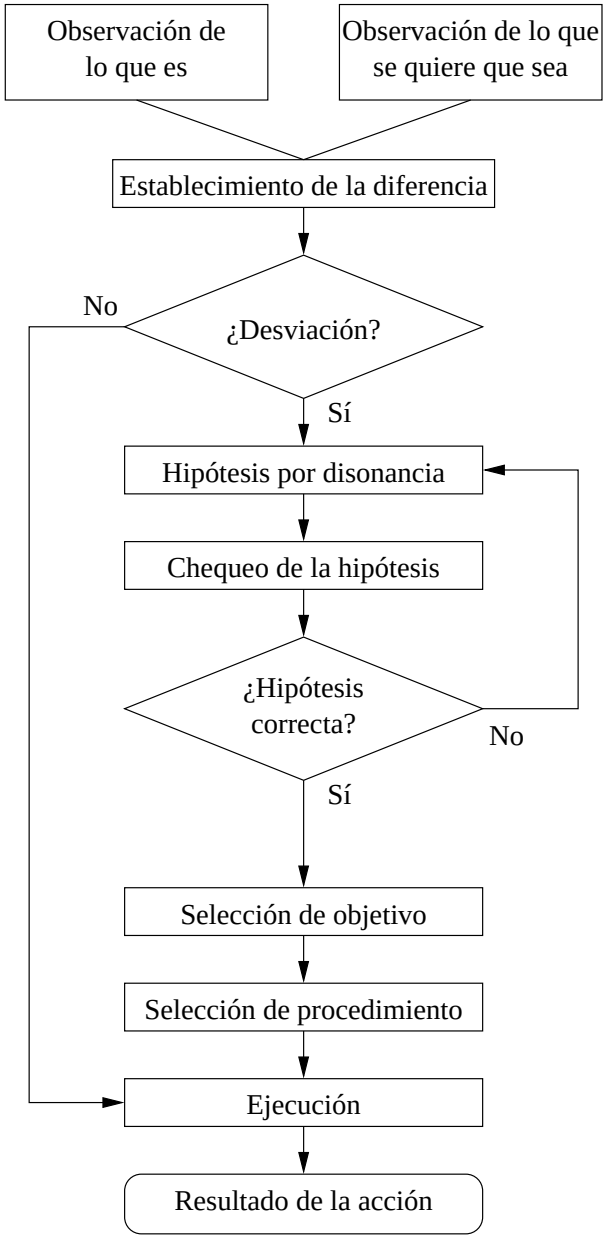


Figura 1.3: Modelo de estadios de la toma de decisiones de Rouse y Rouse (1983).

Estadio	Error
1. Observación del estado del sistema	a. Excesivo
	b. Interpretación errónea
	c. Incorrecta
	d. Incompleta
	e. Inapropiada
	f. Falta de observación
2. Elección de la hipótesis	a. Inconsistente con las observaciones
	b. Consistente pero muy inverosímil
	c. Consistente pero costoso
	d. Funcionalmente irrelevante
3. Chequeo de la hipótesis	a. Incompleta
	b. Aceptación de una hipótesis equivocada
	c. Rechazo de una hipótesis correcta
	d. Falta de hipótesis
4. Selección del objetivo	a. Incompleto
	b. Incorrecto
	c. Innecesario
	d. Falta de selección
5. Selección del procedimiento	a. Incompleto
	b. Incorrecto
	c. Innecesario
	d. Falta de selección
6. Ejecución del procedimiento	a. Paso omitido
	b. Paso repetido
	c. Paso añadido
	d. Pasos fuera de secuencia
	e. Secuencia
	f. Posición discreta incorrecta
	g. Rango continuo incorrecto
	h. Incompleta
	i. Acción inapropiada no relacionada

Tabla 1.1: Categorías de error de los diferentes estadios cognitivos establecidos por Rouse y Rouse (1983).

Niveles cognitivos y el error humano

Una referencia muy empleada en la ingeniería es el modelo de la escalera de decisión de Rasmussen (1983 1986), basado en la psicología del procesado de la información. Es ampliamente reconocido como un modelo decisivo en el modelado de procesos cognitivos, Reason (1990). En este modelo las tareas se pueden clasificar como comportamientos de habilidad, basados en reglas y basados en aprendizaje. El desarrollo de cualquier actividad se compone de elementos de comportamiento de habilidad (apoyado en mecanismos de realimentación y alimentación similares a los mecanismos de control), la aplicación de reglas (adquiridas tras entrenamiento, experiencias o simplemente planificadas con anterioridad al momento de su consideración) y planificación basada en el conocimiento. La ejecución basada en habilidad no requiere la necesidad de atención consciente por parte de la persona, mientras que las basadas en reglas, en las situaciones donde las reglas existen, requieren de de mayor actividad consciente de reflexión sobre que regla aplicar. En situaciones en las que, por ser poco familiares o imprevistas, no existe un conjunto de reglas, el individuo debe apoyarse en su conocimiento acerca del funcionamiento del sistema para resolver los problemas y planificar un conjunto de actuaciones que le permita alcanzar sus objetivos.

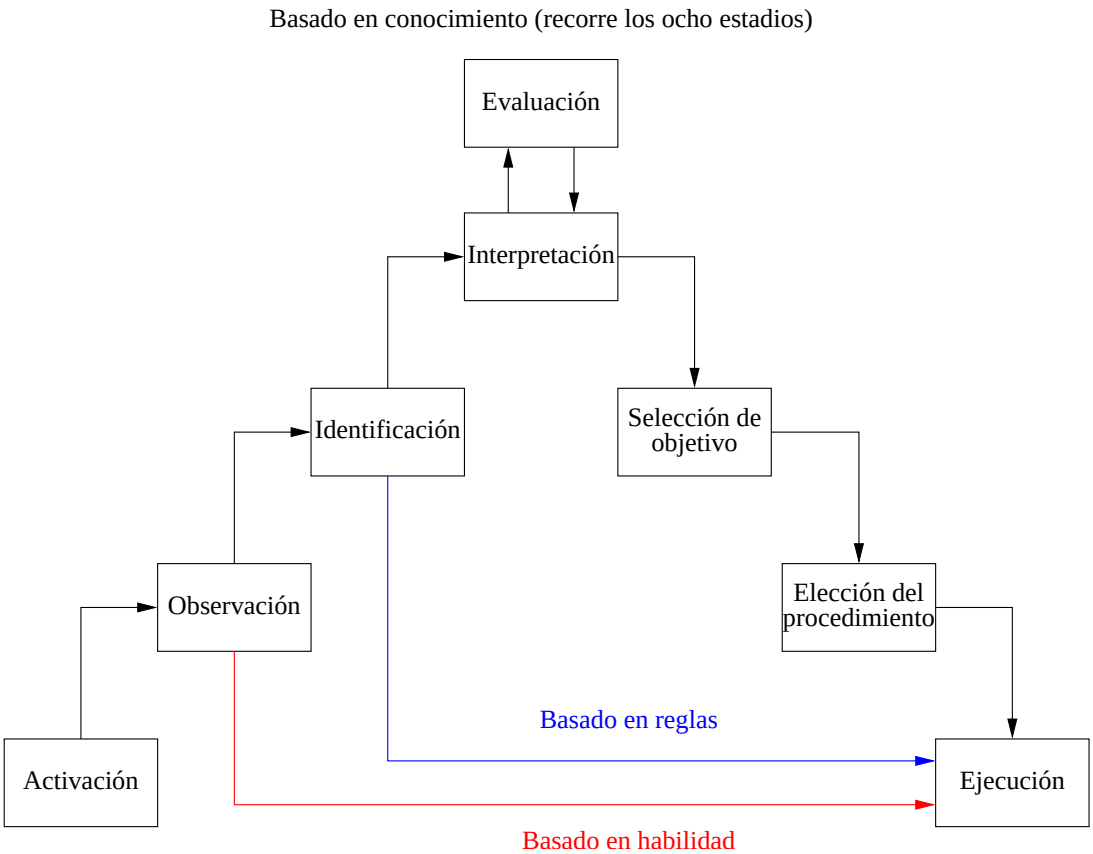


Figura 1.4: Modelo de escalera de toma de decisiones de Rasmussen (1986).

Distingue ocho etapas en el proceso de tratamiento de la información y toma de decisiones, Figura 1.4, teniendo cada una de ellas sus errores característicos. Por ejemplo, las acciones no intencionales como los deslices y los lapsus de memoria son característicos de las ejecuciones basadas en la habilidad. Las basadas en reglas pueden llevar a fallo como resultado de la elección errónea de la regla a aplicar en dicha situación. Fallos originados en el comportamiento basado en el conocimiento son principalmente, mecanismos de erróneos del razonamiento en la compresión del dispositivo que se usa.

El modelo SRK de Rasmussen es uno de los de mayor impacto en todos los campos en que se considera la seguridad y la fiabilidad humana. Por ejemplo, Reason (1990) basa su modelo de GEMS en la aplicación del SRK y el estudio de los modos de transición entre los diferentes modos de comportamiento. El SRK también ha sido empleado para el desarrollo de entornos de estudio de sistemas socio-tecnológicos, como el análisis del trabajo cognitivo (*Cognitive Work Analysis*, CWA), Vicente (1999)[11], y el análisis de tareas cognitivas (*Cognitive Task Analysis*, CTA), Bes y Johnson (1998).

A pesar de ser el modelo con mayor número de aplicaciones, cuenta con sus detractores. Por ejemplo, Dougherty (1990) critica la falta de definición de los niveles de comportamiento cognitivo y la validez del modelo, mientras que Hollnagel (1994), no comparte la definición del proceso de toma de decisiones como un camino de un solo carril, en el que el sujeto pasa por todos los estadios, que es precisamente el caso menos habitual[12]. De hecho, la SRK tiene muy poca consideración en el espectro de técnicas de identificación del error humano (*Human Error Identification*, HEI), Kirwan (1992ab).

Modelo de cognición primitiva, sesgos cognitivos y error humano

La taxonomía del error desarrollada por Reason (1990), se corresponde con una clasificación conceptual. Esta taxonomía es muy referenciada en el campo de la investigación del modelado del error, Tabla 1.2. Su clasificación de los tipos de error es una de las más completas, siendo aconsejable su uso cuando el operador se mueve en dominios fenomenológicos basados en reglas o conocimiento.

Considerando el trabajo previo de Norman (1981), establece que los **deslices** y los **lapsus** son errores resultantes de algún fallo en la ejecución y/o el seguimiento del estado de la ejecución de una secuencia de acciones, independientemente de que el plan que las guíe sea adecuado para alcanzar su objetivo. Los deslices se definen como acciones que no son ejecutadas como estaban planeadas, mientras que los lapsus (fallos de la memoria) pueden pasar desapercibidos a menos de que el individuo se percate de que no ha realizado dicha acción o acciones.

[11] El CWA es un modelo aplicado en el estudio del desarrollo de trabajo mediante el uso de computadoras, no desde el punto de vista de la interacción hombre-máquina, como los métodos clásicos de interacción hombre-computadora (*Human Computer Interaction*, HCI), sino dentro de los denominados métodos de ingeniería de sistemas cognitivos (*Cognitive Systems Engineering*, CSE), enfoque más reciente formulado por Hollnagel y Woods (1983). CSE es una metodología que no se centra en la consideración de la cognición humana como una función interna o un proceso mental, sino como un trabajo cognitivo, es decir, en como la cognición es necesaria para realizar de forma efectiva las tareas relacionadas con objetivos específicos.

[12] Esta diferenciación se verá en más detalle en la Sección 1.1.4.

Descripción	Tipo de error
Acción no ejecutada como estaba planeada (error basado en la habilidad)	Fallo de atención (desliz)
	Fallo de la memoria (lapsus)
Acción ejecutada como estaba planeado, en parte error basado en reglas, un plan fuertemente simplificado está erróneamente planteado[a] (error)	Error basado en las reglas.
	Error basado en el conocimiento
Acción es ejecutada tal como estaba planeado, pero el plan deliberado es erróneo[b] (violación)	Violación rutinaria (frecuente)
	Violación excepcional (raras veces ocurre)
	Acto de sabotage

[a] Se entiende por erróneamente planteado como que no es apropiado para el objetivo considerado por el operador.

[b] Se entiende como violación la desviación de las reglas, procedimientos o políticas de operación. Notar que en contraste con otros autores, Reason no define esta desviación del criterio como un error.

Tabla 1.2: Tipos de errores considerados en la taxonomía establecida por Reason (1990).

Los **errores basados en reglas o en conocimiento** son aquellas acciones ejecutadas tal como estaba planeado pero que no alcanzan el resultado previsto. Ese tipo de error es más sutil, más complejo y más peligroso que los deslices. Además, son más difíciles de detectar ya que no se manifiestan como desviación de la intención del sujeto. Estos errores se pueden clasificar en:

- **faltas de maestría**, donde una cierta solución preestablecida del problema se aplica de forma inadecuada,
- y **carencia maestría**, donde el individuo, no teniendo una rutina disponible apropiada para resolver el problema, es forzado a trabajar con un plan de acciones ideado a partir de su conocimiento.

Reason también describe las **violaciones**, que se pueden definir solamente en términos de marco de motivación y contexto social en los cuales se gobierna el comportamiento. Las violaciones son desviaciones de acciones de procedimientos prescritos. Mientras que las acciones que las provocan pueden ser pensadas, las consecuencias no lo suelen estar generalmente. Las violaciones son quizás los errores más graves, ya que llevan al individuo a estados del sistema que

presentan el mayor riesgo, asociados a fenomenologías de difícil interpretación y muy alejados del marco de operacional normal, donde cualquier error subsiguiente conlleva consecuencias más graves.

Finalmente, Reason (1990) propuso otro marco conceptual en el cual localizar el origen de los tipos básicos de errores humanos, el denominado sistema de modelo genérico del error (*Generic Error Modelling System*, GEMS), que combina el SRK de Rasmussen y una clasificación de los posibles errores distinguiendo entre deslices de habilidad (*skill-based slips*) y lapsus por un lado, y errores basados en reglas y conocimiento por otro lado (*rule-based or knowledge-based mistakes*). Los aspectos formales de esta aproximación se comentarán en detalle en la Sección 1.1.4.

Modelo simple de cognición

En versiones más completas de su aproximación a los tipos de error, Hollnagel (1994) estableció un modelo cognitivo de causas genéricas como base para la taxonomía fenomenológica, que había establecido en trabajos anteriores, denominado modelo simple de cognición (*Simple Model of Cognition*, SMoC), Figura 1.5. Este modelo presenta una estructura similar al modelo SRK de Rasmussen y la formalización GEMS de Reason. Este aspecto ha llevado a realizar su integración armonizando sus diferencias, discutiendo la estructura formal de todas estas aproximaciones y su integración en la Sección 1.1.4.

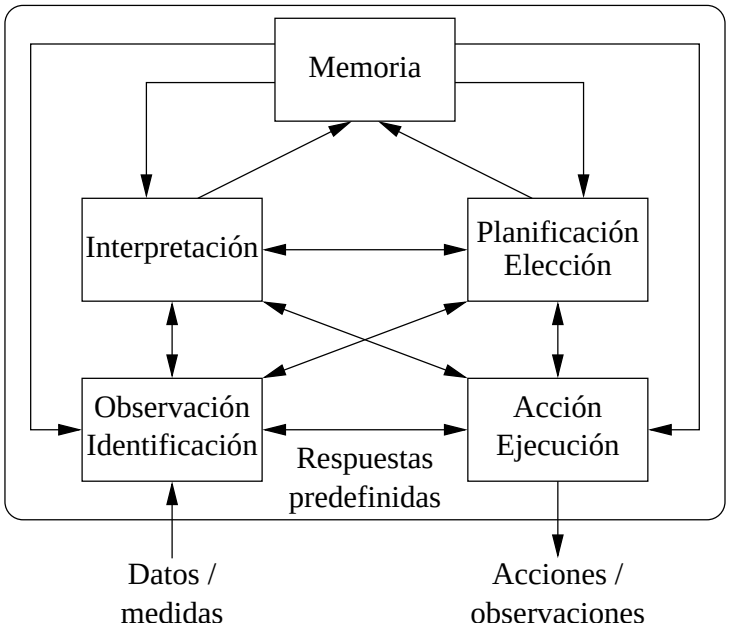


Figura 1.5: Modelo simple de cognición, SMoC, de Hollnagel (1994).

1.1.3.3 Clasificación de estructura de acciones

Se encuadran en esta categoría las estrategias de diseño que pretenden evitar el error. El objeto es producir mejoras mediante la consideración de los elementos en que se estructuran las acciones. Para ello se construye un sistema relacional entre los errores humanos, los tipos de errores y los factores de influencia que les afectan. Destacan los trabajos de Seifert y Brauser (1987) y Rasmussen (1986).

1.1.3.4 El dilema de la automatización

El aprovechamiento por parte de la ingeniería de los beneficios de la aplicación de la automatización, la computerización y la aplicación de sistemas de información para asistir al usuario en procesos de diferente naturaleza no siempre ha ido acompañado de la consideración de las consecuencias que pudiese tener su implementación en el lazo de control cuando en este se incluye el factor humano.

Durante la segunda guerra mundial surgió una corriente en la ingeniería que trataba la interacción hombre-máquina y la integración de la actuación humana de aplicando las misma técnicas de trabajo en ambos dominios del sistemas de control, el automático y el manual. El ejemplo más relevante dentro de estas líneas de trabajo fue la realizada por Fitts (1951)[13]. Respecto al tratamiento de la introducción de sistemas computerizados y de tratamiento de la información surgió dentro del estudio de los factores humanos dos líneas de trabajo relacionadas con la HCI y el diseño y evaluación de las interfases hombre-máquina (*Man Machine Interface*, MMI). Sin embargo, uno de los efectos más importantes de la introducción de las máquinas en los sistemas de producción ha sido el impacto de la automatización en la ejecución y el control de procesos.

No fue hasta finales de los años 70 y principios de los años 80 cuando surgieron partidarios de cambiar la orientación de las metodología de diseño de los automatismos, considerando al operador y sus necesidades cognitivas dentro de los papeles que la automatización le asignaba, resaltando la importancia de considerar la interfase entre los controles automáticos y manuales y una jerarquía entre ambos, sopesando los tiempos de respuesta y los mecanismo cognitivos del operador. Esta idea fue establecida en varios trabajos, entre los que cabe destacar los de Rouse (1981) y Bainbridge (1983). Este último introdujo de forma contundente la necesidad de evaluar el efecto de introducir un alto grado de automatización al definirlo como una ironía y paradójico cuando se hace de forma inapropiada, dejando establecido que cuanto más avanzado es un sistema de control más crucial es la intervención humana[14].

Hasta el momento, el procedimiento seguido de forma más habitual por los diseñadores era aplicar la denominada lista de Fitt, según la cual se decidía qué controles se debían automatizar y cuales se deberían dejar a cargo del operador, aplicando al humano la misma metodología que a la máquina. Bainbridge fue uno de los primeros en objetar contra la aplicación ciega de esta

[13] Hay que resaltar que el trabajo de Paul M. Fitt fue pionero y aún presentan una amplia aplicación en diferentes sectores. Buena prueba de ello es la ley de Fitt, la cual establece entre otros aspectos la incompatibilidad de rapidez y precisión del movimiento humano, Fitts (1954).

[14] Esta idea ya fue expuesta en la presentación del estudio del error humano en la filosofía.

regla. Los argumentos que dio en esta dirección fueron que siguiendo la lista de Fitt como único criterio, el operador quedaba relegado a ejecutar actuaciones que el diseñador era incapaz de automatizar y que las tareas manuales remanentes después de la tarea de automatización solían consistir en tareas de supervisión y en actuaciones manuales en situaciones en las que el operador debía asumir el control del proceso si fallaba el control automático. La crítica nacía de este hecho, ya que en este tipo de implementaciones requiere del operador habilidad para las actuaciones manuales, pero en realidad no se ejercitan, cuestionándose sus capacidades por falta de entrenamiento. Además, resaltaba la necesidad de habilidades cognitivas, debiendo el operador ser capaz en todo momento de monitorizar los controles automáticos y de tener un conocimiento detallado de la situación, aspecto fuera de las especificaciones de la lista de Fitt. Para paliar este problema, Brainbridge aconsejó realizar el diseño de los automatismos aplicando las mismas reglas que rigen el control manual del sistema considerado.

Finalmente, a estos dos efectos indeseados que surgen en sistemas altamente automatizados, falta de habilidad y conocimiento de la situación, hay que añadir otros efectos por deficiencias de diseño de los propios automatismos, que pueden llevar a lo que Fitt denominó degradación elegante (*graceful degradation*), es decir, el automatismo puede llegar a enmascarar sus propias deficiencias realizando tareas aparentemente correctas, dando ventajas al hombre en ciertas circunstancias.

Esta tendencia de los años 80 vino acompañada al final de la década por los partidarios de la aplicación de las últimas tendencias de control difuso, sistemas expertos e inteligencia artificial al control. Esta nueva ola en el diseño de controles llegó al campo de la ingeniería de centrales nucleares, ver por ejemplo Bernard (1989) y Husseiny et al. (1989).

A partir de los años 90, se frenó la euforia asociada a los nuevos desarrollos de automatismos, en cierto modo arrastrados en un principio por el gran avance que experimentaron las ciencias computacionales en la década de los años 80. En este sentido, la década de los años 90 fue una década de maduración de estas tendencias y su unificación en una nueva generación de metodologías basadas en la armonización de la interacción del hombre y la máquina. Un análisis de la situación fue realizado por Parasuraman (1997), donde se hace una revisión del impacto de distintas políticas de implementación de la automatización y de los problemas asociados.

Resumiendo, actualmente existen tres formas de plantearse la implementación de la automatización en un sistema, fuertemente relacionadas con la evolución histórica la automatización, a saber, Grozdanovic y Jankovic (2002):

- La automatización centrada en la máquina (*Machine-centered Automatization*, MCA).
- La automatización centrada en el hombre (*Human-centered Automatization*, HCA).
- La automatización equivalente (*Equivalent Automatization*, EA).

La **metodología MCA** es un acercamiento tecnológico a la automatización en la que el operador queda relegado a un papel suplementario, dando el papel principal del control a los automatismos, esforzándose los diseñadores en alcanzar el mayor grado posible de automatización del

control. La asignación de funciones se realiza basándose en el principio de comparabilidad de hombres y máquinas y sus diferentes versiones, al estilo de los trabajos de Fitt.

Desde la psicología del trabajo y la ingeniería rusa se desarrolló la que se vino a denominar la **metodología HCA**. En ella el operador debe ser considerado como tema central dentro del esquema de reparto del trabajo y los sistemas técnicos se definen como un instrumento del trabajo. Esta metodología aplica el denominado principio de asignación de funciones o el *principio del operador activo*. Este principio define la necesidad de la participación activa y continua del operador humano en el control para tener una reserva fiable ante cualquier fallo de la automatización o cuando se produzca una situación de emergencia o inesperada que requiera mayor protagonismo de éste en el control. Por lo tanto, es prioridad necesaria la implementación de controles semiautomáticos frente a los automáticos. En el campo de los factores humanos en America y Europa, el HCA aplica tales principios de asignación de funciones como el principio de la comparabilidad del hombre y máquina, la asignación dinámica y la asignación adaptativa de funciones. Los principios de la asignación dinámica y de la asignación adaptativa de funciones se basan en definir diferentes niveles de automatización del control y del papel del operador en esos niveles en función de las condiciones de operación del sistema y del estado psicológico del operador. La principal preocupación en estos diseños es la carga de trabajo en sus diferentes manifestaciones, tanto cognitivas como físicas.

En la **metodología EA**, en las que el automatismo y el operador deben alternativamente asumir el papel predominante en el control, se debe garantizar el mismo grado de fiabilidad para las dos partes del sistema. En este sentido, se desarrolla un nuevo principio de asignación de funciones denominado principio de mutua reserva (*Principle of Mutual Reservation*, PMR) del hombre y de la máquina. El PMR define la estrategia del cambio flexible en el grado de automatización en el proceso de control asignando un mayor control al automatismo cuando las funciones del operador sean excesivamente complejas y dando mayores capacidades en el control al operador cuando se presenten fallos en el control automático o situaciones no previstas en el diseño del mismo.

Mientras que la metodología EA se encuentra en una fase inmadura de definición e implementación, investigadores relacionados con el mundo nuclear se esfuerzan en reseñar la necesidad de diseñar los sistemas automáticos empleando el enfoque de la HCA, Cacciabue (1997ab) y Parasuraman et al. (2000). En esta aproximación, la automatización es fragmentada, es decir, en contra de que su participación se establezca como un continuo en todo el proceso de control, queda segmentada apoyando al operador en sus distintas fases de control, tales como procesado de información sensorial, percepción/memoria de trabajo, toma de decisiones y la selección de respuesta. Cabe decir que hay un criterio generalizado, y natural, a rechazar la automatización de forma completa de la fase de toma de decisiones.

Tanto en la aproximación HCA como en la incipiente EA, que denominaremos aproximaciones híbridas a la implementación de la automatización del control, surgen tres aspectos de elevada importancia en lo que respecta al operador:

- La conciencia de la situación (*Situation Awareness*, SA):

  Surge la necesidad de analizar las capacidades el operador para garantizar su fiabilidad en el lazo de control. El operador ante el automatismo debe ser capaz de caracterizar el proceso fenomenológicamente y desarrollar estrategias al respecto. Ambos aspectos requieren de tiempo para la recuperación de la memoria de trabajo del individuo y el seguimiento de actuaciones procedimentadas. Además, se deben considerar tiempos de actuación óptimos que permitan su vigilancia, con dos premisas: el operador debe ser entrenado en como actúa el automatismo y debe entender tanto como actúa el automatismo como el objetivo de sus actuaciones. Si el grado de automatización impide que el operador pueda hacer un seguimiento lógico de las actuaciones automáticas y de la secuencia de sucesos del transitorio puede dar lugar a incapacidad por parte del mismo a la hora de corregir automatismos que fallen o de diagnosticar su error, incluso provocando su incapacidad de continuar con las actuaciones de recuperación. Esta idea estaba siempre presente, aunque se consideró con mayor relevancia a partir de las opiniones críticas de Rouse (1981) y Bainbridge (1983).

- Carga de trabajo:

  Al igual que el SA, el impacto de la automatización sobre la carga de trabajo del operador siempre se ha considerado desde el punto de vista del diseñador pero no siempre con el mismo criterio. Mientras Bainbridge (1983) simplemente asociaba el impacto negativo en la carga de trabajo como producto de la falta de habilidad del operador para la realización de las tareas del control automático y la falta de entrenamiento, actualmente el enfoque se corresponde más con la idea de que un automatismo excesivo aumenta la carga de trabajo cognitiva del operador, sin ningún tipo de consideración adicional, aumentando la posibilidad de fallo a la hora de diagnosticar el funcionamiento de las actuaciones automáticas y aumentando sus tiempos de respuesta en situaciones críticas, Furukawa et al. (2000).

- Modos de error:

  En lo que respecta a los modos de error que introducen la computerización y la automatización en entornos operacionales, existen tres perspectivas. Una es que su implementación introduce errores nuevos y nuevas fuentes de error, otra que son los mismos errores de siempre pero se ejecutan de forma distinta y otros que los errores que se pueden cometer son mucho más serios[15]. En esta línea están los trabajos ya citados de Furukawa

[15]Consideremos, como un ejemplo cotidiano, el cambio que se ha experimentado en los últimos diez o veinte años en los sistemas operativos de los ordenadores, en el cual se ha pasado de interfases de línea de comando basadas en texto a interfases basadas en menus visuales. Todo el mundo estará de acuerdo en que los nuevos sistemas operativos con interfase de usuario gráfica de ventanas y de menus contextuales ofrecen un entorno de trabajo más amigable y que aumenta la producción, pero también es cierto que incrementa el daño ante un error. Si consideramos que puede hacerse de forma errónea en cada una de estas interfases, es fácil comprobar como toda una categoría de error de la interfase de línea de comando (entiéndase la referente a errores de escritura y tipográficos) ha sido eliminada mediante las interfases de menus visuales. Simplemente, este tipo de errores ya no es posible. A pesar de que la interfase de comandos presenta una cantidad significativa de posibles errores, casi la totalidad de ellos no tienen ningún efecto (solamente mensajes de mala sintaxis o de comando inexistente). Sin

et al. (2000), cuyas consideraciones llevan a concluir que los errores debido a tiempos inadecuados de ejecución serían más probables, o como resalta Cacciabue (1997ab), que la automatización a niveles elevados deja poco margen a los errores de omisión, (*Errors of Omission*, EoO), pero como contrapartida aumenta las probabilidades de errores de comisión, (*Errors of Commission*, EoC). Es evidente que cualquier perspectiva actual está lejos del espíritu que se vivía en los años 80, en los que los más críticos veían los automatismos como herramientas para mitigar errores del operador, Bainbridge (1983). Esta perspectiva, aunque no deja de ser cierta, se considera ahora con cautela.

En el sector nuclear la preocupación está vigente, y existen diversidad de estudios para evaluar este aspecto, pudiéndose destacar los trabajos teóricos de Furukawa et al. (2000), en el estudio de funciones cognitivas del operador mediante las técnicas discretas de simulación de sucesos (*Discrete Event Simulation*, DES), Kim y Seong (2006), centrados en el efecto de fallos de la instrumentación y de los controles que den lugar a fallos de causa común al quedar anuladas la actuación automática y la manual y, finalmente, de Cacciabue (2000), cuyos trabajos están orientados a la evaluación de sistemas de control automáticos, MMI y otros aspectos del HCI.

En la vanguardia de la mejora de estos aspectos y en el desarrollo de herramientas para la evaluación del grado de automatización de un sistema se pueden destacar los trabajos de Cacciabue, Parasuraman, Sheridan y Wickens, a los cuales ya se ha hecho referencia varias veces. Entre dichas herramientas se pueden citar INTEROPS, Schryver (1988), empleada para evaluar los criterios de asignación de funciones, o la herramienta HERMES, Cacciabue (1997ab), para evaluar la interacción dinámica entre el hombre y la máquina de forma global y específicamente en el diseño de controles.

Aunque las mejoras en los últimos años han sido sustanciales, desde el punto de vista teórico se requiere la maduración de las metodologías de EA, aplicando las nuevas teorías de cooperación entre automatismos y operadores, como la desarrollada por Skjerve y Skraaning (2004). En estas nuevas aproximaciones, al igual que en la HCA, se establece que el operador debe ser el punto de partida en todo diseño de automatismos y que el sistema automático debe ser diseñado para asistir al operador en el alcance de los objetivos/metas operacionales, pero su mayor innovación radica en que se establecen reglas de mejora para la gestión de la información que el operador recibe del estado del proceso, pasando del concepto de MMI al de cooperación en el control. Para presentar la idea de cooperación establece que a pesar de que los controles automáticos pueden llegar a dominar un sistema, en realidad el responsable último de los hechos es el operador, produciéndose lo que denomina una relación asimétrica cuyos aspectos negativos se acentúan al poder llegar a sentirse el operador segregado del control sobre el sistema y, sin embargo, ser el responsable de los posibles daños o perjuicios, llegando incluso al extremo de que el operador desarrolle estrategias contra las actuaciones del control para evitarlo[16]. Para evitar este tipo de conductas del operador, las metodologías EA establecen que es necesario

embargo, en los sistemas basados en menus visuales, el único posible error es el de sustituir un comando por otro, el cual no solamente tendrá efecto, sino que además tendrá inevitablemente un efecto no deseado y, posiblemente, con una potencialidad en el daño superior.

[16]El operador dota de intención a la máquina y rivaliza con sus objetivos. Véase un ejemplo de ello en el incidente de la central alemana de Stade introducido al principio del capítulo.

que los automatismo se justifiquen, muestren toda la información posible sobre su actividad y demuestren que es correcta, buscando una relación cerrada entre los objetivos de la máquina y del operador, basándose en estas ideas el concepto de cooperación.

En lo que respecta a la industria nuclear, la base para determinar qué actuaciones ligadas a las especificaciones de diseño de sistemas de seguridad se deben automatizar y cuales no, están rigurosamente establecidas en el estándar ANSI-58.8, *Time response design criteria for safety-related operator actions*, de obligado cumplimiento, o bajo la supervisión del impacto de la automatización en la supervisión del operador y la realización de acciones correctoras[17]. El sector nuclear siempre se ha caracterizado por un alto grado de inmovilismo tanto en la etapa de diseño como en la de gestión operacional, pero esta política está cambiando en los últimos años. En este sentido, los organismos reguladores se han visto obligados a hacer un seguimiento más detallado de los cambios de política, incluyendo las modificaciones relacionadas con del grado de automatización considerando el impacto en la actuación humana cuando se hagan cambios que puedan afectar a la fiabilidad de la actuación de los sistemas de protección. Así, la NRC (1991) publicó en 1991 una carta genérica en la que revisaba los criterios en las actuaciones manuales del operador deben reemplazar la automáticas tras detectar cierta anomalía en la aplicación de los criterios por parte de los explotadores. Posteriormente, publicó una nota informativa en 1997, NRC (1997), en la que se alertaba a los explotadores de la obligación de evaluar el impacto asociado a las modificaciones de los grados de automatización de tareas relacionadas con la actuación de los sistemas de protección. En este sentido, parece haber cierta necesidad de metodologías que permitan evaluar el impacto de estas modificaciones, existiendo actualmente grupos de trabajo volcados en esta línea de investigación. Uno de los grupos de investigación referencia desde el punto de vista del establecimiento de la base teórica y del desarrollo de metodologías es el del departamento de ciencias y tecnologías de la energía del laboratorio nacional de Brookhaven (*Brookhaven National Laboratory*, BNL), Higgins et al. (2002 2004), O'Hara (1999), O'Hara y Brown (1999). Hay referencias de aplicación de metodologías clásicas pero orientándolas a la evaluación de los grados de automatización, siendo trabajos principalmente realizados en el campo de la aeronáutica, Shorrock et al. (2003), aplicando metodologías de juicio de expertos (p. ej. HAZOP) y de análisis de fiabilidad y factores humanos (SHERPA, CREAM y TRACEr).

A esta preocupación hay que añadir que, en general, la evolución del sector nuclear está encabezada por nuevos diseños de reactores con alto grado de automatización, como es el caso de la cuarta generación, que presentan una tipología de problemática desde el punto de vista de la seguridad completamente diferente, Hines y Uhrig (2005). Estos diseños hacen un uso extensivo de todo tipo de herramientas generadas a partir de la implementación de las últimas tecnologías en tratamiento de la información, computerización de procedimientos y sistemas de monitorización de procesos[18] y el desarrollo teórico y la implementación de nuevas metodologías para la evaluación de la actuación humana en este tipo de entornos se hace mas acuciante.

[17]Este aspecto se trata en detalle en la Sección 1.2.1, que describe el tratamiento de las acciones del operador relacionadas con las actuaciones de los sistemas de seguridad (SROA).

[18]Para tener una visión más amplia de los sistemas desarrollados se puede consultar la base de datos que mantiene la IAEA al respecto, IAEA (1996).

1.1.4 Definición de error humano y su taxonomía

El error humano es el resultado no deseado de la comisión u omisión de una acción[19] desde la libertad y la convicción exclusiva del individuo, es decir, sin condicionantes de ningún tipo impuestos por agentes externos.

Es importante destacar la diferencia que se establece entre el error humano y la acción errónea, considerando que el error humano es libre y, por contra, la acción errónea está condicionada en su planteamiento, ejecución o valoración por algún agente externo. Ejemplos de estos agentes en las distintas etapas consideradas podrían ser los objetivos de diseño del sistema no compatibles con las creencias del individuo o con procedimientos mal diseñados, limitaciones de MMI y criterios de analista de accidentes, respectivamente. El error humano se debe definir en cuanto a la divergencia de la voluntad e intención depositadas por el individuo en las acciones y el resultado obtenido de ellas, sin condicionantes adicionales.

Durante el proceso de redefinición se han desechado las definiciones clásicas al uso en los estudios de ingeniería, Rigby (1970), Swain y Guttman (1983), Norman (1986) y Reason (1990), Sección 1.1.3, siendo el argumento el ya expuesto en dicha sección: todas ellas establecen la definición del error humano en términos de los requerimientos derivados del sistema. Esta definición es práctica para la ingeniería, pero no define el error humano de forma general.

1.1.4.1 Aproximación fenomenológica a la taxonomía del error humano

En lo que respecta a la taxonomía se ha decidido adoptar prioritariamente la taxonomía fenomenológica de Hollnagel (2000). La aplicación de esta taxonomía fue llevada a cabo mediante un conjunto de experimentos realizados en el Proyecto de Reactor de Halden (*Halden Reactor Project, HRP*) demostrando sus capacidades, Kaarstad et al. (1994 1995).

En esta aproximación, la distinción entre causas y manifestaciones refleja una distinción paralela entre tipos de error y modos de error. Un tipo de error es una categoría que está basada y deriva su significado de un modelo subyacente de las acciones humanas, generalmente del procesado de la información por humanos o de los procesos cognitivos de la mente. Un ejemplo bien conocido de estos tipos de errores son el rango que abarca desde las EoO y las EoC hasta los lapsus y errores derivados de los mecanismos cognitivos basados en la habilidad, en reglas y conocimiento, ya comentados al introducir el estudio del error en la ingeniería. Por contra, los modos de error, o también denominados modos de fallo humano, se refieren a una descripción de las manifestaciones observables. Los modos de error pueden incluso estar lógicamente estructurados refiriéndose a un conjunto de posibles fallos físicos.

Considerando el tipo de estudio a realizar, para un análisis de accidentes retrospectivo puede ser importante construir una explicación aceptable de las condiciones y causas del accidente, prestando atención a los tipos de error. Sin embargo, para realizar un estudio predictivo, tal como se hace en el HRA, es mucho más importante identificar los tipos de acciones incorrectas

[19] Se entiende por acción (o conjunto de ellas) al ejercicio de la posibilidad de hacer como fruto de la voluntad del individuo, siendo errónea si no cumple con el primero de las tres dimensiones reconocidas por Hollnagel para el error, Sección 1.1.3, pág. 15.

que pueden darse, sin considerar las causas, y por lo tanto centrarse exclusivamente en los modos de error.

Cabe comentar que, aparte de esta clasificación, Hollnagel toma prestada la terminología de la genética, atendiendo a fenotipos como los patrones de las acciones humanas que son observables y se manifiestan por ellos mismos en el comportamiento humano. Así, un modo de error está fuertemente relacionado con el concepto de fenotipo. Mientras que el genotipo, describe el conjunto probable de las causas que en la situación dada son necesarias y suficientes para explicar el fenotipo observado. En este sentido, no hay que confundir el concepto de genotipo con el de tipo de error, ya que, como se extrae de su definición, no son equivalentes. Empleando esta aproximación se evita la necesidad de establecer que funciones cognitivas dan lugar a los mecanismos de fallo cognitivos que propician el error humano. En este caso, bastaría con identificar posibles fenotipos de modos de error e identificar el genotipo o genotipos asociados a los mismos.

En lo que respecta al modelo cognitivo de Hollnagel, éste puntualiza que hay muchas formas de categorizar las funciones cognitivas, pero que una de las más simples es diferenciar entre análisis y síntesis. Así, define el análisis como el conjunto de funciones usadas para identificar la situación actual, incluyendo la observación, la identificación, el reconocimiento, el diagnóstico, etc. La síntesis es el conjunto de funciones que se usan para determinar que hacer y como hacerlo, incluyendo la elección, la planificación, la programación en tiempos de las acciones, etc.

En el modelo implementado en este trabajo se ha identificado el análisis con la observación y la interpretación, la síntesis con la planificación y, finalmente, la ejecución, cuyas categorías están íntimamente relacionadas con los modos de error. Una relación de los modos de error considerados y de los modos de error genéricos cognitivos definidos como posibles mecanismos de activación de los mismos se dan en las Tablas 1.3 y 1.4. En lo que respecta a las categorías no relacionadas con la persona, es decir, los genotipos definidos en la categoría de tecnología y de aspectos de organización, se han considerado de interés exclusivamente los procedimientos y el entrenamiento, Tablas 1.5 y 1.6.

Varios trabajos resaltan que esta taxonomía es particularmente relevante pues es una de las aproximaciones de mayor alcance, en el sentido de que proporciona una forma estructurada de modelar un espacio completo de posibles modos de error en actuaciones humanas, Fields (1999). Además, una ventaja que presenta la aproximación fenomenológica al error frente a la causal es que da la capacidad de simular el fallo humano de forma determinista a partir de un estudio previo del contexto determinando posibles activadores, es decir, los genotipos. Sin embargo, el estudio de activadores puede o no apoyarse en una aproximación cognitiva y causal a la acción humana, aunque si se requiera desde un punto de vista teórico por completitud. Esta aproximación cognitiva se aborda en la sección siguiente.

Modo de error	Efectos específicos	Definición / explicación
Tiempos	Demasiado pronto	Una acción iniciada demasiado pronto, antes de que se produzcan o la señal o las condiciones requeridas (acción prematura)
	Demasiado tarde	Una acción iniciada demasiado tarde (acción tardía)
	Omisión	Una acción que no fue hecha en absoluto (dentro del intervalo de tiempo permitido)
Duración	Demasiado larga	Una acción que continua más allá del punto en que debería haber parado
	Demasiado corta	Una acción que fue parada antes de cuando debería haberse hecho
Fuerza	Poca	Fuerza insuficiente
	Mucha	Fuerza excesiva, demasiado esfuerzo
Distancia / Magnitud	Demasiado lejos	Un movimiento llevado demasiado lejos
	Demasiado cerca	Un movimiento no llevado suficientemente lejos
Velocidad	Demasiado rápido	Acción realizada demasiado rápido, con demasiada velocidad o finalizada demasiado pronto
	Demasiado lento	Acción realizada demasiado despacio, con poca velocidad o finalizada demasiado tarde
Dirección	Dirección equivocada	Movimiento en la dirección equivocada, es decir, adelante en vez de atrás o izquierda en vez de derecha
	Movimiento equivocado	Tipo de movimiento equivocado, por ejemplo tirar de un pomo en vez de darle vuelta
Objeto equivocado	Vecindad	Un objeto que está físicamente próximo al que debería de haberse usado
	Objeto similar	Un objeto de apariencia similar al objeto que debería de haberse usado
	Objeto no relacionado	Un objeto usado por error, incluso sin tener relación con el objeto que debería haberse usado
Secuencia	Omisión	Una acción que no fue realizada. Esto incluye en particular la omisión de la última actuación o actuaciones de una serie (interrupción)
	Salto adelante	Se saltan una o más acciones de la secuencia
	Salto atrás	Una o mas acciones que habían sido llevadas a cabo se realizan de nuevo
	Repetición	La acción previa es repetida
	Trasposición	El orden de dos acciones consecutivas de altera
	Acción errónea	Una acción extraña o irrelevante se lleva a cabo (acción por inercia)

Tabla 1.3: Modos de error básicos en la aproximación fenomenológica de Hollnagel.

Función cognitiva	Modo potencial de error cognitivo	
Ejecución	E1	Ejecución errónea de una acción, con respecto a fuerza, distancia, velocidad o dirección
	E2	Acción realizada en destiempo, tanto como demasiado pronto como demasiado tarde
	E3	Acción sobre objeto equivocado (vecindad, similitud o no relacionado)
	E4	Acción realizada fuera de secuencia, tales como repeticiones, saltos y trasposiciones
	E5	Acción no realizada (omisión), incluyendo la omisión de las últimas acciones en una serie (*undershoot*)
Interpretación	I1	Diagnóstico fallido, también diagnóstico erróneo o incompleto
	I2	Error de decisión, también no tomar una decisión o tomar una decisión errónea o incompleta
	I3	Interpretación tardía, es decir, no hecha a tiempo
Observación	O1	Observación del objeto equivocado. La respuesta es dada al estímulo o suceso equivocado
	O2	Identificación errónea, debida por ejemplo por una pista equivocada o una identificación parcial
	O3	Observación no realizada (omisión), pasar por alto una señal o una medida
Planificación	P1	Error de prioridad, como la elección del objetivo erróneo (intención)
	P2	Formulación inadecuada de plan, cuando el plan es incompleto o equivocado

Tabla 1.4: Genotipos relacionados con la persona establecidos por Hollnagel.

Consecuencia general	Definición / explicación	
Procedimientos inadecuados	P1	El texto del procedimiento es ambiguo y abierto a la interpretación. La lógica del procedimiento puede que no sea clara
	P2	El texto es incompleto, las descripciones dadas por el procedimiento son incompletas, y asume que el usuario tiene conocimiento adicional
	P3	Las descripciones del procedimiento son incorrectas.
	P4	El texto del procedimiento no encaja con la realidad física, debido, por ejemplo, a actualizaciones de equipos

Tabla 1.5: Categoría de procedimientos dentro de los genotipos relacionados con la tecnología de Hollnagel.

Consecuencia general	Definición / explicación	
Habilidades insuficientes	T1	Fallo en la realización por falta de habilidades (experiencia práctica), lo que significa que la tarea no puede completarse
	T2	Manejo deficiente de equipos, producido por falta de habilidad (experiencia práctica), lo que significa que el equipo es usado incorrectamente
Conocimiento insuficiente	T3	Confusión. La persona no tiene certeza acerca de lo que tiene que hacer, debido a falta de conocimiento
	T4	La persona pierde el conocimiento de la situación (compresión) debido a una falta de conocimiento

Tabla 1.6: Categoría de entrenamiento dentro de los genotipos relacionados con la organización de Hollnagel.

1.1.4.2 Aproximación causal a la taxonomía del error humano

La misma noción de error implica la existencia de una causa[20], lo cual es motivo suficiente para realizar una aproximación causal al establecimiento de los mecanismos cognitivos a considerar, buscando un esquema causal clásico que respalde la taxonomía de genotipos y fenotipos de Hollnagel. En nuestro caso, el esquema causal escogido está basado en la SRK de Rasmussen en su versión formalizada por Reason, considerando a su vez la clasificación de tipos de errores proporcionada por Swain en la discusión de los diferentes elementos. De esta forma, se intenta demostrar que el esquema fenomenológico escogido cubre de forma completa las posibles manifestaciones de mecanismos de fallo causales, además de incluir la totalidad de los modos de fallo por ellos considerados.

La visión clásica de la clasificación de fenotipos de errores humanos de Swain se puede presentar, reestructurada atendiendo a los criterios de clasificación actuales, como:

- Error de omisión.
- Error de comisión. Se pueden distinguir:
  - Error de secuencia.
  - Error de sustitución.
  - Error de tiempo inadecuado de ejecución.
  - Error cuantitativo.
  - Error de selección.

Esta taxonomía de Swain del error ha sido criticada por su ambigüedad al ser muy sensible a la definición del término de acción errónea, resultando en unos límites entre los diferentes tipos de error difusos. Por ejemplo, un error de comisión siempre podrá redefinirse como uno de omisión en función de qué acción se considere como requerida y un error de secuencia se puede considerar en algunos casos como un error de tiempos, Hollnagel (2000). Desde la definición de Swain de esta taxonomía, la consideración de los errores de comisión y de omisión ha suscitado una discusión continua en cuanto a su definición y su diferente impacto, como ya ha quedado claro, y aspecto que se ha salvado al escoger la taxonomía establecida por Hollnagel.

La clasificación de Swain fue posteriormente mejorada por Reason (1990), definiendo de nuevo los fenotipos de errores considerando una aproximación a genotipos cognitivos en su aproximación formalizada a la SRK, Tabla 1.2:

- Basado en habilidad: este nivel se caracteriza porque se fundamenta en la recuperación de la memoria de un patrón de instrucciones para realizar una tarea. Los errores establecidos por Reason son los deslices (*slips*) y los lapsus (*lapses*), usualmente errores de falta de atención o de distracción.

[20] De hecho, es usual referirse con el término error a la causa, al suceso y al resultado que se obtiene, confusión que se intenta evitar a lo largo de todo el trabajo pero debido al profundo arraigo cultural puede que no se consiga con éxito.

- Basado en reglas: los problemas familiares son abordados empleando las ayudas disponibles en sala de control en forma de procedimientos. Se consideran los errores (*mistakes*) como resultado de escoger las reglas inapropiadas, y causados por un fallo en el establecimiento del estado del sistema, reconocimiento de patrón de operación demasiado entusiasta, apuesta por sucesos más frecuentes y reglas deficientes. El proceso cognitivo en el cual se localiza este fallo es las denominada búsqueda sistemática[21].

- Basado en conocimiento: los problemas novedosos son abordados mediante la aproximación analítica a la situación, denominándose al proceso cognitivo relacionado como la búsqueda topológica[21]. De nuevo aquí se definen los errores asociados, pero esta vez causados por comprensión incompleta del sistema, predisposición en la confirmación, exceso de confianza o tensión cognitiva, por ejemplo.

Con la intención de caracterizar la importancia de cada uno de estos tipos de error cognitivos, Reason (1990) acompaña su trabajo con una estimación a partir de sucesos de la frecuencia de errores en estos niveles y otros parámetros relacionados con acciones correctivas ejecutadas tras la detección del error, Tabla 1.7.

Nivel cognitivo	Frecuencia de error	Detección del error	Corrección del error
Basado en habilidad	61 %	75-95 %, media 86 %	70 %
Basado en reglas	27 %	50-90 %, media 73 %	50 %
Basado en conocimiento	11 %	50-80 %, media 70 %	25 %

Tabla 1.7: Frecuencias de error en los niveles cognitivos definidos por Rasmussen y otros parámetros relacionados.

Como se puede comprobar, los errores de habilidad son los más frecuentes, pero hay que considerar que los humanos suelen ejecutar más tareas en niveles de habilidad que de reglas, y más en el rango de reglas que de conocimiento, por lo que se puede concluir que una tarea que sea ejecutada en el nivel de conocimiento es más probable que falle. También es de resaltar que, en lo que respecta a la eficiencia en su detección, los errores ligados a la ejecución de acciones en el nivel de habilidad se caracterizan por tener cierta resistencia a ser detectados, debido a la nula carga cognitiva que requieren y, por tanto, escasa atención por parte del individuo tanto en su ejecución como en los resultados. Por razones similares y con parecidas consecuencias, los operadores tienen problemas para realizar un seguimiento de las actuaciones realizadas en el nivel basado en reglas si se exige una posterior evaluación de las acciones realizadas, llevando a situaciones de desconocimiento del estado de componentes y sistemas, faltando base de juicio para la toma de decisiones. El origen de estos problemas radica en que este nivel exige un grado de atención bajo, fomentando actitudes pasivas.

En otros campos, destacando los estudios realizados por Wiegmann y Shappell (1997) para la aviación aplicando metodologías de determinación de causas de accidentes se han estimado las frecuencias de ocurrencia de los diferentes tipos de error establecidos por la taxonomía

[21]Los procesos de búsqueda sistemática y topológica se explican más adelante en este mismo apartado, pág. 41.

Tipo de error	Frecuencia (%)
Desliz	14,28
Lapsus	11,18
Error	57,13
Violación	17,42

Tabla 1.8: Frecuencias de errores en función de la taxonomía de Reason.

de Reason, Tabla 1.8, obteniendo resultados similares. En este caso, los resultados parecen indicar que en entornos fuertemente procedimentados, los errores (*mistakes*) son los fallos más comunes.

Según el modelo SRK de Rasmussen, dependiendo del grado de rutina asociado a una acción, se tenderá a llevar a cabo su ejecución moviéndose en el nivel de habilidad, mientras que para el caso de actuaciones en las que se tenga poca práctica, situaciones de emergencia, el procedimiento de procesado de información se podría extender hasta el nivel del conocimiento. Así, según Rasmussen (1986), se pueden dividir los procedimientos de desplazamiento de un nivel cognitivo a otro como:

- La **búsqueda topográfica**, realizada de niveles superiores a inferiores. El experto, en la búsqueda del origen del problema, parte de una investigación de las posibles causas y las evalúa de forma que deriva, desde su propio estado mental, hipótesis de causas y su grado de exactitud. Así, la búsqueda de arriba a abajo parte de suposiciones acerca de las posibles causas en el nivel basado en el conocimiento.
- La **búsqueda sistemática**, realizada de niveles inferiores a superiores. El experto trata, vía el uso de procedimientos de reconocimiento de patrones, reconocer las causas correspondientes al problema dentro de su propio espacio de problemas posibles, siendo por lo tanto capaz de clasificarlo.

Si el uso de ambas estrategias, la búsqueda topográfica y la sistemática, no obtienen un patrón de comportamiento en un nivel inferior, entonces se pasa a un nivel cognitivo superior. Cuanto menor sea el nivel de comportamiento, menor atención consciente se requiere, resultando que en el nivel basado en la habilidad el procesado de la información tiene lugar de forma completamente inconsciente. En el nivel basado en reglas, se requiere atención consciente en la selección de las reglas, las cuales pueden ser posteriormente implementadas con un grado bajo de atención , Theureau et al. (2000). Finalmente, en el nivel basado en el conocimiento, los procedimientos de procesado de la información tienen lugar de forma exclusiva bajo control consciente por parte del sujeto.

Sin embargo, cabe distinguir entre el procesado de la información y la percepción de la misma. En este sentido, tanto el nivel basado en reglas como el basado en conocimiento realizan la percepción de la información en el nivel basado en la habilidad, estando fuertemente condicionados por los procedimientos de reconocimiento de patrones. Sin embargo, la diferencia surge en el momento en que se accede a la información. En el caso del proceso de búsqueda topográfica, la percepción de información solo tienen lugar durante la comprobación de las

hipótesis realizadas, comparando las hipótesis con los patrones observados, y en el caso del proceso de búsqueda sistemática, tiene lugar durante cada fase de reconocimiento de patrones, siendo el punto de partida del proceso cognitivo. Por lo tanto, el nivel basado en habilidad es usado durante el proceso de evaluación cognitiva del nivel basado en reglas, y durante el proceso de identificación del nivel basado en conocimiento, convirtiéndose en un nivel básico para el procesado de la información en los niveles superiores. Este hecho implica que cualquier tipo de error que se considere en estos niveles superiores debe incluir efectos del hábito.

Introducido a nivel teórico el modelo de Rasmussen, hay que aclarar que ciertas dificultades surgen al intentar aplicarlo, ya que no hay asociado a los diferentes niveles ningún parámetro observable que permita definir las transiciones, lo que hace que en algunos casos sea fuertemente dependiente del juicio del analista la asignación de fallos a un nivel o a otro durante los estudios retrospectivos.

Observada esta limitación, Reason (1990) formalizó los mecanismos de transición entre los niveles de comportamiento. En esta aproximación el comportamiento basado en la habilidad prevalece si existen habilidades que apliquen perfectamente a la situación. La transición al nivel basado en reglas se produciría cuando se observasen desviaciones en la situación respecto a los modos de comportamiento de habilidad, y cuando se tenga conocimiento de reglas que pueden ser aplicadas. Finalmente, el nivel de conocimiento es aplicado solo en el caso de que la desviación de la situación respecto a la forma de comportamiento aprendida sea tan grande que no se pueda identificar un conjunto de reglas que permitan gestionar la situación. Esta aproximación es mucho más formal que la aportada originalmente por Rasmussen ya que define la base de la transición entre los niveles en función de las posibilidades de los niveles. Por contra, Rasmussen simplemente indica que se pasa a un nivel superior cuando no se encuentra ningún patrón adecuado del comportamiento en el uso de las estrategias de búsqueda definidas, dejando este parámetro libre y dependiente no del contexto sino del sujeto que realice el juicio, siendo mucho más difícil de concretar.

En resumen, la formalización de Reason presenta un grado de objetividad superior a la hora de realizar estudios predictivos, ya que solo hay que considerar aspectos externos al sujeto para la evaluación del nivel de comportamiento cognitivo de cada momento, suponiendo una respuesta cognitiva estándar por parte del sujeto. Por ejemplo, el uso del nivel basado en la habilidad en situaciones de operación anormal o de emergencia estaría condicionado por el entrenamiento en simuladores y el hábito en su realización dentro del rango de la operación normal. El uso del nivel basado en reglas se definiría mediante un estudio de los procedimientos aplicables al estado del sistema, anormal o de emergencia. Y, finalmente, siendo el más difícil de evaluar, el nivel cognitivo llevaría asociada la concreción del grado de conocimiento del sujeto del estado del sistema a partir de los conocimientos que pueda poseer a partir de formación teórica. Un aspecto adicional que no se ha comentado antes, es que en los niveles basados en reglas y en conocimiento habría que considerar la experiencia operativa y en simuladores de los operadores y como influye esta en sus juicios. Este tipo de aspectos son analizados, entre muchos otros, en los simuladores de escala real de salas de control. Los resultados obtenidos manifiestan una tendencia de los operadores a seguir los procedimientos de forma estricta y mostrar un comportamiento basado en reglas cuando su experiencia es baja o avanzada, detectándose con más frecuencia comportamientos de violación de los procedimientos en el rango de experiencia

intermedia, comprendido entre los diez y los trece años, Parzer et al. (2003) y Park et al. (2005). En estos trabajos, además se evaluó la relación entre la desviación en el seguimiento de los procedimientos y la complejidad de las acciones comprendidas en ellos, cuantificada mediante metodologías de análisis basadas elementos objetivos ponderados por factores subjetivos. Los resultados concluyeron que los operadores tienden a modificar las acciones o alterar el orden de realización de las mismas cuando la complejidad de las actuaciones es intermedia, mientras que para grados de complejidad bajos o altos, realizan las actuaciones tal y como se registran en los procedimientos. Esta idea está relacionada con el hecho de que los operadores solo alteran la ejecución de los procedimientos cuando hay un balance adecuado de comprensión del objetivo de las actuaciones y, una de dos opciones, una divergencia respecto a la forma de alcanzarlos o incomprensión de la relación de los objetivos con los pasos registrados en los procedimientos.

Es importante resaltar en lo que respecta al análisis de accidentes y a las ideas extraídas que la mayoría de los accidentes se dan por una acumulación de errores latentes, siendo en su mayoría de naturaleza humana. Estos errores latentes pueden estar relacionados con deslices o lapsus durante el mantenimiento[22], errores latentes en el diseño del sistema, la organización, la planificación y, particularmente importantes, los relacionados con los procedimientos de emergencia. Es importante destacar, que incluso errores latentes no detectados pueden hacer que acciones aparentemente correctas parezcan erróneas, provocando mayor incertidumbre en el juicio y en la ejecución de acciones posteriores.

Respecto a los errores producidos en el nivel basado en reglas, se pueden decir que tienen como origen la falta de experiencia en ese tipo de fallos del sistema, ya que el entrenamiento es raras veces suficiente para producir un comportamiento basado en reglas en situaciones fuera de la operación normal, Theureau (2000). Frente al desarrollo de acciones en el nivel basado en el conocimiento, cabe observar que la complejidad del sistema y el estrés provocado por una situación de emergencia, provocan que se favorezca una respuesta basada en reglas. Esta idea se fomenta si se considera que la implementación de la defensa en profundidad y de la automatización puede obstaculizar las actividades cognitivas asociadas a las actuaciones en niveles cognitivos superiores.

Esta polaridad registrada entre comportamientos basados en reglas y en conocimiento se ha puesto de manifiesto recientemente con preocupación en numerosos trabajos, p. ej. Theureau et al. (2000) y Park et al. (2005). De hecho, está ampliamente demostrado que una fuente importante de errores proviene de operar en un nivel cognitivo equivocado. En este sentido se han observado tres comportamientos de naturaleza completamente dispar, Shen et al. (1997), Karin (2002) y Kim y Seong (2005):

- Los operadores son, generalmente y dependiendo de su grado de experiencia, reticentes a pasar del nivel basado en reglas al de conocimiento incluso con conciencia de que las reglas puede que no sean apropiadas o estén fallando. Además de los aspectos ya comentados, como la complejidad del sistema, el estrés y la automatización, en los simuladores se ha detectado que los procedimientos suelen bloquear su capacidad de análisis, tomando

[22] Por ejemplo, las válvulas mal alineadas de TMI.

actitudes pasivas y desentendiéndose del problema si hay una rotura entre las actuaciones demandadas por los procedimientos y las expectativas del operador. Si el operador no tiene un conocimiento de la situación bien establecido, prefiere atenerse a las reglas prescritas.

- También se ha detectado el comportamiento opuesto, es decir, que cuando el operador sigue un procedimiento puede decidir realizar otro conjunto de actuaciones que considere más apropiadas, saliéndose de lo estipulado, cuando su juicio de la situación presenta una desviación sustancial del aparentemente considerado en los procedimientos[23].

- En situaciones en las que el operador actúa en el nivel basado en el conocimiento, presenta un comportamiento similar al primeramente expuesto para el nivel de reglas, según el cual, incluso ante evidencias de que su gestión del suceso no es la adecuada, tiende a obviar los parámetros que la contradicen y a favorecer la observación y consideración de aquellos que la favorecen, permaneciendo en su postura hasta que la situación real presenta un alto grado de disonancia respecto a la esperada.

Todos estos comportamientos observados en simuladores ponen en entredicho la definición de los procedimientos como un conjunto de reglas prescritas que se siguen incondicionalmente, tal y como se considera en los análisis de seguridad y en la evaluación del diseño de los EOP.

1.1.4.3 Armonización de las taxonomías fenomenológica y causal

En los modelos de Rasmussen y de Reason, se puede así identificar básicamente dos aspectos diferentes que son críticos cuando se realiza la elección del nivel de comportamiento cognitivo. Primeramente, se debe considerar el fenómeno del procesado consciente de la información y, posteriormente, las formas automatizadas de comportamiento, así como el papel que desempeñan ambas en las etapas del proceso cognitivo. No es difícil relacionar estos estadios cognitivos y las fases cognitivas de análisis y síntesis de Hollnagel. Los estadios de procesado e información se corresponderían con la etapa de análisis, mientras que la determinación de objetivos lo haría con la de síntesis. Considerando la relación formal entre estos estadios, la separación de fases cognitivas de la metodología SRK y los errores estipulados por Reason en cada una de ellas, se encuentra el respaldo causal a la aproximación fenomenológica de Hollnagel, Figura 1.6.

La relación establecida podría conllevar el establecimiento de un paralelismo formal entre los tipos de error establecidos por Hollangel, Tabla 1.4, y los correspondientes a Reason para cada nivel cognitivo de la SRK, Tabla 1.2, pero la relación no es biunívoca, Rasmussen (1987). Sin embargo, se puede establecer una relación directa en lo que respecta al grado de atención entre

[23]Este comportamiento puede estar motivado, por ejemplo, por el hecho de los procedimientos tienden a considerar el estado del sistema en momentos específicos del incidente (realizando evaluaciones excesivamente puntuales durante la progresión del evento), la reticencia del operador a gestionar las emergencias de forma segura (que es la base de diseño de los procedimientos) pero no optimizada, y los problemas para seguir el orden de pasos informado por divergencia de criterios, Theureau et al. (2000).

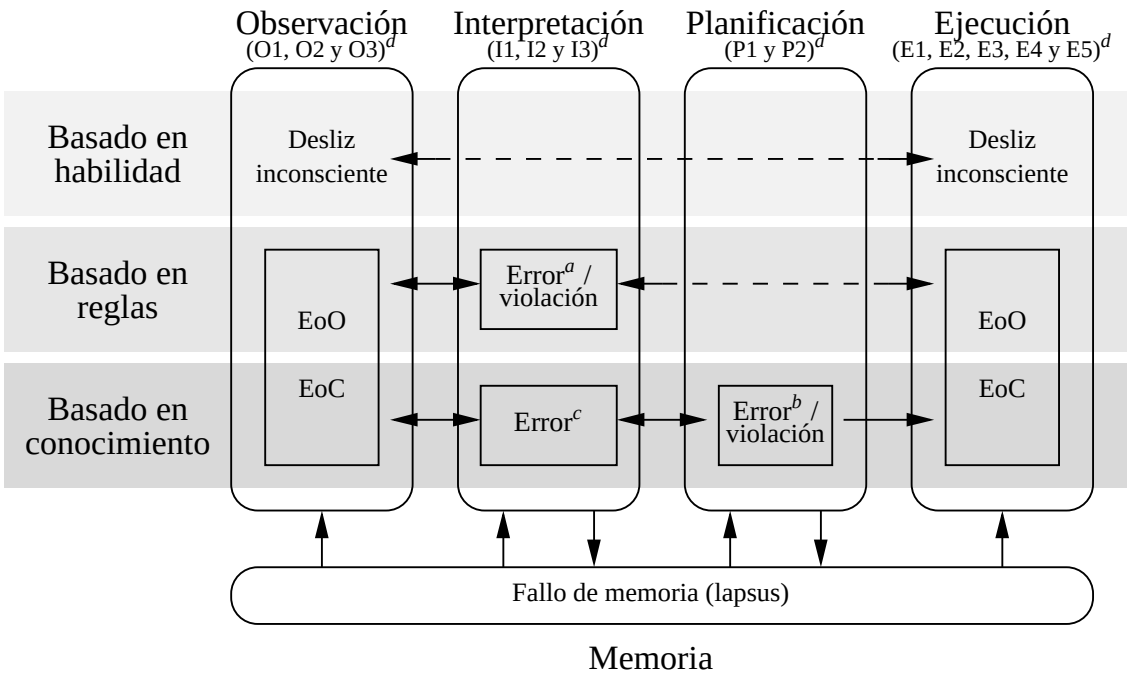
comportamiento cognitivo basado en habilidad y él grado de atención que requiere cada nivel cognitivo de la SRK y los genotipos cognitivos de la aproximación de Hollnagel. En este sentido, se han determinado los diferentes tipos de error en cada aproximación y se ha comprobado como, aunque no sea de manera formal, ambas aproximaciones se apoyan conceptualmente.

Los lapsus de memoria pueden afectar a todas las etapas cognitivas, ya que todos los mecanismos de observación, interpretación, planificación o ejecución se apoyan en la memoria. En lo que respecta a los EoC, los EoO y los deslices se pueden dar en las etapas de observación y ejecución, aunque sus consecuencias pueden provocar otros errores en las otras etapas cognitivas, conllevando interpretaciones o juicios incompletos o erróneos al hacer fallar los mecanismos de búsqueda, tanto sistemática como topológica, dando lugar a los errores (*mistakes*) basados en reglas o conocimiento de forma inducida. Es evidente que los mecanismos de búsqueda sistemática y topológica tienen sus propios modos de fallo, como ya se ha expuesto anteriormente, relacionados con los conceptos de faltas de maestría y carencia de maestría de Reason. Todos estos conceptos están relacionados con los modos de fallo de Hollnagel, Figuras 1.6 y 1.7.

Mientras que los EoO están ampliamente contemplados en el diseño y paliados por sistemas automáticos, esta revisión de los modos de error no se puede cerrar sin hacer una mención especial a los EoC, que tanto debate han conllevado en los últimos 15 años. Desde principios de los años 90 el debate sobre este concepto ha sido acalorado, y no sin razón, ya que la experiencia operativa vino a demostrar que las metodologías HRA no contemplaban de forma adecuada este tipo de errores. Para considerar de forma completa esta casuística hace falta el respaldo de un modelo de cognición y, por lo tanto, se hizo necesaria una evolución de los métodos de análisis de factores humanos para incluir esta nueva dimensión del error, naciendo lo que se vino a denominar la segunda generación de metodologías de HRA[24]. Actualmente, hay una conciencia clara de la importancia de los EoC y su consideración en los análisis de seguridad, siendo amplia la base bibliográfica al respecto, CSNI (1998), Macwan (1992), Dang y Reer (2002), y los estudios teóricos, pudiendo destacar entre los que actualmente se están llevando a cabo la línea conjunta de investigación del instituto Paul Scherrer (PSI) de Suiza y el Gesellschaft für Reaktorsicherheit (GRS) de Alemania, Hirschberg (1999), Hirschberg (2004) y Dang (2006), así como los estudios con base en la experiencia operativa, Pyy et al. (2001).

Es importante destacar que la mayoría de los trabajos apuntan a la importancia de los EoC en los estadios de diagnosis, interpretación y planificación, destacando la necesidad de integrarlos en un estudio de las otras etapas, pues su activación suele estar ligado a otros tipos de errores en las etapas de observación o ejecución. De hecho, ciertos autores consideran que los errores en SA (por ejemplo en la etapa de diagnosis) y formación de intención son de mayor importancia cuando están relacionados con otros mecanismos de error en otras etapas cognitivas, Hirschberg (2004). Trabajos recientes han constatado que los errores de EoC en el diagnóstico del suceso inicial, SA y planificación, son provocados en su mayoría por deficiencias en los procedimientos en los accidentes que presentan dinámicas complejas, NRC (2000).

[24]Se pueden destacar entre estas metodologías la ATHEANA, CREAM, CAHR y CODA, entre otras.



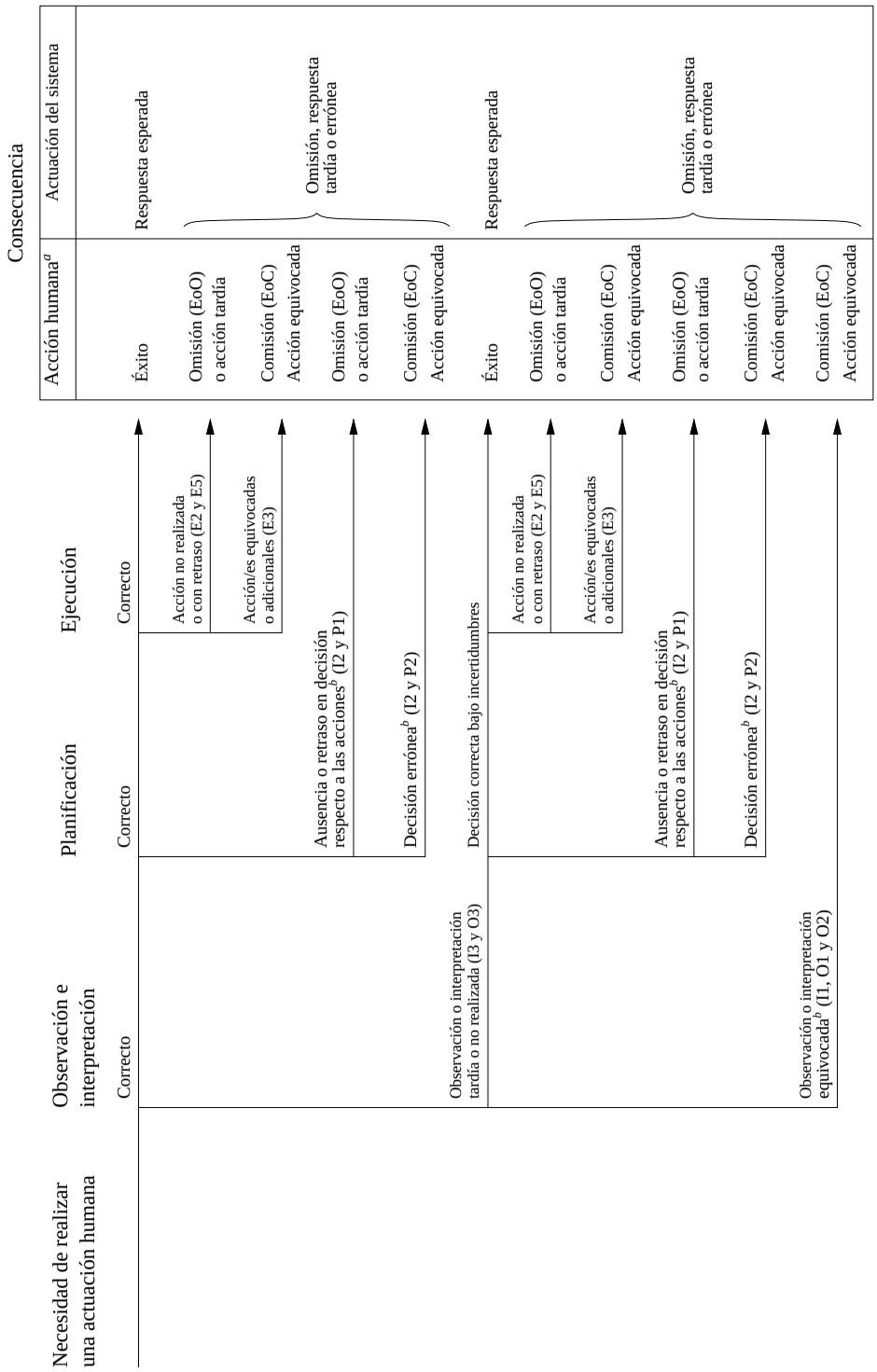
[a] *Rule-based mistake*, fallo en la búsqueda sistemática.

[b] *Knowledge-based mistake*.

[c] Fallo en la búsqueda topológica.

[d] Cada uno de los tipos de error considerados por las otras metodologías puede ser debido a uno o más de los modos de error consdierados por Hollnagel.

Figura 1.6: Relación de los genotipos cognitivos de Hollnagel con otras aproximaciones cognitivas.



[a]En todos los EoO se considera por separado la acción tardía para evitar la confusión con los EoC, Hollnagel (2000).

[b]No se considera doble fallo, es decir, identificación errónea y retraso en actuación manual.

Figura 1.7: Relación de los modos de error humanos con las definiciones de EoC y EoO.

1.2 Consideración del factor humano en los estudios de seguridad en centrales nucleares

Durante el periodo inicial del desarrollo de la energía nuclear, entre 1950 y 1960, los profesionales que se encargaban del diseño de las instalaciones y que se ocupaban del licenciamiento de las mismas, se percataron de que las consecuencias de un accidente podrían ser catastróficas. Por ello, establecieron que era importante mantener la probabilidad de esos accidentes lo más baja posible. A pesar de no tener técnicas de estimación para cuantificar dicha probabilidad, se decidió aplicar una filosofía de diseño basada en dos piedras angulares: la defensa en profundidad y los márgenes de seguridad. La defensa en profundidad, tal como se define actualmente, consiste en la existencia de múltiples barreras que previenen la liberación de radiactividad, definiéndose usualmente cinco niveles, Tabla 1.9. Si uno falla, este debe ser compensado por el subsiguiente nivel y, por ello, su implementación se realiza de forma que su efectividad es independiente de la de los niveles inferiores o superiores. Las medidas relativas a los tres niveles se deben considerar en las bases de diseño para garantizar el mantenimiento y la integridad estructural del núcleo y para limitar los riesgos de radiación del público. Por contra, las medidas del nivel cuatro deben considerarse más allá de la base de diseño para mantener la probabilidad de emisiones en condiciones severas tan bajas como sea posible (*As Low As Reasonably Achievable*, ALARA), considerando factores económicos y sociales. Al mismo tiempo, se estableció el concepto de criterio de fallo único, diferenciando entre accidentes creíbles o no creíbles. Se puede resaltar el hecho de que el principal foco de atención fue la protección contra accidentes de pérdida importante de refrigerante (*Large Brake Loss of Coolant Accident*, LBLOCA). Este enfoque para alcanzar la seguridad del reactor se definió como la aproximación determinista en el diseño de seguridad. Estas especificaciones de diseño establecían un rango en las condiciones de operación y de los sucesos considerados explícitamente para los cuales la planta debería tener capacidades suficientes para no sobrepasar ninguno de los límites considerados, mediante el uso planificado de los sistemas de seguridad. La verificación de este diseño base se realiza mediante el denominado estudio de seguridad determinista (*Deterministic Safety Assessment*, DSA).

La primera voz que se alzó demandando una nueva aproximación a la seguridad de reactores fue la de Reg Farmer, de la Autoridad en energía atómica británica (*United Kingdom Atomic Energy Authority*, UKAEA), Farmer (1967). Argumentó su crítica en el hecho de que carecía de lógica distinguir entre accidentes creíbles y no creíbles, apoyando la tesis de que todos los accidentes deberían ser estudiados. Para hacer viable la consideración de todos los posibles accidentes, se debería establecer para ello un criterio de exclusión basado en la probabilidad de ocurrencia. Esencialmente, formuló la idea básica de lo que se vendría a denominar el análisis probabilista de seguridad, (*Probabilistic Safety Assessment*, PSA). El primer estudio de PSA que se publicó fue en EUA en 1974, el informe WASH-1400, también más conocido como el informe Rasmussen (1975). Debido a que la principal preocupación hasta el momento había sido diseñar protecciones contra el LBLOCA, este estudio constató que los contribuidores dominantes al daño del núcleo eran el LOCA pequeño y los transitorios. Además, este estudio cuantificó por primera vez la probabilidad de daño al núcleo, estimándola en $5{\cdot}10^{-6}$/(reactor·año), valor que

Nivel	Objetivo	Medidas	Verificación
Nivel 1	Prevención de operación anormal y de fallos	Diseño conservativo y altos grados de calidad en la construcción y la operación	Bases de diseño
Nivel 2	Control de la operación anormal	Control, limitación y detección de fallos en los sistemas de protección y otros aspectos característicos de la vigilancia	Cubierto por el DSA
Nivel 3	Control de los accidentes dentro de la base de diseño	Características de los sistemas de seguridad y procedimientos de emergencia	DSA
Nivel 4	Control de las condiciones severas de la planta, incluyendo prevención del accidente, progresión y mitigación de las consecuencias de los accidentes severos	Medidas complementarias y gestión del accidente	PSA
Nivel 5	Mitigación de las consecuencias radiológicas de la liberación significativa de materiales radiactivos	Planificación de emergencia en el exterior	Plan de emergencia exterior

Tabla 1.9: Objetivo de cada nivel de protección y los medios considerados para alcanzarlos, IAEA (2001).

ascendía a $3{\cdot}10^{-5}$/(reactor·año) al considerar incertidumbres y establecer un criterio de intervalo de confianza del 95 %, resultando ser esta última estimación inesperadamente alta. Como contrapartida, también concluyó que las consecuencias de un suceso con daño al núcleo tampoco eran tan graves como en un principio se consideraron. Por otro lado, también destacó que las actuaciones del operador y la correcta operación de los sistemas soporte eran muy importantes. Para considerar el factor humano, en este informe se aplicó por primera vez la técnica de HRA denominada Técnica de predicción de la frecuencia de error humano (*Technique for Human Error Rate Prediction*, THERP), desarrollada en los años sesenta por Swain. Sin embargo, cabe resaltar que la trayectoria del desarrollo de las primeras técnicas de HRA había sido larga, comenzando los primeros estudios de factores humanos y ergonomía durante la segunda guerra mundial.

En general, y atendiendo a los objetivos marcados, los estudios de ingeniería se pueden clasificar en:

- Estudios retrospectivos: siendo los más típicos los dirigidos a la investigación de accidentes. Su objetivo es identificar las causas raíz de los fallos de sistemas y los errores humanos, basándose para ello en la determinación del flujo de los sucesos y las interaccio-

nes con acciones humanas y, mediante un modelo cognitivo y una taxonomía adecuados, determinar la casuística de la fenomenología observada en el accidente.

- Estudios prospectivos: que abarcan el diseño y los estudios sistemáticos de seguridad, cuyo objetivo es estimar el riesgo de una instalación industrial. Para ello, se requieren que estos tipos de estudios se apoyen en modelos completos del sistema a simular para realizar predicciones. Además, para el caso de los estudios sistemáticos de los sistemas de seguridad, es necesaria la implementación de un método probabilístico que proporcione las frecuencias de ocurrencia de los sucesos, partiendo de las frecuencias de sucesos básicos relacionados con los errores humanos y los fallos de sistemas.

Los estudios de DSA, PSA y HRA se encuadran dentro de los estudios prospectivos, y debido al interés que presentan para este trabajo, son los que se tratarán en detalle en esta sección. El objetivo común de estos estudios es garantizar los niveles de seguridad definidos en la defensa en profundidad. En la Tabla 1.9, se hace referencia al papel que desempeña cada estudio dentro la verificación de los criterios de seguridad de la instalación.

1.2.1 El estudio determinista de seguridad, DSA

El objetivo del DSA es establecer un conjunto de sucesos base de diseño (*Design Basis Event*, DBE) y analizar sus consecuencias mediante el uso de metodologías de cuantificación. Un DBE se define como un fallo específico, o conjunto de fallos, partiendo de unas condiciones iniciales conservadoras y suponiendo que los sistemas de control y de seguridad actúan según especificaciones de diseño.

La consideración del papel del operador en este estudio está relacionada con el último de los aspectos considerados dentro de las especificaciones de un DBE, es decir, la actuación de los sistemas de control y de seguridad. La consideración de estas actuaciones dentro de la operación de la instalación, así como su modificación y la evaluación del impacto en el riesgo, ha sido tratado extensivamente en numerosos trabajos recientemente, pudiendo destacar entre ellos, los realizados por Higgins et al. (2004).

En la fase diseño, el criterio empleado para establecer cuando un control o sistema relacionado con la seguridad debe ser actuado de forma automática o manual se establece en el estándar ANSI/ANS 58.8 *Time response design criteria for safety-related operator actions*, ANS (2001), definiéndose en términos de los tiempos de actuación del operador. La aplicación de este estándar está restringida a los DBE que provocan disparo del reactor y que su análisis es requerido en el DSA para su inclusión en el informe de análisis de seguridad, (*Safety Analysis Report*, SAR)[25].

Al ser el contexto del estándar específico de los DBE, donde se aplica el criterio de fallo único, se considera el error humano como una acción incorrecta u omitida por el operador al intentar realizar una acción relacionada con la seguridad (*Safety-related Operator Action*, SROA)

[25]La guía reguladora 1.70 de la NRC, *Standard Format and content of safety Analysis Report for Nuclear Power Plants* especifica los DBE que se deben considerar.

en respuesta a un evento iniciador. Aclara que cualquier actuación ejecutada posteriormente a la acción errónea y consistente con la misma no se considera un error adicional. En general, una SROA es una acción manual requerida por los EOP que es necesaria para que un sistema relacionado con la seguridad realice su función de seguridad durante el curso de un DBE, siendo habitual que el éxito de la realización de la SROA puede requerir que las manipulaciones discretas sean realizadas en un orden específico.

En lo que respecta a los tiempos de actuación, se define una secuencia de eventos y de intervalos de tiempos, Figura 1.8, en los que se consideran los sucesos claves para analizar la viabilidad de las SROA, Tablas 1.10 y 1.11.

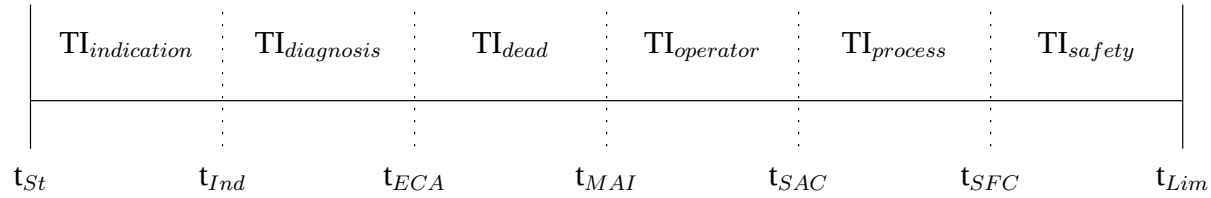


Figura 1.8: Definición de eventos discretos e intervalos temporales para las SROA según el estándar ANSI/ANS 58.8.

Se pueden destacar las siguientes ideas dentro del conjunto de consideraciones del estándar:

- Todos los sistemas y componentes relacionados con la seguridad que deban actuar durante el intervalo TI$_{diagnosis}$, con la finalidad de realizar funciones de seguridad y prevenir la superación de algún límite de diseño, deben ser iniciados por sistemas de protección automáticos.
- Las SROA solo tendrán credibilidad si la consideración de un solo error de omisión del operador no resulta en la superación de algún límite de diseño requerido por el DBE bajo consideración.
- No se deben tener en cuenta acciones de recuperación del error, aunque se consideran los procedimientos, entre otros mecanismos, como posibles medidas para corregir fallos en la ejecución de las SROA.
- Todas las SROA que se consideren dentro de los treinta minutos siguientes al inicio del DBE (t$_{Ind}$) se deben poder realizar desde la sala de control.
- Para realizar cualquier cuantificación se pueden emplear datos experimentales siempre que se demuestre que su valor está dentro de intervalo de confianza del 95 %.

La cuantificación de los intervalos temporales definidos se realiza considerando la condición de planta (*Plant Condition*, PC) que provoca el suceso considerado, en relación a su frecuencia de ocurrencia, Tabla 1.12. A partir de la PC identificada se estiman el intervalos de tiempo para el diagnóstico del suceso, TI$_{diagnosis}$, Tabla 1.13, y los tiempos de ejecución de cada actuación del operador requerida, TI$_{operator}$, Tabla 1.14. Obtenidos los valores de estos intervalos temporales,

Suceso	Definición
Evento inicial, t_{St}	Tiempo en el cual comienza el DBE
Indicación del suceso, t_{Ind}	Tiempo en el cual hay información accesible de que el suceso ha ocurrido (alarmas o indicadores en pantallas)
Acción considerada más temprana, t_{ECA}	Tiempo mínimo tras t_{Ind} en el cual se considera el inicio de la SROA
Acción manual iniciada, t_{MAI}	Tiempo en al cual se considera el inicio de la actuación manual del operador
SROA completada, t_{SAC}	Tiempo en el cual se evalúa la realización de la SROA
Función relacionada con la seguridad completada, t_{SFC}	Tiempo en el cual se obtiene una indicación de que el sistema de seguridad está realizando la función requerida de seguridad
Límite para el evento, t_{Lim}	El tiempo mínimo en el cual un límite de diseño sería excedido en el caso de que la función de seguridad no se completase

Tabla 1.10: Eventos de la secuencia establecida por el estándar ANSI/ANS 58.8 para las SROA dentro de los DBE.

se estima el tiempo requerido por el operador para realizar las SROA consideradas para impedir la violación de cada t_{Lim},

$$T_{SFC} = TI_{diagnosis} + \sum_{1}^{n} (TI_{dead} + TI_{operator} + TI_{process})$$

estimando para cada actuación los intervalos TI_{dead} y $TI_{process}$ aplicando juicio de ingeniería o valores experimentales siempre que se emplee un intervalo de confianza del 95 %.

Si durante la evaluación el intervalo de tiempo TI_{safety} = t_{Lim} - T_{SFC} presenta un valor negativo, lo cual significa que las actuaciones manuales no son posibles en el tiempo en el cual un parámetro de seguridad viola sus límites, t_{Lim}, se dan tres posibles opciones para estipular la actuación del sistema o control como manual:

- Aumentar la automatización o cambiar el diseño, de forma que se reduzca el número de actuaciones manuales.

Intervalo	Definición
Indicación $TI_{indication} = t_{Ind} - t_{St}$	Intervalo de tiempo entre el inicio del DBE y la primera indicación del mismo al operador.
Diagnosis $TI_{diagnosis} = t_{ECA} - t_{Ind}$	Intervalo de tiempo entre la primera indicación del DBE al operador y el tiempo requerido para el inicio de la primera acción considerada. En este intervalo se supone que el operador verifica las actuaciones automáticas, observa los parámetros de la planta y plantifica acciones subsiguientes en respuesta al DBE
Muerto $TI_{dead} = t_{MAI} - t_{ECA}$ o $t_{MAI} - t_{SAC}$	Intervalo/s de tiempo entre $TI_{diagnosis}$ y TI_{safety} en los cuales se da crédito a la actuación del operador, pero sin que se realice una SROA. Un TI_{dead} se debe considerar tras t_{ECA} para la primera acción del operador y tras t_{SAC} para cada una de las acciones subsiguientes sin considerar la última
Respuesta del operador $TI_{operator} = t_{SAC} - t_{MAI}$	Intervalo de tiempo durante el cual el operador inicia y completa las SROA
Respuesta del proceso $TI_{process} = t_{SFC} - t_{SAC}$	Intervalo de tiempo entre la evaluación de la finalización de la SROA y la indicación, mediante la respuesta de equipos y del proceso, de que la correspondiente función de seguridad se ha completado
Seguridad $TI_{safety} = t_{Lim} - t_{SFC}$	Intervalo de tiempo entre la finalización de la última función de seguridad y cuando el suceso límite habría sido alcanzado sin actuación del operador.

Tabla 1.11: Intervalos temporales de la secuencia establecida por el estándar ANSI/ANS 58.88 para las SROA dentro de los DBE.

- Automatizar o modificar el diseño para reducir los tiempos muertos.
- Cambiar el diseño o automatizar para aumentar el tiempo mínimo disponible.

El estándar fue revisado a raíz de la base experimental generada tras los experimentos ORE del EPRI, dando lugar a una nueva definición de los eventos considerados en las secuencias de las actuaciones del operador pero no a ningún cambio relevante en la base del estándar.

Condición de planta	Frecuencia estimada de ocurrencia (F) por reactor y año
PC-1	Operación normal
PC-2	$F \geq 10^{-1}$
PC-3	$10^{-1} > F \geq 10^{-2}$
PC-4	$10^{-2} > F \geq 10^{-4}$
PC-5	$10^{-4} > F \geq 10^{-6}$

Tabla 1.12: Definición de la condición de planta en función de la frecuencia del suceso considerado.

Condición de planta	$TI_{diagnosis}$ **mínimo** (min.)
PC-2	5
PC-3	10
PC-4 y PC-5	20

Tabla 1.13: Tiempo mínimo establecido para el diagnóstico del suceso en función de la PC.

Condición de planta	**Fijo** (min.)	**Variable**[a] (min.)
PC-2	1+	n
PC-3	3+	n
PC-4 y PC-5	5+	n
Actuaciones fuera de la sala de control	30+	n

[a] *n* implica el número de actuaciones manuales discretas requeridas para completar una actuación demandada.

Tabla 1.14: Tiempo mínimo establecido para las actuaciones consideradas del operador en función de la PC.

1.2.2 El análisis probabilista de seguridad y el análisis de fiabilidad humana

El primer estudio de PSA realizado para una central nuclear fue realizado por Reg Farmer en 1967. Sin embargo, no fue hasta 1975, con la publicación del informe WASH-1400 *Reactor Safety Study* por la NRC, cuando se desarrolló de forma completa el primer PSA, aplicando la técnica de árboles de fallo y árboles de sucesos. Las principales conclusiones ya han sido comentadas, aquí solo recordaremos que en este trabajo fue donde por primera vez se integró la técnica THERP de HRA en los estudios de seguridad nuclear. Hasta el momento, ambas metodologías de análisis habían evolucionado por separado.

1.2.2.1 Evolución histórica del PSA

Tras la publicación del informe WASH-1400, la NRC formó un grupo de estudio del riesgo, conocido como el comité Lewis, para llevar a cabo una evaluación independiente de WASH-1400. Este comité realizó un serie de recomendaciones, plasmadas en el informe NUREG/CR-0400, resaltando especialmente la necesidad de hacer uso de la experiencia operativa para cuantificar el riesgo de las instalaciones, apuntando de forma directa al WASH-1400 como una metodología para estimar la potencialidad de secuencias y determinar los posibles precursores. Posteriormente, la división de análisis de riesgo de la NRC arrancó en 1979 el programa de precursores de secuencias de accidentes (*The Accident Sequence Precursor Program*, ASP), con el objetivo de satisfacer dicha recomendación, aunque cabe comentar que su creación estuvo especialmente incentivada por el, por aquellas fechas, reciente accidente de TMI. El primer informe de impacto del programa fue el NUREG/CR-2497, *Precursors to Potential Severe Core Damage Accidents: 1969-1979, A Status Report*. En este informe se incluyó al estudio de PSA realizado para las plantas de Zion e Indian Point, añadiéndose a las ya consideradas en el WASH-1400, Peach Bottom y Surry.

Tras estas aplicaciones del PSA para el análisis de seguridad de las instalaciones, este tipo de estudios fue adquiriendo mayor protagonismo. Dentro de esta tendencia, la NRC potenció sus capacidades de intervención en la gestión, administración y evaluación de la seguridad en las instalaciones, y buena prueba de ello son las la aprobación de la *Backfitting rule*[26] (1984) y la declaración del objetivo de la política de seguridad[27]. Sin embargo, las actuaciones más relevantes vinieron con la carta genérica GL88-20 (1988) relativa a la obligación de realizar el IPE en todas las plantas americanas y el NUREG-1150 (1989), informe que supuso una ampliación de los estudios realizados en la línea del WASH-1400, permitiendo la evaluación del comportamiento de la contención en accidentes severos. Cabe destacar, que a pesar de que las técnicas de

[26] La regla 10 C.F.R. 50.109, denominada *Backfitting rule*, proporciona un protocolo por el cual la NRC puede imponer nuevos requerimientos denominados *backfits*. Son, esencialmente, requerimientos nuevos o modificados impuestos por la NRC, que pueden darse tras la adopción de nueva regulación o a través de la reinterpretación de la ya existente por parte del personal de la NRC.

[27] Tras seis años de trabajo la NRC adoptó su declaración de política de objetivos de seguridad para los reactores nucleares (*Policy Statement on safety goals for nuclear power reactors*). En esta declaración se marcan los objetivos cualitativos de seguridad para los miembros individuales del público, realizando a su vez estimaciones cuantitativas de los mismos.

PSA habían evolucionado notablemente, los resultados y los rangos de incertidumbre obtenidos en ambos estudios fueron similares.

En los años 90, tuvieron lugar el anuncio y el refuerzo de la regla de mantenimiento[28], llevados a cabo en 1991 y 1996 respectivamente, y el establecimiento de la política respecto al PSA[29]. Finalmente, a finales de los noventa, se realizó el respaldo completo a la regulación informada por el riesgo, la regulación basada en la operación (SECY-98-144) y la toma de decisiones basada en el riesgo (RG 1.174), desarrollando finalmente en 1999 el denominado *Reactor Oversight Process* (ROP), NUREG-1649 Rev. 3, como la integración de todas las herramientas para el seguimiento y la evaluación de la operación de las centrales nucleares americanas. Es en esta nueva política de la evaluación de la seguridad de centrales nucleares donde los factores humanos están fuertemente presentes en todo el planteamiento, siendo uno de los cuatro pilares de la metodología. Las directrices para el tratamiento de los factores humanos se desarrollan en base a la siguiente documentación técnica:

- El NUREG/CR-6775, Gertman et al. (2002), *Human Performance Characterization in the Reactor Oversight Process*, donde se realiza una revisión del tratamiento de la actuación humana en el ROP, describiendo los medios de seguimiento, análisis y realimentación empleados. Una de las conclusiones más relevantes de este informe consiste en que la resolución deficiencias relativas a los factores humanos requieren de actuaciones en todos los niveles de la defensa en profundidad, a saber: operación, diseño y prácticas de modificaciones de diseño, prácticas de mantenimiento y de su control, diseño y desarrollo de procedimientos y seguimiento de la gestión.
- El NUREG-1764, Higgins et al. (2004), *Guidance for the Review of Changes to Human Actions*, donde se realiza un estudio que sirve de guía para la evaluación del impacto de la modificación de las actuaciones del operador relacionadas con funciones de seguridad (SROA).
- El NUREG-0711, O'Hara et al. (2004), *Human Factors Engineering Program Review Model*, siendo la referencia de la NRC para la evaluación de todos los aspectos relacionados con la ingeniería de los factores humanos (*Human Factors Engineering*, HFE), tanto para las solicitudes de permisos de construcción, licencias operativas, el estándar de diseño y para la realización de enmiendas de licencias.

1.2.2.2 Evolución histórica del HRA

Mientras que el estudio del factor humano en la ingeniería se remonta a los años de la Segunda Guerra Mundial, en la industria nuclear no se realizó su primera aplicación dentro del marco

[28] Publicada en 1991 como la 10 CFR 50.65, *Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants*, pretende garantizar la efectividad del seguimiento continuo de los programas de mantenimiento para garantizar la fiabilidad de equipos, componentes y sistemas relacionados con funciones de seguridad, además de minimizar las actuaciones espúreas e innecesarias.

[29] Reflejada en la 60 FR 42622 de 1995, establece un respaldo formal al uso extensivo del PSA como parte de las actuaciones de la regulación informada por el riesgo, de forma que complemente la aproximación determinista y soporte y apoye la filosofía de la defensa en profundidad.

del PSA hasta el informe WASH-1400, realizado por Rasmussen (1975). A partir de entonces, empezaron a surgir nuevas metodologías HRA en el ámbito nuclear, proceso que se intensificó tras el accidente de TMI, Figura 1.9.

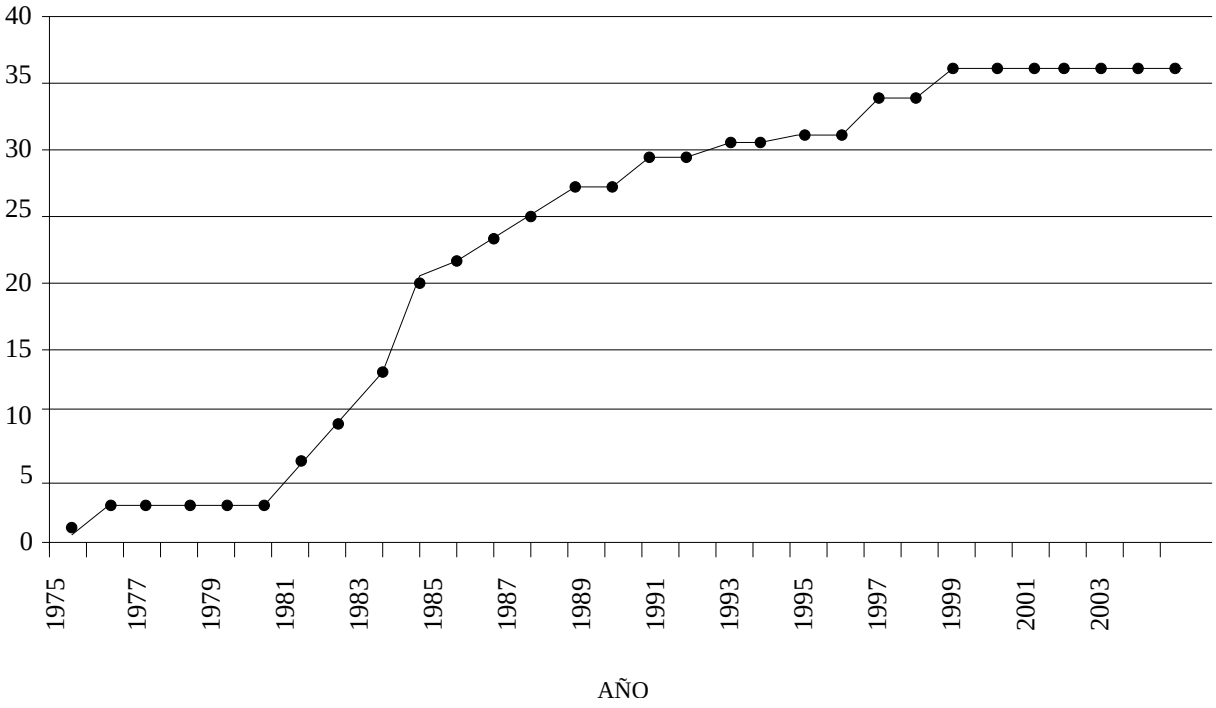


Figura 1.9: Número acumulativo de metodologías de HRA en función del año de publicación, Hollnagel (2005a).

Desde el punto de vista histórico, se puede dividir la evolución del estudio de la fiabilidad humana en cuatro fases, LaSala (1998):

1. Los orígenes del estudio de la fiabilidad humana, las décadas de los años 50 y 60.
2. Los desarrollos llevados a cabo por la US Navy entre principios de los 60 hasta finales de los años 70.
3. El periodo de alta intensidad de trabajo de la NRC de la década de los años 80.
4. El periodo de transición de la década de los años 90.

Fue en la etapa de los orígenes, en 1964, cuando se desarrolló la THERP de Swain (1963), metodología que se usa actualmente como parte de los estudios de seguridad de la industria nuclear y de la NASA. Esta metodología se desarrolló a partir de numerosos estudios realizados dentro de la defensa de los EUA, especialmente ligados al ejército del aire, para clasificar la fiabilidad humana en función de las tareas a realizar. En el segundo periodo, entre 1960 y finales de 1970, surgieron a la luz los trabajos realizados hasta el momento, y el apoyo de la US Navy

a su desarrollo contribuyó en gran medida a su aplicación en otros ámbitos, tal como ocurrió en la industria nuclear. Fue en esta época en la cual se realizó una de las primeras revisiones de los modelos para la estimación de la fiabilidad humana, Meister (1971). Con el accidente de TMI en 1979, la NRC tomó el relevo de la US Navy en el apoyo al desarrollo y la implementación de las metodologías de estudio de la fiabilidad humana. En 1983, la NRC adoptó la THERP como método de referencia para realizar los HRA, integrándolo en el PSA. Entre 1982 y 1983, la NRC se embarcó en un ambicioso programa de desarrollo de modelos y datos para los estudios que dio como fruto un elevado número de metodologías. Además, según avanzó la década, la NRC reconoció la necesidad de una buena base de datos de referencia para los estudios de HRA, creando la *Nuclear Computerized Library for Assessing Reactor Reliability*, Gertman et al. (1988).

Finalmente, en los años 90 se inició un periodo de maduración de estas metodologías y de esclarecimiento de líneas futuras de desarrollo, marcado por el trabajo de Haney et al. (1989). Como ya se ha comentado, autores como Swain (1990), Dougherty (1990), Lydell (1992) y Bley et al. (1992) establecieron la línea de salida para el desarrollo de nuevas metodologías, partiendo de las limitaciones de las desarrolladas hasta el momento. La mayoría de las críticas estaban dirigidas al uso excesivo de opiniones de expertos, a las deficientes metodologías HRA en uso y a la ausencia casi completa de la consideración de los factores de organización, estando muchas de ellas aún vigentes, Spurgin y Lydell (2002). Tras estos trabajos, se establecieron dos grupos en los que respecta a las metodologías de HRA desarrollas desde ese momento: las metodologías de primera generación o metodologías clásicas, y las de segunda generación, desarrolladas con la intención de mejorar dichas deficiencias.

En general, los métodos de HRA actuales se pueden clasificar considerando, Figura 1.10, Pyy y Andersson (1997), CSNI (1998), Sträter (2004), Kohlhepp (2005) y Forester et al. (2006):

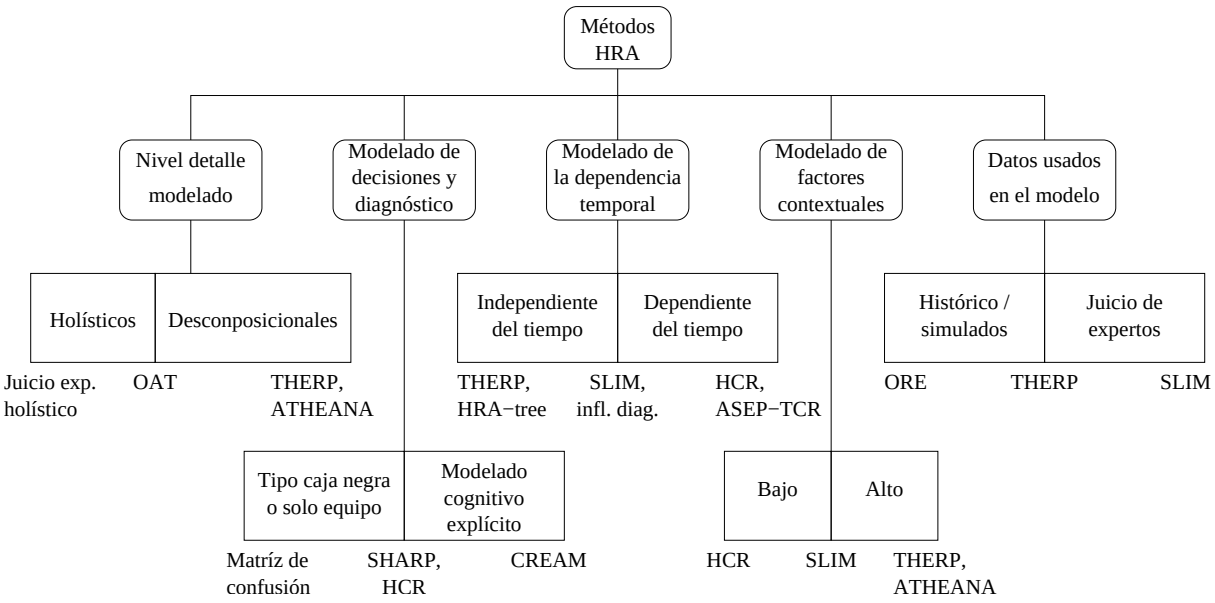


Figura 1.10: Clasificación de los métodos de HRA.

El nivel de detalle

Los métodos HRA se clasifican en holísticos y descomposicionales. Los métodos holísticos, como los basados en juicio de expertos, tienen como objetivo estudiar las actuaciones humanas como un todo, sin modelar aspectos del comportamiento humano. Por contra, los métodos descomposicionales, son métodos de detalle que descomponen las acciones humanas en tareas, considerando incluso los flujos de información internos del operador y sus procesos cognitivos. El modelo más usado en este último caso es el SRK.

Entre estos extremos, se sitúan métodos con niveles de detalle intermedios, como por ejemplo el caso de los árboles de acciones del operador (*Operator Actions Tree*, OAT), que dividen las actuaciones en detección, diagnóstico y acciones manuales.

Normalmente, el nivel de detalle en el tratamiento de las actuaciones humanas está relacionado con los datos disponibles o el objetivo del estudio en cuanto a la gestión del riesgo se refiere.

El tratamiento de los mecanismos cognitivos y de diagnóstico y toma de decisiones

Se puede distinguir entre los métodos de HRA que tienen por objetivo el estudio del efecto de las acciones humanas en la fiabilidad de sistemas, denominados métodos de caja negra, y los que tratan de explicar los mecanismos de fallo internos del hombre, es decir, los modelos cognitivos. Mientras que los métodos holísticos y de caja negra son aproximaciones parejas, los modelos cognitivos son una de las corrientes principales actuales de los HRA descomposicionales.

En el caso de los métodos denominados de caja negra se puede destacar el método de matrices de confusión, mientras que en el caso de los modelos cognitivos se encuadran algunas de las nuevas metodologías de segunda generación, como es el caso de CREAM.

El tratamiento de la dependencia temporal

Los modelos independientes del tiempo son apropiados para estudiar las acciones humanas anteriores al IE, ya que el tiempo disponible no es uno de los factores decisivos para el éxito de las actuaciones de mantenimiento y pruebas. La metodología THERP es un ejemplo de este tipo de estudios.

Por otra parte, los modelos dependientes del tiempo, como el TRC (*Time Reliability Correlation*, TRC), son los métodos que se emplean en el estudio de las actuaciones humanas en caso de que el tiempo disponible para realizarlas sea un parámetro determinante en la cuantificación de la probabilidad de fallo humano. Principalmente se aplican para las acciones posteriores al IE y, especialmente, cuando el tiempo disponible es reducido.

Otra aproximación para considerar el efecto del tiempo disponible es considerarlo como un factor del contexto y cuantificarlo mediante juicio de ingeniería, pudiéndose considerar SLIM-MAUD como una metodología de este tipo.

El tratamiento de los factores contextuales

En esta categoría se encuadran aquellas metodologías que realizan una caracterización del contexto en que se realizan las actuaciones considerando un conjunto relevante de factores contextules.

Dentro de este grupo, se pueden considerar aquellas que los consideran de forma implícita, como puede ser el caso del juicio de expertos, o de forma explícita, como por ejemplo SLIM o ATHEANA. La aplicación de los factores contextuales está fuertemente condicionada por la disponibilidad de fuentes de datos que respalden su estimación.

Las fuentes de datos empleadas para estimar la HEP

Esta clasificación es independiente del uso que se realice de los datos, para estimación directa de la HEP o de forma indirecta en los PSF, dependiendo exclusivamente de la naturaleza de los mismos. Así, por ejemplo, la metodología THERP trabaja con datos genéricos de fuentes múltiples. Otras fuentes de datos puede ser datos específicos de planta, datos obtenidos a partir de experimentos en simuladores o la experiencia operativa. En el caso de esta última, la calidad de los datos no es adecuada debido a la dificultad de clasificarlos y a que los esfuerzos en su recolección y estudio son raros.

Dentro de esta clasificación, y como ya se ha visto en el caso de los modelos cognitivos, encajan algunos de los denominados métodos de segunda generación, como ATHEANA, MERMOS, CAHR y CREAM. Actualmente no hay una definición clara del término HRA de segunda generación, aunque si se pueden distinguir dos corrientes en su conjunto:

- Los métodos cognitivos, representados por el método CREAM.
- Los métodos que hacen un uso extensivo de los factores contextuales. Dentro de este grupo se pueden destacar MERMOS y ATHEANA.

1.2.2.3 Importancia del PSA y del HRA en la evaluación del riesgo

Como conclusión final, y considerando la evolución histórica del uso del PSA y del HRA, desde el informe WASH-1400 hasta el ROP, se puede concluir que estas metodologías han ido adquiriendo cada vez más importancia, llegando a convertirse en un elemento de la toma de decisiones dentro de los procesos de mejoras en el diseño, la operación, el mantenimiento y la organización. Este hecho ha conllevado y conlleva cierta preocupación por la calidad las metodologías HRA, poniendo de manifiesto su importancia. Tal como ya se ha comentado en la introducción del capítulo, se ha llegado a determinar que entre el 15 y el 80 % de la CDF calculada en los PSA está relacionada con el fallo de alguna actuación manual por parte del operador, NEA (2004), dependiendo dicho peso porcentual de las consideraciones realizadas en el HRA, o dicho de otra forma, de la calidad del mismo. Además, considerando los resultados de

algunos estudios, se ve con preocupación la importancia del impacto de las actuaciones humanas en la cuantificación del CDF y el uso de las metodologías empleadas en su cuantificación, Forester et al. (2006),

Considerando la importancia de estas ideas, en el siguiente apartado y desde el punto de vista técnico, se comentará en detalle el carácter de la integración de las metodologías de HRA en el PSA, considerando la base de los procesos de cuantificación habituales en las metodologías de HRA.

1.2.3 Integración de las técnicas HRA en los PSA. Metodologías y evaluación.

El conjunto de actividades del personal de planta durante la operación de una central nuclear es muy amplio, realizando funciones de operación, mantenimiento, modificaciones y pruebas en diferentes partes de la instalación. Este tipo de actividades son las denominadas actividades primarias, o también acciones de línea frontal (*front line actions*), en las cuales el personal está directamente implicado en el desarrollo de los procesos y en las capacidades de los equipos disponibles. Las actividades secundarias serían aquellas relacionadas con la planificación, el diseño, la supervisión de las actuaciones primarias, por ejemplo. Se puede generalizar diciendo que las actuaciones primarias deben ser explícitamente modeladas en el PSA. El efecto de las actividades secundarias, también llamadas a veces influencias organizativas, suelen considerarse en el HRA usando los denominados factores de perfilado del comportamiento (*Performance Shaping Factors*, PSF), relacionados con los factores contextuales mencionados en el apartado anterior y que se explicarán en detalle más adelante en este apartado. Ejemplos de actividades secundarias son el entrenamiento, el control de calidad, la planificación del trabajo, la supervisión, las inspecciones, el análisis y la preparación de documentos de planta, incluyéndose en esta última categoría los documentos de apoyo para la gestión de emergencias, es decir, la disponibilidad y calidad de los EOP y las SAMG. En algunos casos, la influencia de factores secundarios puede ser significativa. Por ejemplo, las deficiencias en el entrenamiento o en los procedimientos pueden aumentar la probabilidad de fallo humano en situaciones críticas. Independientemente de la naturaleza de la actuación, el HRA tiene como objetivo la transformación de las acciones humanas en sucesos del PSA, estimando la probabilidad de fallo humano (*Human Error Probability*, HEP). Para estimar la HEP, no es solo necesario saber el número de errores registrados al realizar una tarea y la frecuencia de ejecución de dicha tarea, también hay que considerar las circunstancias bajo las cuales se realiza. Estas circunstancias relativas a la tarea deben compararse con los PSF de la tarea a cuantificar. De esta forma, se le asigna mayor relevancia a la estadística que presente PSF similares.

En un principio, solo las actuaciones humanas importantes son incluidas explícitamente en el PSA para no aumentar la complejidad del modelado sin necesidad. Ejemplos de estas acciones son

- Las acciones del operador necesarias tras un suceso iniciador, también denominadas **acciones post-IE** (*Initiating Event*). Las acciones del operador post-IE, como el arranque

manual de una bomba en una situación en la que la señal automática ha fallado, y la gestión del accidente afectan a la cuantificación del PSA de forma positiva. Normalmente, incluyen diferentes acciones para equilibrar el estado de la planta o para mitigar el curso de un accidente, ambas normalmente consideradas en las estrategias de gestión de emergencias, es decir, en los EOP o las SAMG. La consideración de este tipo de acciones en la cuantificación del PSA son el objeto principal del HRA.

- Por otro lado, las acciones que se contemplan antes del suceso iniciador, **acciones pre-IE**, son los mantenimientos planificados, las pruebas, la restauración de equipo defectuoso y las dependencias funcionales inducidas por humanos. La indisponibilidad debida a reparaciones de fallos no críticos debe estar explícitamente incluida en el modelo de PSA si se considera importante, mientras que la debida a fallos críticos generalmente se incluye en los parámetros fiabilidad de sistemas y componentes.

- Finalmente, se consideran las **actuaciones humanas que llevan al IE**, cuyo efecto debe ser considerado en las frecuencias de ocurrencia de los IE.

Para las acciones pre-IE y aquellas que causan el IE, su efecto se considera de forma implícita, por ejemplo, como parte de los parámetros de la fiabilidad de un componente o en las frecuencias de los sucesos iniciadores. Debido a que estos tipos de acciones se modelan desde el punto de vista del error, su consideración conlleva un impacto es negativo, y su omisión conlleva estimaciones optimistas.

Las acciones humanas se pueden clasificar a su vez de acuerdo con el papel que desempeñen en la actuación de un sistema. Se pueden distinguir dos casos:

- sistemas que carecen de señal automática de actuación, por lo que se requiere una actuación manual para su actuación,

- y los que presentan una señal de actuación automática, quedando la actuación manual del sistema como una opción de respaldo.

Debido a la alta fiabilidad de las señales de protección automáticas, las acciones manuales de respaldo tienen poca importancia en el PSA frente a la actuación de sistemas que dependen puramente de acciones manuales. Un caso especial de las acciones primarias de respaldo son las denominadas de recuperación. Las actuaciones humanas post-IE pueden ser consideradas como de recuperación si están dirigidas a la mitigación del efecto de los fallos propios o de otros, o incluso fallos de sistemas. La recuperación mediante actuaciones manuales solo es posible si se dispone del tiempo, recursos, herramientas y conocimiento requeridos. En este sentido, no suelen considerarse en el PSA su impacto positivo. Sin embargo, las actuaciones de recuperación que al fallar tengan un impacto negativo significativo deben ser implementadas.

1.2.3.1 Clasificación de las actuaciones humanas consideradas en el PSA

Partiendo de las diferentes clasificaciones conceptuales de las acciones humanas que se han presentado anteriormente, a continuación se comentará la **clasificación de las acciones humanas** más habitual dentro de los estudios de PSA, estableciendo tres categorías, Hannaman y Spurgin (1984) y CSNI (1998):

- **Categoría A** (Tipo 1): actuaciones humanas que tienen lugar antes del suceso que inicia el escenario, es decir, el IE. Los errores asociados con estas acciones producen que equipos en espera no estén disponibles para realizar su función tal y como se espera tras la ocurrencia del IE, denominándose **errores latentes**. También se puede dar la circunstancia de que mejoren la disponibilidad de sistemas por restauración de operabilidad de equipos tras pruebas o mantenimiento, y así se registra en la cuantificación del HRA para el PSA. Un ejemplo puede ser una válvula configurada en posición errónea tras ajustes o mantenimiento, pudiéndose dar su posicionamiento correcto en pruebas o actividades de mantenimiento posteriores.

- **Categoría B** (Tipo 2): actuaciones humanas que inician un escenario, también denominados como sucesos iniciadores inducidos por humanos. Son también conocidos como **errores activos**. Un ejemplo podría ser una fuga del primario por operación incorrecta de algún equipo.

- **Categoría C**: acciones realizadas por personal de planta tras el suceso iniciador. El personal realiza estas actuaciones en respuesta al escenario para corregir el transitorio y llevar la planta a un estado seguro. Estas acciones, las cuales también se denominan acciones dinámicas del operador[30], pueden estar guiadas por procedimientos o no estarlo.

  Para incorporar esta categoría de acciones en los análisis de PSA, ésta suele separarse en tres tipos diferentes:

  – **Categoría C1** (Tipo 3): acciones procedimentadas relacionadas con la seguridad. Estas acciones abarcan el éxito o el fallo al realizar acciones que se consideran en los procedimientos o que forman parte de reglas aprendidas por el operador como respuesta ante una secuencia accidental. En el espacio de fallos, estas acciones se suelen referir como **errores de omisión**.

  – **Categoría C2** (Tipo 4): acciones agravantes, también referidas como **errores de comisión**.

  – **Categoría C3** (Tipo 5): **acciones improvisadas de recuperación/reparación**. Incluyen la recuperación de equipamiento no disponible previamente o el uso de procedimientos no estandarizados para aliviar las condiciones del accidente. Estas acciones suelen realizarse en base a un conocimiento adquirido por entrenamiento. Para que tengan éxito requieren un diagnóstico correcto de la situación y la ejecución correcta de las actuaciones consideradas.

[30] Las actuaciones denominadas no dinámicas serían las clasificadas dentro de las categorías A y B.

		Base de la acción	
		Planeada	No planeada
Efecto	Favorable	C3	C4
	Desfavorable	C5	C6

Tabla 1.15: Subdivisión de las actuaciones del operador de categoría C, Sträter (2000).

Cabe aclarar que la subdivisión de las actuaciones de categoría C no es del todo consistente en la bibliografía. En IAEA (1992), por ejemplo, solo se consideran acciones erróneas planeadas por el personal dentro del tipo 4. En Hirschberg (1990), por otro lado, el tipo 4 abarca todas las acciones erróneas realizadas por el personal. Una reestructuración propuesta por Sträter (2000) de las diferentes subdivisiones de la categoría C lleva a distinguir entre actuaciones planeadas y no planeadas, Tabla 1.15.

1.2.3.2 Tratamiento en el PSA de los diferentes tipos de acciones

A continuación se realiza una exposición pormenorizada del tratamiento de los diferentes tipos de acciones en el PSA. Debido a la diversidad de fuentes consultadas y a la amplitud de opiniones y aspectos considerados, no se incluyen de forma explícita las referencias relacionadas con cada planteamiento. Sin embargo, cabe decir que algunas de las referencias clave empleadas han sido los PSA de plantas españolas, CSNI-PWG5 (1983), CSNI (1998), Sträter (2000), Pyy (2000), Hirschberg (2004), Sureda (2001abc).

Actuaciones de categoría A

Normalmente afectan a equipos y/o componentes, y por este motivo deben analizarse detenidamente en el modelo de fiabilidad de los sistemas para obtener así todas las dependencias de actuaciones humanas posibles. Su contribución a la probabilidad de fallo está incluida en la probabilidad de fallo del componente tecnológico, en otras palabras, desde el punto de vista de la fiabilidad humana, están indirectamente incluidas en la probabilidad de error de un suceso básico técnico.

Este tipo de acciones no se encuentran, generalmente, entre los contribuyentes dominantes al riesgo. En la mayoría de los casos las razones son el impacto positivo de la redundancia, la diversidad y la separación de los sistemas de seguridad en espera. Respecto al modelado, se puede decir que es directo, aunque puede complicarse al considerar acciones que lleven a fallos dependientes que puedan llevar a indisponibilidad de grupos de componentes. Debido a que se realizan gran cantidad de actividades de categoría A de forma regular, tal como mantenimiento y actividades de prueba, la experiencia de planta puede dar información al respecto de su tratamiento. Se pueden obtener datos cuantitativos de fallos en la calibración de instrumentación, fallos al posicionar válvulas correctamente tras la realización de pruebas y mantenimiento, y fallos de reconexión del suministro eléctrico tras el mantenimiento. Las estimaciones que se obtienen para el PSA

se someten a cierto juicio técnico, de hecho, la consideración del impacto de acciones de restauración de operabilidad perdida por error humano previo requiere de un conocimiento profundo de aspectos específicos de la planta, tales como procedimientos, diseño y control de procesos, implicando este tipo de consideraciones mayores incertidumbres en su implementación.

Actuaciones de categoría B

No se requiere, normalmente, que sean implementadas en el modelo, dado que su efecto está incluido en las frecuencias de ocurrencia de los IE. Por otra parte, las frecuencias de IE se pueden cuantificar sin problemas a partir de la experiencia operativa.

Actuaciones de categoría C

Representan el mayor reto en la cuantificación, siendo las fuentes de datos escasas debido principalmente a que los escenarios anormales o de emergencia raramente ocurren. Gran parte de la atención se ha depositado en las acciones procedimentadas, las de Tipo 3, que normalmente aparecen en las secuencias de accidente que dominan la cuantificación del riesgo de la planta. En general, las actividades Tipo 3 y 4 son básicamente acciones de operación que pueden considerarse a nivel de sistema, y por ello se deben implementar en los árboles de fallo de los mismos. En el caso particular de las acciones Tipo 4, son las más complicadas de tratar y normalmente son consideradas de forma limitada en los PSA, por ejemplo, los errores de comisión que no empeoran la condición de la planta son tratados como errores de omisión Tipo 3, y sus probabilidades son sumadas a las consideradas para los errores de omisión. Un segundo tipo de error de comisión se produce cuando el operador diagnostica correctamente el suceso pero escoge una estrategia que no esta optimizada para gestionarlo. Finalmente, la tercera clase de errores de comisión podría darse cuando la imagen mental de operador respecto al estado de la planta difiere del estado actual, conllevando la realización de acciones que el operador considera correctas pero aplicadas a la gestión del suceso equivocado. La identificación de los errores de comisión de clase dos y tres es difícil, y no se ha desarrollado ninguna metodología sistemática para ello. Sin embargo, algunos PSA los incluyen de forma puntual. Ejemplos de errores de comisión se pueden encontrar entre los LER, pero los datos existentes son insuficientes para realizar un estudio completo de los mismos.

Las acciones Tipo 5 son acciones de recuperación, que pueden afectar tanto a nivel de sistema como de componente. Suelen corresponderse con el conjunto de las actuaciones del operador que no están procedimentadas. Para este tipo de acciones hay fuentes de datos relativamente amplias. Por ejemplo, los tiempos de recuperación del suministro eléctrico exterior o los tiempos de reparación de componentes. Normalmente, estos datos requieren de juicio técnico[31].

[31] En los PSA españoles, este tipo de actuaciones no se suele considerar.

1.2.3.3 Cuantificación de la HEP para los diferentes tipos de acciones

En algunos casos, puede que el efecto de las acciones humanas de categoría A no estén consideradas en las probabilidades de fallos de componentes, o que las acciones humanas de categoría B no estén incluidas en las frecuencias de iniciación de los IE. Típicamente, este es el caso cuando las probabilidades de fallo de un suceso básico se determina con la ayuda de material de pruebas o si la frecuencia del IE se estima mediante el uso de árboles de error. En estos casos, la metodología THERP, Swain y Guttman (1983), sigue constituyendo una referencia base en la obtención de las HEP para estas acciones. Esta metodología dispone de datos para las HEP de acciones básicas que integradas bajo juicio de ingeniería, dan la HEP de las actuaciones consideradas. Estas HEP básicas se corresponden con diversas fuentes, no solo dentro de la ingeniería nuclear, y han sido adaptadas para su uso en las condiciones típicas de las centrales nucleares norteamericanas. Además, documenta la forma en que estas HEP pueden ser ajustadas mediante diferentes PSF y ofrece una guía para su integración en el PSA.

Para las actuaciones dentro de la categoría C, es decir, las actuaciones dinámicas, la disponibilidad de datos adecuados es muy limitada, tal y como se ha comentado, pudiéndose considerar:

- Datos obtenidos de los registros de operaciones reales de emergencia así como en sesiones de entrenamiento, siendo esta última fuente la más abundante.
- Datos respecto a los PSF se puede obtener en el entorno de trabajo por observación directa de las operaciones llevadas a cabo durante operación normal o mediante entrevistas y cuestionarios en todos los niveles de la organización.
- Los datos de las bases de datos de reportes de accidentes, incidentes y sucesos operacionales.

En el caso de que las fuentes de datos en su conjunto no sean suficientes para estimar de forma fiable la HEP asociada a una actuación se puede recurrir a las metodologías de HRA para su estimación. Cabe decir que el conjunto de metodologías disponibles actualmente es muy amplio, tal como se describió en el apartado anterior y en general la aplicación de los mismos de realiza desde enfoques mixtos en función del tipo de actuación considerada.

Cuantificar, en su conjunto, la totalidad de las actuaciones humanas demandadas durante el estudio de una secuencia es completamente inviable, y por ello se han diseñado metodologías que ayudan a determinar la importancia de las actuaciones y a realizar primeras aproximaciones a la cuantificación de la HEP asociada, de forma que se pueda determinar cuales requieren ser consideradas para un análisis más detallado e integrarlas en los árboles de fallo de sistemas o directamente en los cabeceros de los árboles de sucesos.

Por ejemplo, el EPRI ha desarrollado la denominada *EPRI HRA Calculator*, Forester et al. (2006), que conjuga las metodologías THERP, ASEP, HCR/ORE y CBDTM para estimar la HEP de los diferentes tipos de actuaciones. El principal objetivo de esta herramienta es permitir obtener resultados consistentes entre distintos analistas, eliminando factores que introduzcan

subjetividad en el estudio de HRA. Por otro lado, se puede destacar el uso de técnicas de aplicación de las metodologías de HRA, como por ejemplo la técnica SHARP, Hannaman y Spurgin (1984), que se apoya en las HRA THERP y TRC para realizar la cuantificación detallada de las HEP de las acciones definidas como relevantes. Debido a que esta última metodología es una de las más usadas en la realización del HRA de las centrales nucleares, se han considerado THERP y TRC como las más adecuadas para ilustrar como se realiza la cuantificación de la HEP en el HRA.

Ejemplo de cuantificación de la HEP de las acciones Tipo 1 con la metodología THERP.

La metodología THERP, Swain y Guttman (1983), es la técnica más antigua y más utilizada en fiabilidad humana. Las etapas del THERP son similares a las propias de los análisis de fiabilidad de sistemas, excepto en que las actividades humanas sustituyen a los equipos y componentes. Los pasos a realizar son:

- Definición de los fallos de interés del sistema.
- Lista y análisis de las operaciones humanas requeridas.
- Estimación de las probabilidades de error relevantes.
- Estimación de los efectos de los errores como sucesos de fallo del sistema.
- Cambios al modelo y posible recuantificación.
- Documentación.

En nuestro caso nos centraremos en los pasos de análisis de las operaciones humanas requeridas y de la estimación de las probabilidades de error (HEP), ya que el resto de los pasos tienen una carga considerable de juicio de ingeniería y no son ilustrativos dentro de los objetivos del presente trabajo.

Para la realización del paso relativo al análisis de las operaciones humanas, la metodología THERP parte de una taxonomía del error que considera los errores de selección (selección del control erróneo, elección de procedimientos de forma incorrecta), en la secuencia (acciones llevadas a cabo en orden incorrecto), temporales (acciones llevadas a cabo muy pronto / muy tarde) y cualitativos (acción realizada en mucho / en poco). En función de esta taxonomía realiza el análisis de actuaciones humanas considerando los posibles fallos. Dentro de las fuentes de acciones humanas se consideran los procedimientos de operación normal, fallo y los de emergencia, para detectar posibles errores que puedan llevar a cabo los operadores a nivel de componentes del sistema.

Para la cuantificación de los árboles de sucesos de fiabilidad humana, a parte del proceso de establecimiento del conjunto de actuaciones de interés y los posibles fallos asociados llevado a cabo en el paso anterior, se requiere realizar la estimación de la probabilidad de ocurrencia de dichos fallos. Para ello, en el capítulo 20 de la THERP se da una base de datos que contiene la información necesaria para realizar esta tarea. Un ejemplo del tipo de información incluida en dicha base de datos se muestra en la Tabla 1.16.

ÍTEM	TIPO DE OPERACIÓN DE COMPROBACIÓN[a]	HEP
1	Verificación de tareas rutinarias utilizando material escrito (incluye inspecciones, verificación del posicionamiento de válvulas operadas localmente, interruptores, circuitos, conectores, etc., y verificaciones de listados escritos, etiquetados, o exactitud de los procedimientos)	0,1
2	Lo mismo que en el item 1, pero sin material escrito.	0,2
3	Verificación especial en corto plazo con factores de alarma.	0,05
4	Verificaciones que requieren participación activa, como son realización de medidas especiales.	0,01
Dada la verificación de posición de una válvula accionada localmente (ítem 1), advertir que no está completamente abierta o cerrada (items 5, 6 y 7):		0,5
5	Indicador Posición[b], solo.	0,1
6	Indicador de Posición[b] y un registrador con poca precisión.	0,5
7	Ni indicador ni registrador.	0,9
8	Comprobación por un operario de la tarea llevada a cabo por un equipo de dos personas, o comprobación por un segundo operario, tarea de rutina (se da crédito a no más de dos operarios).	0,5
9	Comprobación del estado de un equipo si su estado afecta la seguridad de la persona que comprueba.	0,001
10	Comprobación por un operario del cambio o restablecimiento de tareas realizadas por un operario de mantenimiento o tareas muy específicas de chequeo.	HEP/2[c]

[a]Esta tabla aplica a casos en operación normal en condiciones en las que una persona comprueba el trabajo llevado a cabo por otros, mientras se realiza la tarea o después de acabada.

[b]Un indicador de posición incluye una escala que indica la posición relativa de la válvula a completamente abierta o completamente cerrada. Un registrador de poca precisión establece la posición de la válvula en una escala asociada.

[c]HEP de los apartados de la tabla dividido por dos. Se trata de comprobaciones realizados expresamente por otro operador, o cuando una persona de operación revisa una tarea realizada por una persona de mantenimiento, que siempre lo hace con una atención especial.

Tabla 1.16: Ejemplo de aplicación de la metodología THERP: probabilidades estimadas de que un controlador falle en detectar errores cometidos por otros.

Una vez cuantificadas las actuaciones humanas consideradas, se deben incluir los errores humanos resultantes del paso de análisis en el modelo del sistema, normalmente en los árboles de fallos, con las HEP estimadas como probabilidad de fallo asociada a los mismos, corregidas mediante los PSF considerados.

Ejemplo de la cuantificación de la HEP de las actuaciones Tipo 3, 4 y 5 empleando las metodologías THERP y TRC.

Las acciones humanas de categoría C se componen de una parte cognoscitiva y una parte manual, Figura 1.11. La parte cognoscitiva evalúa la probabilidad de error de no realizar la acción o de no hacerla en el tiempo disponible, P_c. La parte manual representa la probabilidad de error humano en la realización física de la acción, P_m. La cuantificación de la probabilidad de error se realiza mediante la metodología TRC, Hall et al. (1982), para la parte cognoscitiva y la metodología THERP para la manual.

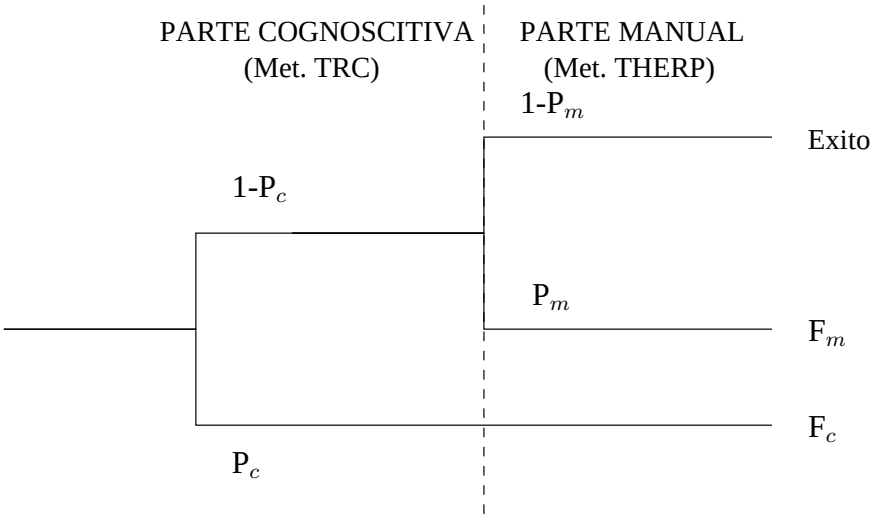


Figura 1.11: Ejemplo de cálculo de la HEP de una acción humana Tipo 3 en la técnica SHARP.

La metodología TRC se basa en suponer que, en este tipo de situaciones, la disponibilidad de tiempo para la diagnosis y toma de decisiones es el factor fundamental del éxito en el inicio de la respuesta adecuada por parte del operador ante una situación anormal o de emergencia. Es importante tener en cuenta que se considera que una acción humana posterior al IE está dominada por el tiempo, y por tanto se podrá aplicar el modelo TRC, si el tiempo disponible para la realización de la acción es inferior a una hora.

Para la estimación de P_c, en la metodología TRC existen dos pares de curvas, Figura 1.12:

- Un par se aplica a los errores basados en reglas, por ejemplo en procesos de diagnosis incorrectos, mala previsión o toma de decisiones incorrectas en el seguimiento de las reglas, p. ej. los procedimientos, empleando una de las curvas cuando no hay ambigüedad, y la otra cuando la toma de decisiones se realiza bajo dudas. Este tipo de acciones se corresponden con los Tipos 3 y 4.
- El segundo par de curvas se utiliza cuando la diagnosis se realiza con ausencia de reglas, este es el caso de acciones de recuperación que se realizan después de un incidente y que además no están procedimentadas. Las acciones consideras son las clasificadas como Tipo 5.

Una vez estimado el tiempo disponible para la acción, se puede calcula el valor de P_c a partir de dichas curvas. El valor específico para la acción considerada estará condicionado por el valor de los PSF incluidos en el modelo de acción desarrollado.

Para la parte manual, el valor de P_m se obtiene aplicando la metodología THERP, empleando el proceso descrito en el apartado anterior, y empleando el mismo tipo de tablas, Tabla 1.16.

Finalmente, y de esta forma, la HEP para este tipo de acciones vendrá dada por,

$$HEP = P_c + (1 - P_c) \cdot P_m$$

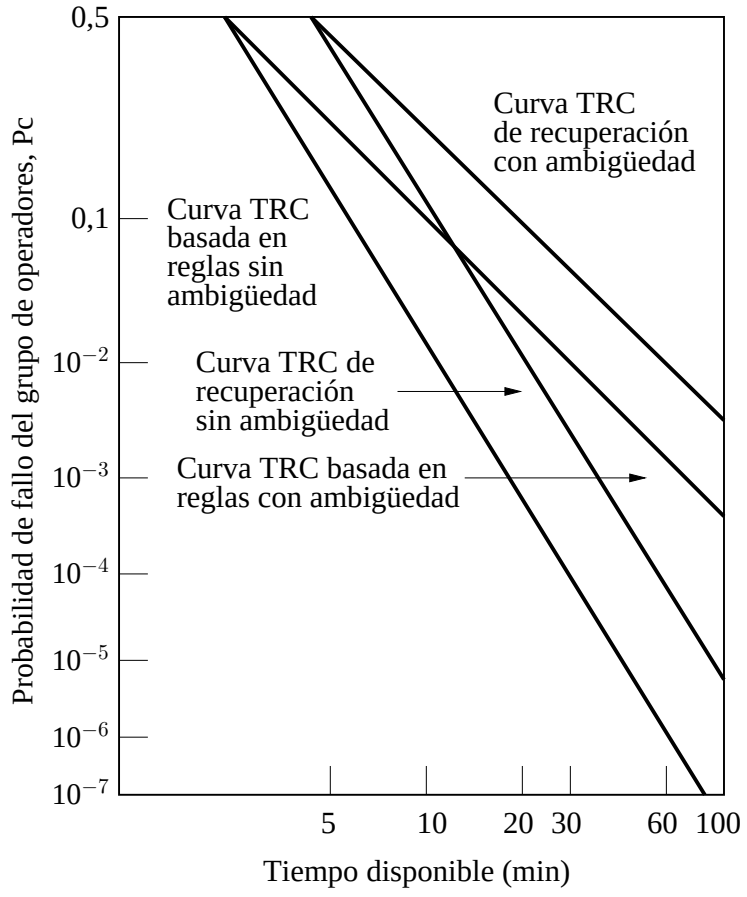


Figura 1.12: Curvas de cálculo de la HEP empleadas en la metodología TRC.

1.3 Necesidad de una nueva metodología para la evaluación de los procedimientos de operación en la gestión de accidentes de centrales nucleares

El interés del estudio de los procedimientos en el ámbito de los estudios de seguridad ha conllevado la consideración de los mismos en la evaluación de la seguridad de las plantas de formas muy diversas, dependiendo del grado de integración de las tecnologías disponibles en el momento y de las tendencias en el tratamiento de la problemática del factor humano en la gestión de emergencias. En este sentido, se pueden diferenciar tres grupos:

1. La integración de los procedimientos en los sistemas de simulación de la planta, considerando puntualmente actuaciones del operador e implementándolas en el fichero de entrada de parámetros del código de simulación. Esta aproximación se corresponde con la integración de las actuaciones del operador como condiciones de contorno del modelo del sistema físico, siendo una de las opciones para el estudio de las actuaciones del operador y su impacto en la gestión de emergencias. Generalmente, este tipo implementaciones tiene su rango de aplicación los PSA de nivel 1 y 2, y otros estudios de evaluación de la seguridad, siendo la base de simulación de la mayoría de los PSA actuales. Un ejemplo de implementación más elaborada pero basada en los mismos principios se puede encontrar en Hardy et al. (1994).

2. Estudios de evaluación de los procedimientos considerando los aspectos relacionados con factores humanos y considerando o no el impacto en el sistema físico. Las metodologías empleadas son diversas, aunque la mayoría se caracterizan por trabajar sobre abstracciones de los procedimientos empleando metodologías muy variadas como, por ejemplo, las de tipo objetivos y metas, Hollnagel (1996) y Qin y Seong (2005), o las basadas en redes de Petri, Lee y Seong (2003).

    - En el caso de los estudios que **no consideran** el impacto de los procedimientos en el sistema físico, la finalidad de los trabajos es localizar deficiencias en el diseño de procedimientos desde el punto de vista de los factores humanos, principalmente centrados en aspectos cognitivos: problemas de interpretación en los procedimientos, excesiva carga cognitiva, etc, Jung et al. (2001), Park et al. (2001 2002 2004ab).
    - Sin embargo, para el caso de los trabajos que **consideran** el impacto en el sistema físico integrando en el simulador de procesos un modelo de procedimientos, el objetivo consiste en evaluar la interacción de estos mecanismos y aspectos cognitivos con el proceso físico del sistema durante un transitorio, cuando se acopla el modelo de procedimientos desarrollado a un simulador con un modelo del sistema físico. Durante la realización de estos estudios, el grado de abstracción de los procedimientos que se alcanza puede llegar a ser muy elevado, llegando a reducir el conjunto de procedimientos a grupo de objetivos operacionales y de tareas a desarrollar para alcanzarlos. A su vez, se establecen jerarquías y condiciones relacionales entre los

objetivos operaciones, llegando a desarrollar sistemas expertos y de conocimiento que simular los procesos de decisión del personal de la sala de control, Schryver (1988), Chandrasekaran et al. (1991), Cacciabue (1997ab), Cacciabue et al. (1992), Jakubowski y Beraha (1996), Mosleh y Chang (2004) y Lee y Seong (2004). Estas herramientas y metodologías de evaluación de los procedimientos suelen estar relacionadas con las denominadas metodologías de HRA de segunda generación.

3. Los trabajos de computerización de procedimientos con la finalidad de implementarlos como sustitución de los procedimientos en papel o como herramienta de apoyo a los mismos en la sala de control o en simuladores de entrenamiento, Chang et al. (1995) y Niwa y Hollnagel (2002), Niwa et al. (1996). En este tipo de trabajos se suele evaluar la experiencia operativa relacionada con el empleo de los procedimientos clásicos y se identifican problemas y limitaciones. El objetivo final es diseñar un sistema de procedimientos computerizado (*Computerized Based Procedures*, CBP) que sustituya, mejore y amplíe la funcionalidad de los procedimientos clásicos. Los CBP se evalúan desde el punto de vista de la ergonomía y los factores humanos, con la finalidad de realizar diseños optimizados para su empleo en emergencias minimizando la carga de trabajo y favoreciendo el SA y la capacidad de diagnóstico del personal de la sala de control, O'Hara et al. (2000ab). En estos trabajos no se realiza un modelo de los procedimientos, sino que se lleva a cabo una implementación nueva de los mismos.

4. Aproximaciones a la computerización de la ejecución de las acciones contempladas en los EOP y consideración de su implementación en planta. Un ejemplo de este tipo de trabajos es Husseiny et al. (1989), existiendo referencias más recientes.

Los estudios realizados dentro de los grupos tercero y cuarto quedan fuera del alcance de este trabajo, teniendo más relación los considerados en los dos primeros grupos.

Históricamente, la evaluación del factor humano en los PSA se ha realizado con metodologías del grupo uno. Estas metodologías presentan tres limitaciones relevantes:

- La consideración completa del conjunto de las actuaciones del operador suele conllevar la realización de una carga de trabajo de ingeniería a veces excesiva en la simulación de las secuencias.

- No se corresponden con procedimientos sistemáticos, lo que implica que la realización de un estudio de forma reproducible es limitada.

- Carecen de versatilidad y el alcance de las mismas es limitado. Este último aspecto se debe principalmente a la complejidad de los transitorios en los cuales se considera la interacción entre el proceso y las actuaciones humanas. Entre los factores que aumentan la complejidad de la simulación son los aspectos cognitivos los que tienen mayor importancia.

Tras estas metodologías surgieron los trabajos relacionados con metodologías cognitivas del HRA, consideradas en el segundo grupo, desarrollando modelos de operador integrados con simuladores de procesos. Estas aproximaciones se caracterizan por su alto grado de complejidad en el modelado de los aspectos cognitivos y fuertes limitaciones en el modelado del proceso, pudiendo excluir de esta última limitación a la herramienta ADS. Ambos aspectos implican grandes incertidumbres en sus aplicaciones, lo que las hace, hoy por hoy, poco aplicables en los estudios de ingeniería, siendo aún herramientas en desarrollo y validación.

En el ámbito internacional, la mayoría de las herramientas desarrolladas o en fase de desarrollo se orientan a la evaluación y diseño de MMI (p. ej. SRG Hollnagel et al. (1992), OASYS Chang et al. (1995) o MIDAS Corker y Sinith (1993)) o la evaluación de factores humanos y aspectos cognitivos del operador (p. ej. FAME Hollnagel y Bye (2000), INTEROPS Schryver (1988), SYBORG Sasou et al. ((1996), CAMEO Fujita et al. (1993) y COSIMO Cacciabue et al. (1992)). Sin embargo, son pocas las herramientas orientadas a la evaluación predictiva del efecto de la consideración de los EOP en la simulación de procesos y su integración en los PSA (p. ej. NORMAT Hardy et al. (1994), CES Woods et al. (1987) y ADS-IDAC Hsueh y Mosleh (1996), Macwan et al. (1991), Mosleh y Chang (2004)), objetivo final del desarrollo del simulador integral, cuando se incorpore en la metodología ISA, Sección 7.4.2.

En cuanto a la herramienta NORMAT, Hardy et al. (1994), es un desarrollo comercial del EPRI del cual no existe prácticamente fondo bibliográfico. Esta herramienta se basa en la integración del código MAAP acoplado a un modelo de EOP y un modelo de operador basado en una base de conocimiento con un sistema experto que simula los mecanismos de toma de decisiones. El carácter probabilístico de la simulación en lo que respecta a las actuaciones humanas se consigue mediante una implementación de la metodología HCR para la estimación del tiempo de respuesta y la probabilidad de fallo del operador en el tiempo disponible. La herramienta permite la simulación de secuencias al estilo del PSA, sin embargo, cabe constatar que es una aproximación pionera al concepto de integración de los EOP en las simulaciones de procesos orientada al PSA y que muchas de las especificaciones están obsoletas y no son consideradas dentro de las líneas de trabajo planteadas para el simulador integral TRETA/COPMA-III.

Considerando las herramientas CES y ADS-IDAC, se pueden extraer las siguientes ideas:

- Presentan modelos avanzados de simulación cognitiva del operador, permitiendo simular la mayoría de los aspectos considerados en los análisis de HRA actuales y de segunda generación, tales como los EoC, SA, toma de decisiones, etc.
- La integración de un modelo de EOP en CES se estaba evaluando, Roth et al. (1994), integrándolo en el modelo cognitivo que emplea, denominado EAGOL (Pople et al. (1994)), aunque no hay referencias que constaten que se haya llevado a cabo. El grado de implementación de los EOP en la herramienta ADS-IDAC parece corresponderse con una abstracción a nivel de objetivos y tareas de los procedimientos, no siendo una implementación estricta de un modelo de procedimientos y si más bien una base de conocimiento con un conjunto de reglas para la toma de decisiones y la realización de acciones.
- CES y ADS-IDAC tienen interfases de comunicación que les permiten acoplarse con simuladores de procesos avanzados. En el caso de CES no hay referencias de dichas

aplicaciones. La herramienta ADS-IDAC lleva integrada en el módulo ADS una versión del simulador RELAP5, con mejoras relacionadas con la posibilidad de realizar cálculo paralelizado.

Cabe aclarar, que en este estudio se han considerado otras aproximaciones a la evaluación de los EOP en la gestión de emergencias, pero por diferir en sus objetivos de forma significativa a los planteados en este trabajo no se incluyen de forma detallada, a saber:

- La herramienta OPSIM, Dang (1996), es un prototipo actualmente fuera de desarrollo. Se caracteriza por tener un modelo cognitivo del operador de nivel medio y un modelo de procesos prácticamente sin desarrollar, con una implementación adhoc de un modelo de físico cuyo alcance de simulación se limita a las secuencias de de pérdida del RHRS.
- Herramientas e implementaciones similares pero sin aplicación dentro del ámbito del PSA, p. ej. EOPAS Jakubowski y Beraha (1996), ATOPS Lee y Seong (2004) y SCOOPE/SIPA Chatry y Poizat (1999).
- Herramientas cuya orientación es la aplicación en el PSA pero no son lo suficientemente versátiles o no incluyen modelos de EOP de la naturaleza en que se ha considerado en este trabajo, p. ej. Miao et al. (1997) y DETAM (DYLAM) Chao y Chang (2000).
- La aproximaciones a la evaluación de EOP basadas en análisis de objetivos y tareas o mediante abstracciones funcionales de los mismos, p. ej. Hollnagel (1996), Lee y Seong (2003) y Qin y Seong (2005).
- Las herramientas denominadas *What if?*, basadas en el análisis predictivo de consecuencias en la toma de decisiones, p. ej. CAMS Owre (2001).

La conclusión más relevante de la revisión de los trabajos realizados a nivel internacional, considerando la afinidad con los objetivos considerados en este trabajo, es que la mayoría de ellos presentan modelos cognitivos bastante evolucionados, con unas especificaciones de diseño orientadas a cubrir las necesidades de simulación de las metodologías de HRA tanto de primera generación como de segunda generación. Estas implementaciones se basan en versiones computacionales de los modelos cognitivos discutidos en este capítulo, correspondiéndose la mayoría a versiones mixtas de las diferentes aproximaciones.

En este trabajo, y habiendo destacado la importancia de los EOP en la gestión de emergencias y su integración en los estudios de seguridad para la cuantificación del riesgo de las instalaciones, se pretende desarrollar una herramienta para la evaluación de los EOP de centrales nucleares con los siguientes objetivos:

- Análisis de la estructura de los procedimientos para detección de deficiencias en estructura y formato. Además, como objetivo derivado, puede analizarse la sintaxis y semántica utilizada valorando su adecuación y niveles de estandarización, así como los pasos donde se exige una transición y elección de alternativas al operador, etc., que pueden ser causa manifiesta de dificultad para el operador en el control adecuado de los transitorios de la planta.

- Conexión del sistema con modelos de planta para la simulación de transitorios y accidentes en los que se deba utilizar procedimientos de operación de emergencia.
- Utilización como herramienta auxiliar en tareas de formación de personal y, especialmente, en formación y licenciamiento de operadores y supervisores de centrales nucleares.

Habiendo considerado estos objetivos, el resultado del trabajo consiste en una herramienta de simulación de uso sencillo e inmediato, en contra de las nuevas tendencias, complejas y cuyo alcance está aún sin evaluar, que permita un estudio cuantitativo del impacto de las actuaciones del operador en las secuencias de accidente.

Al no haberse planteado el desarrollo de un modelo cognitivo dentro de los objetivos iniciales del trabajo, este aspecto se trata como un desarrollo futuro para la mejora de la herramienta, y de hecho así se describe en la Sección 7.4.2, teniendo en cuenta la posibilidad de expandir el alcance de la metodología ISA para que abarque el HRA.

Capítulo 2

Descripción de una nueva herramienta para la simulación integral de secuencias de accidente en centrales nucleares de agua ligera

Índice

Las secuencias accidentales comienzan en operación normal, tanto en modos de potencia como en parada. En las primeras etapas, especialmente cuando la secuencia comienza desde operación a potencia,el comportamiento de la planta está caracterizado por la actuación automática de un elevado número de sistemas y un comportamiento global dominado por la actuación de los sistemas de control. Normalmente, los procesos físicos tienen lugar dentro de sus condiciones óptimas de diseño, pudiéndose realizar una serie de aproximaciones e hipótesis en el modelado del sistema. La preocupación principal de la simulación de estas etapas, en lo que respecta al simulador de procesos, es considerar todas las interacciones entre los sistemas y procesos implicados. Cuando el accidente está ya iniciado y ha progresado, la cuantía de sistemas en interacción con el proceso es significativamente inferior, pero la complejidad fenomenológica es, generalmente, mucho mayor. Sistemas que en operación normal estaban en espera o en modos pasivos actúan, y nuevos procesos con fenomenologías específicas son importantes desde el punto de vista de la evolución de la secuencia. Por ello, los requerimientos para los modelos de simulación son, en varios aspectos, muy diferentes respecto a los empleados en operación normal. Algunas de las hipótesis y aproximaciones realizadas no son aplicables pero, en algunos casos, pueden ser posibles otras simplificaciones. El comportamiento global de la planta está principalmente dominado por la fenomenología de la secuencia y las actuaciones de protección tanto automáticas como manuales. De acuerdo con las necesidades de simulación descritas, para cubrir todas las etapas de las secuencias accidentales, el modelo de simulación debe cumplir una de las siguientes condiciones:

- Ser lo suficientemente detallado como para cubrir todas las situaciones consideradas.
- Emplear diferentes modelos en cada situación, garantizando que la transferencia entre los modelos se realiza de forma gradual y consistente.

La primera solución demanda capacidades de computación elevadas debido a que suele implicar que el modelo de máxima complejidad se emplea en todas las etapas de la simulación. Sin embargo, la segunda aproximación es mucho más conveniente para los objetivos del presente trabajo, ya que demanda capacidades de computación mucho menores y permite el uso de modelos simplificados para situaciones específicas.

Por otro lado, en lo que respecta a la consideración de las actuaciones del operador, su simulación se suele realizar mediante el uso de condiciones de frontera del modelo de sistema definido en en fichero de entrada del código. Uno de los inconvenientes de esta implementación de las actuaciones humanas, es que requiere de varias ejecuciones de cada secuencia para poder establecer cual es la distribución temporal de las actuaciones del operador. Así, según aumenta el número de posibles actuaciones, las modificaciones del fichero de parámetros del modelo adquiere mayor complejidad, llegando a ser impracticable su implementación.

En este sentido, cabría la posibilidad de implementar las actuaciones humanas en la simulación de forma interactiva, considerando el estado puntual del proceso de simulación. Una solución posible, consistiría en una interfaz de usuario interactiva que permitiese actuar sobre el código de simulación del sistema de la misma forma que en el sistema real, es decir, tal como lo hace

un operador sobre la planta. Para esta implementación, no es necesario computerizar los procedimientos, aunque sí sería deseable. Este método de simulación es adecuado para una gran variedad de aplicaciones, pero tiene dos deficiencias relevantes para los objetivos del presente trabajo. Por un lado, la imposibilidad de disponer de resultados reproducibles, ya que el momento en que cada instrucción es ejecutada está sujeto a incertidumbres que tienen su origen en el comportamiento humano. Por otro, la necesidad de realizar las simulaciones en tiempo real conllevaría que en la mayoría de los casos conllevasen tiempos de simulación prohibitivos para las aplicaciones que son de interés para el presente trabajo.

Por ello, una propuesta para implementar un simulador de procesos conjuntamente con un sistema de ejecución de procedimientos computerizados, consiste en un modelo de operador automático que sea capaz de decidir acerca del seguimiento y ejecución de las acciones consideradas en los procedimientos de la planta. Este método permite un análisis sistemático de los efectos de la ejecución de las acciones consideradas en los procedimientos en la evolución del estado de la planta.

Como conclusión, se definen dos elementos constituidos por un modelo del sistema físico y un modelo de las actuaciones humanas aplicables a la situación, que en una central nuclear, se corresponden con los procedimientos de operación de la misma. Ambos modelos requieren de códigos específicos de simulación, diseñados de forma separada y consistente cada uno con sus requerimientos. El carácter diferenciado o modular de ambos códigos presenta las ventajas de permitir la simulación de ambos elementos por separado, pudiéndose realizar diferentes implementaciones de ambos códigos de simulación en cualquier tipo de plataforma. Además de mantenerse la funcionalidad de simulación de ambas herramientas por separado, se debe garantizar que de forma integrada conjugan sus capacidades para llevar a cabo simulaciones integrales. En este sentido, se hace necesaria la definición de una interfaz de comunicaciones que permita establecer una consistencia completa entre la información gestionada por ambos procesos, en lo que respecta a los modelos de planta y procedimientos, y al intercambio de actualizaciones de dicho estado, considerando variables físicas, de proceso, de estado de componentes o sistemas o de parámetros de modelos matemáticos que, teniendo su origen en uno de los modelos, afecten a la simulación que lleva a cabo otro código externo sobre otro modelo de alguno de los elementos, en este caso, los procedimientos.

La implementación escogida en el presente trabajo se ha realizado considerando como código para la simulación del modelo de planta el código TRETA de simulación de reactores de agua a presión, que se explica en detalle en la Sección 2.1. Este código, por sus especificaciones de diseño, presenta un alto grado de funcionalidad de comunicaciones y de versatilidad en la implementación de modelos para la simulación. Por otro lado, para la simulación de los procedimientos de operación se ha escogido el código COPMA-III desarrollado por el HRP que, tal como se explicará en la Sección 2.2, cumple con los requerimientos establecidos en este capítulo. Para la integración de ambos códigos, se ha realizado un estudio de las diferentes posibilidades y, de forma resumida (explicándose en detalle en el Capítulo 5), se exponen los motivos para la solución adoptada en la Sección 2.3, relacionada con el uso de la librería de comunicaciones SWBus desarrollada por el HRP.

Resumiendo, los códigos de simulación que constituyen la plataforma de simulación integral,

en su implementación final son, Figura 2.1:

- Un código de simulación de transitorios, en nuestro caso se emplea el código TRETA, Izquierdo (1987), orientado a la simulación de centrales de agua a presión (*Presurized Water Reactors*, PWR). La implementación del código TIZONA, Queral et al. (1999), orientado a las centrales de agua en ebullición (*Boiling Water Reactors*, BWR), en el simulador integral es inmediata al presentar especificaciones de diseño idénticas a las del código TRETA. Ambos códigos son modulares, están codificados en C y Fortran, y han sido desarrollados por el CSN y el DSE-UPM.
- El sistema de procedimientos computerizados COPMA-III, Bisio et al. (2005), codificado en Java y desarrollado por el OECD-HRP. Durante la realización de este trabajo, COPMA-III ha sido adaptado para la simulación automática de procedimientos por el grupo de desarrolladores del HRP.
- La interfase de integración de ambos códigos de simulación, desarrollada mediante el uso de la librería de comunicaciones SWBus, HRP (2002a).

En las siguientes secciones se explicará en detalle la funcionalidad de los diferentes elementos, detallándose los modelos de planta, procedimientos y funcionalidad de la interfase de integración de los códigos en los Capítulos 3, 4 y 5, respectivamente.

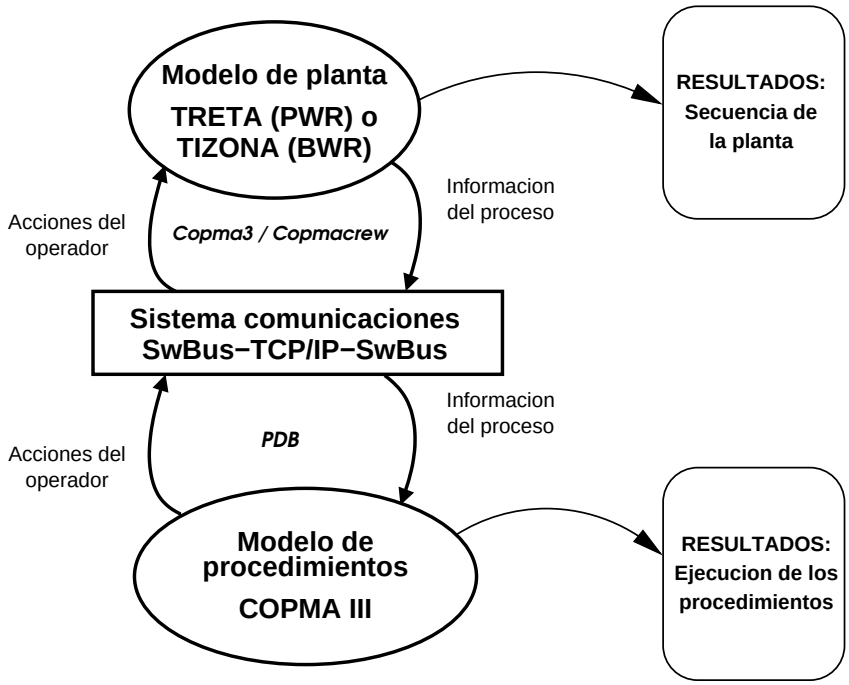


Figura 2.1: Esquema de la aplicación integral TRETA/COPMA-III.

2.1 Código de simulación de sistema dinámicos TRETA

TRETA (*Transient REsponse and Test Analiser*), es una herramienta de simulación diseñada y desarrollada por el CSN. Orientada principalmente a la simulación de centrales nucleares, su estructura modular permite su uso para la simulación genérica de sistemas físicos. Está diseñado para capacitar al usuario en la realización de modelos sencillos de simulación de sistemas mediante una implementación rápida de modificaciones y cambios en los parámetros del modelo.

Desde el punto de vista de la arquitectura del código, se pueden destacar dos elementos clave:

- El *driver* capaz de resolver la red de bloques que constituyen el modelo y los modelos numéricos. El *driver* se encarga de la gestión de los parámetros de entrada, la simulación temporal del problema, el cálculo secuencial de los bloques del modelo del sistema para cada instante, la gestión de las realimentaciones y el almacenamiento y gestión tanto parcial como final de la información de salida generada en la simulación.
- El catálogo de módulos que permiten al usuario definir, con diferente nivel de detalle, el conjunto de operaciones a realizar en cada bloque del sistema.

Una característica relevante de TRETA es su capacidad de ser acoplado, en un esquema de simulación temporal discreta, con otros programas, permitiendo la simulación distribuida. Hay ejemplos de esta versatilidad, Meléndez (1992) e Izquierdo et al. (1994), siendo este trabajo uno de ellos.

Considerando la complejidad y el grado de detalle de los modelos de simulación para describir los procesos y sistemas de centrales nucleares, durante el desarrollo del código TRETA se han considerado como referencia aquellos modelos empleados por los suministradores de centrales nucleares y sus códigos de licenciamiento. De hecho, algunos de los modelos usados en el código se han inspirado en ellos. Una descripción sucinta de los modelos específicos del código se da en la Sección 2.1.3.

2.1.1 Definiciones de los elementos de modelado del código TRETA

En este apartado se definen el conjunto mínimo de conceptos que integran tanto la herramienta de simulación como los modelos que se desarrollen para la misma, Figura 2.2.

Driver Se define como el conjunto de subrutinas que gestionan el flujo de cálculo para llevar a cabo la simulación del sistema modelado.

Módulo Es el elemento básico para la construcción del modelo. Un modulo consiste en código escrito (compuesto de una o más funciones o subrutinas), asociada a un solo tipo de definición de tratamiento de la señal. Puede representar tanto como una parte física del sistema o una herramienta matemática.

Bloque Es el conjunto constituido por un módulo y su papel estructural en el modelo del sistema, también llamado éste último como la información topológica. Esta información se compone de, Tabla 2.1: el título, el número de indentificación del bloque, las conexiones de entrada, la información de gestión de realimentaciones, etc.

Topología Es el conjunto de conexiones entre los bloques con el orden de cálculo estipulado, y las posibles desviaciones de este orden, es decir, las realimetaciones.

Rama Es el medio de transferencia de información entre los bloques. Cada rama tiene un número de identificación único. Un bloque tiene tantas ramas como señales de salida genera y, de hecho, en el caso especial de los bloques sin salidas, siempre un bloque posee el menos una rama cuya numeración coincide con la del bloque. De esta forma, las ramas asociadas a un mismo bloque presentan numeración secuencial, siendo el número de la primera rama el mismo que identifica al bloque.

Diagrama de bloques Es la red de bloques en la cual se muestra la información relativa a la topología, en la forma de ramas que conectan los diferentes bloques.

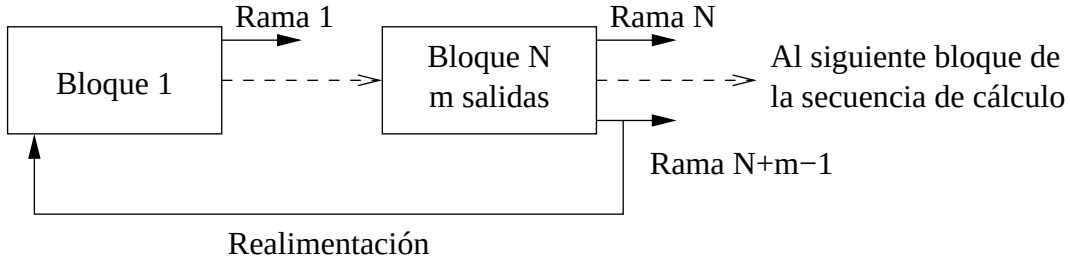


Figura 2.2: Esquema topológico de las conexiones de los bloques del código TRETA.

Nº línea	**Estructura de un bloque**			
	Título			
1	Título del bloque			
	Especificaciones topológicas			
2	Nº id. bloque	Nº bloque real.	Op. Impresión	
3	Nº id. ramas			
	Tratamiento			
4	Tipo de módulo	Op. depuración	Inic. salidas	
	Información de realimentación			
5	Max. iteraciones	Criterio convergencia	Alg. empleado	Nº ramas + convergencia
6	Nº ramas convergencia			
7	Criterio ramas + convergencia			

Tabla 2.1: Estructura de un bloque en el fichero de entrada del código TRETA.

2.1.2 Método general de resolución del modelo del sistema

TRETA resuelve las redes de diagramas de bloques compuestas de ecuaciones algebraicas y ecuaciones diferenciales ordinarias no lineales. Su comportamiento es similar, en muchos aspectos, al de los denominados lenguajes de simulación. Sin embargo, la estructura en bloques permite el desarrollo progresivo del modelo del sistema, aumentando el grado de detalle o la complejidad del mismo de forma gradual sin necesidad de replantear de forma completa su diseño.

El diagrama de bloques representa el sistema a simular en ciertas condiciones iniciales y durante un cierto intervalo de tiempo. Para alcanzar este objetivo, las salidas de los bloques del diagrama son calculadas cada paso de tiempo, definiendo el estado físico del sistema completo en cada instante considerado.

En este planteamiento, el *driver* de TRETA lleva a cabo, Figura 2.3:

- La gestión del fichero de entrada de parámetros del modelo y la inicialización de las variables.
- La actualización del modelo con el tiempo durante la simulación.
- La gestión de las salidas y las entradas de cada bloque del modelo.
- Para cada instante temporal, el cálculo completo del diagrama de bloques, que conlleva:
    1. El cálculo secuencial de cada bloque del diagrama definido en el fichero de entrada. Gestión de las realimentaciones, mediante un esquema de cálculo iterativo.
    2. Almacenamiento temporal de las salidas del modelo.
- El procesado de las salidas del modelo, en tiempo real (en configuraciones integradas con interfases gráficas) o la generación de ficheros de datos numéricos acompañados de reprentaciones pseudográficas mediante caracteres ASCII.

Dentro de este esquema, la sección dedicada al cálculo está dividida en dos subsecciones separadas, correspondientes al cálculo del estado inicial estacionario y el cálculo del transitorio. Estas dos subsecciones son muy similares en funcionalidad, presentando como mayor diferencia los modelos físicos en su parte temporal.

En la subsección del cálculo transitorio, se pueden observar dos lazos. El lazo temporal, implementado en el bloque de decisión 18, gestiona el avance del tiempo y la finalización de fase de cálculo. Por otra parte, el lazo topológico, anidado en el lazo temporal e implementado en el bloque de decisión 20, llama secuencialmente a las rutinas asociadas con los bloques del diagrama del modelo, es decir, los diferentes módulos del código con sus correspondientes datos de entrada. Cuando se detecta un lazo de realimentación en el diagrama del modelo, el esquema de cálculo secuencial se rompe, y el lazo de realimentación se resuelve mediante un esquema de cálculo iterativo de los bloques que abarque dicho lazo, Figura 2.4. La secuencia de cálculo de la realimentación se finaliza cuando se alcanza el criterio de convergencia especificado. En

caso de sobrepasarse un número especificado de iteraciones, el código aborta la simulación de forma controlado mostrando toda la información necesaria para definir el problema, bloque 25.

Finalmente, una vez finalizada la simulación del lazo temporal, bloque 18, los resultados se vuelcan en los medios de almacenamiento especificados, bloque 28.

Figura 2.3: Diagrama de flujo del código TRETA.

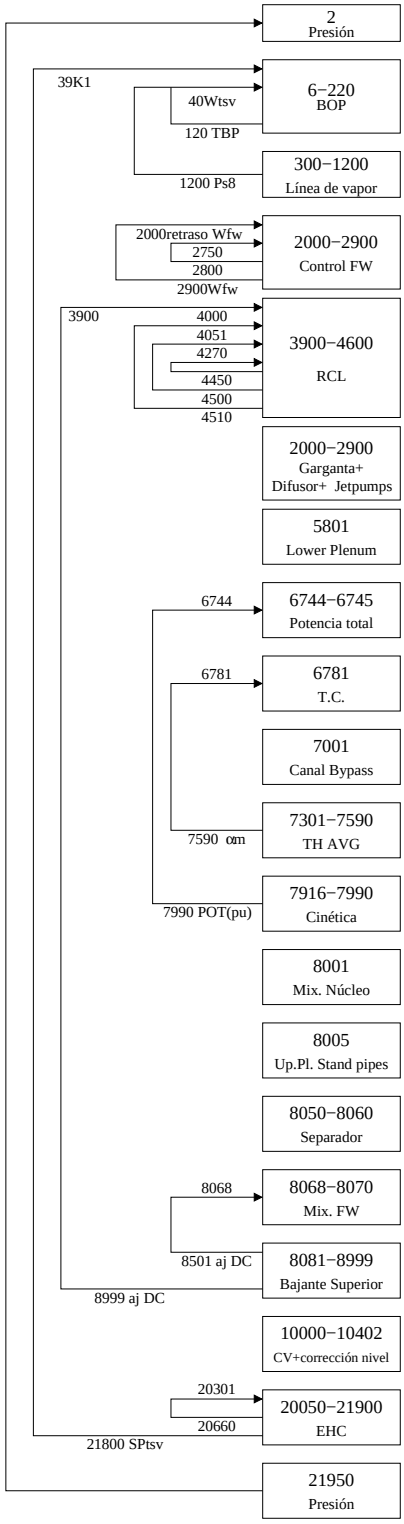


Figura 2.4: Esquema de realimentaciones del modelo de una planta BWR-GE.

2.1.3 Descripción de los modelos específicos para centrales nucleares

Los modelos específicos de partes del sistemas incluidos en el código TRETA en forma de módulos son:

Presionador

Se compone de un modelo de dos regiones, líquido y vapor, en el cual se computan los balances de masa y energía en el presionador, mediante un esquema de cálculo basado en volúmenes de control variables, considerando que el nivel de líquido puede variar con las condiciones de los transitorios. A pesar de que cada región se considera uniforme, es decir, se considera mezcla perfecta, se permiten condensación y sobrecalentamiento en la región del vapor y evaporación y subenfriamiento en la del líquido. Además, se considera una distribución uniforme de gotas de líquido y burbujas de vapor en ambas regiones, suponiendo una velocidad constante de caída y elevación.

Integrados en el modelo, se encuentran considerados los efectos de los calentadores, la ducha y las válvulas de alivio y seguridad. Los flujos de caudal de las válvulas de alivio y de seguridad, potencia calorífica de los calentadores y caudal de la ducha deben ser suministrados por modelos externos diseñados por el usuario.

Generador de vapor

Como características propias del módulo, la transferencia de calor del primario al secundario se computa empleando un coeficiente de transferencia de calor global (UA), adecuadamente inicializado para alcanzar el estado inicial indicado en el fichero de entrada suministrado por el usuario. La región de transferencia de calor es dividida radialmente en tres regiones que se corresponden con las resistencias térmicas de la película del primario, del tubo de metal y de la película del secundario; cada una de ellas tiene una fracción nominal de la resistencia térmica global que es fijada en el fichero de entrada. La resistencia del tubo se supone constante durante el transitorio. La correlación de Dittus-Boelter para convección forzada se emplea para calcular la contribución de la película del primario, presentando una dependencia el coeficiente de global de transferencia de calor del caudal del primario. La correlación de Jens-Lottes para tranferencia de calor en ebullición se emplea para calcular la resistencia de la película del lado secundario, introduciendo dependencias del flujo calorífico, presión e inventario másico del secundario. Adicionalmente, se incluye una opción para considerar el efecto de la degradación del área de transferencia de calor por descubrimiento de los tubos por pérdida de inventario de agua. El usuario debe introducir como parámetro del fichero de entrada el volumen de líquido del secundario por debajo del cual comienza el descubrimiento, esto origina un reducción lineal del área de transferencia en función de la reducción del volumen de agua.

El lado secundario del generador de vapor se representa mediante un nodo colapsado de mezcla saturada de líquido y vapor; esto implica que el modelo de masa y energía es

equivalente a una ecuación diferencial ordinaria no lineal en vez del conjunto original de ecuaciones en derivadas parciales que consideran la distribución espacial de las propiedades del fluido y de los materiales. Como el fluido del secundario se supone siempre en condiciones de saturación, sus propiedades (presión del vapor, entalpía y densidad) son evaluadas como propiedades de saturación. Todas las estructuras del generador de vapor se suponen con la misma temperatura que el vapor del secundario, considerando los efectos asociados a la energía almacenada en función de la capacidad calorífica del sistema. Se aconseja, debido a las limitaciones del modelo, que la actuación de los sistemas de seguridad no se demande en función de la correlación de cálculo de nivel suministrada con el código, sino en una equivalencia nivel-masa del secundario definida por el usuario.

Bomba de refrigerante del reactor

La ecuación básica de la bomba de refrigerante del reactor (*Reactor Cooling Pump*, RCP) se resuelve incluyendo los efectos de pérdidas por fricción, elevación, altura manométrica y momento del fluido. La altura monométrica y el torque de la RCP se obtienen mediante las curvas homólogas adecuadas, que son incluidas por el usuario en el fichero de entrada. La ecuación de la velocidad de la bomba incluye los efectos del torque del motor de la bomba, el torque hidraúlico en el impulsor, la pérdida por resistencia fluidodinámica de la bomba y la fricción y la inercia de giro de la bomba. Este modelo de RCP puede ser usado para simular cálculos de *coastdown*, bloqueo del rotor y caudal de circulación natural. Sin embargo, a pesar de que el modelo es capaz de simular transitorios con caudales inversos, dentro de los modelos de sistemas no puede ser simulado durante un transitorio, por lo que no se debe considerar esta posibilidad.

Transferencia de calor del combustible

Emplea un número fijo de nodos axiales, especificados por el usuario, y uno radial, siendo uno por lazo. Se define un coeficiente global de transferencia de calor (UA) función de la temperatura radial media del combustible, considerándose un ajuste parabólico de los valores especificados por el usuario. Otro ajuste parabólico se usa para determinar la capacidad calorífica específica del combustible como función de la temperatura del combustible.

Cinética

Se usa un modelo de cinética puntual con seis grupos de neutrones diferidos, estando también incluido un término fuente. El módulo puede considerar cambios de reactividad suministrados por modelos externos diseñados por el usuario relativos al efecto Doppler, la concentración de boro, la posición de las barras de control, etc.

Calor residual

Se emplea un modelo de precursores de cinco grupos muy similar al empleado en el modelo de los precursores de neutrones retardados. Alternativamente, se puede escoger emplear el estándar ANSI-51.1.

Finalmente, cabe resaltar en lo que respecta a las capacidades de simulación de canales termohidraúlicos y de elementos de control y señales que el código TRETA presenta un conjunto amplio y completo de módulos que permiten el diseño de sistemas termohidráulicos y de control de gran complejidad, Tabla 2.2.

Nº módulo	Nombre	Función
1	Integrador con límites	Valct
2	Resolución de sistemas de EDO lineales de coeficientes variables	Linvar
3	Dispositivos lineales no generales	Alin
4	Controlador PID	Pidn
5	Combinación lineal	Comblin
6	Núcleo de convolución exponencial	Convex
7	Extracción de la perturbación	Pertex
8	Convolución de Laguerre	Conlag
9	Retardo puro de tiempo	Delay
10	Transferencia de calor en el generador de vapor	Uasg
12	Función de disparo	Trip
13	Funciones bilineales	Bilinin
14	Puerta nalógica-lógica	Logate
15	Entradas como función de tiempo	Fint
18	Evaluación del flujo de calor crítico	Mdnbr
24	Mezcla a la entrada de la vasija del reactor	Mixrvi
25	Mezcla y derrame en la salida del núcleo	Mixrco
26	Flujo de entrada y entalpía en las ramas calientes del RCS	Hlhin
27	Funciones analíticas	Funin
28	Acoplamiento de masa, entalpía y momento (inversa) con caudal volumétrico	Pipei
29	Acoplamiento de masa, entalpía y momento (directa) con caudal volumétrico	Piped
30	Presionador	Pres1
31	Tablas de propiedades del agua	Mtab
32	Funciones matemáticas dependientes de una variable	Funmat1
33	Mezcla general	Sumt
34	Transmisión de calor en el núcleo	Qcalc
36	Salidas binarias	Salbin
37	Lectura de archivos	Files
38	Escritura de archivos ASCII	Writes

continúa en la página siguiente

continúa desde la página anterior		
Nº módulo	**Nombre**	**Función**
39	Resolución de EDO de primer orden	Metodo
41	Funciones matemáticas dependientes de dos variable	Funmat2
42	Funciones lógicas	Funlog
43	Funciones matemáticas varias	Funmix
44	Lectura de las tablas de propiedades del agua	Leerta
48	Modelo de flujo crítico	Flucrit
51	Acoplamiento de masa, entalpía y momento (inversa) con caudal másico	Pipem
1001	Resolución del modelo de cinética puntual	Cineti
1002	Realimentación combinada de los coeficientes Doppler y de densidad del moderador	React
1003	Modelo de calor residual ANSI 5.1 con constante histórica	Memres
1004	Válvulas de control, aislamiento y chequeo	Valves
1012	Bomba centrífuga	Centrifu

Tabla 2.2: Tipos de módulos presentes en el código TRETA

2.2 Código de simulación de procedimientos COPMA-III

La primera versión del sistema de simulación COPMA (*Computerized OPerator MAnuals*) fue desarrollada en 1985 como un sistema basado en *Lisp* e instalable en computadoras *Lisp* de Texas Instruments. La motivación que llevó a su desarrollo fue la implementación de procedimientos computerizados en centrales nucleares, considerando los beneficios que pudiese proporcionar y el impacto que tendría en los operadores. A lo largo de 1990 el sistema COPMA-II se integró en máquinas UNIX y X-Windows. COPMA-I y COPMA-II se basaban en dos módulos denominados el núcleo (*kernel*) y el cliente (*client*), apoyándose en el uso de un lenguaje para la computerización de procedimientos denominado Prola. COPMA-II también tenía un editor gráfico de procedimientos denominado PED-II. Durante la integración de COPMA-II en diversos sistemas de simulación, se determinó que el lenguaje Prola presentaba serias limitaciones en la estructura y la funcionalidad de los procedimientos, resultando que los procedimientos debían ser adaptados para su computerización. En 1994 se inició la búsqueda de una nueva forma de computerización de los procedimientos, resultando en la elección del XML. La primera versión de COPMA-III se presentó en el año 2000, basada en XML como lenguaje básico de computerización de los procedimientos, Figura 2.5. Los módulos que integran las herramienta están programados en Java y C++.

Dentro del HRP y de la línea del desarrollo del sistema COPMA en sus primeras versiones, se consideró la posibilidad de realizar aplicaciones del sistema a la simulación automatizada de procedimientos, desarrollándose diferentes proyectos en esta línea con el CSN, Hortal (1996a). Sin embargo, la aplicación de COPMA-III se ha orientado principalmente a su uso en simuladores de salas de control, como por ejemplo el simulador HAMBO del HRP, o simuladores de entrenamiento, p. ej. el proyecto de simulador de entrenamiento de la CN de Kola, Roverso

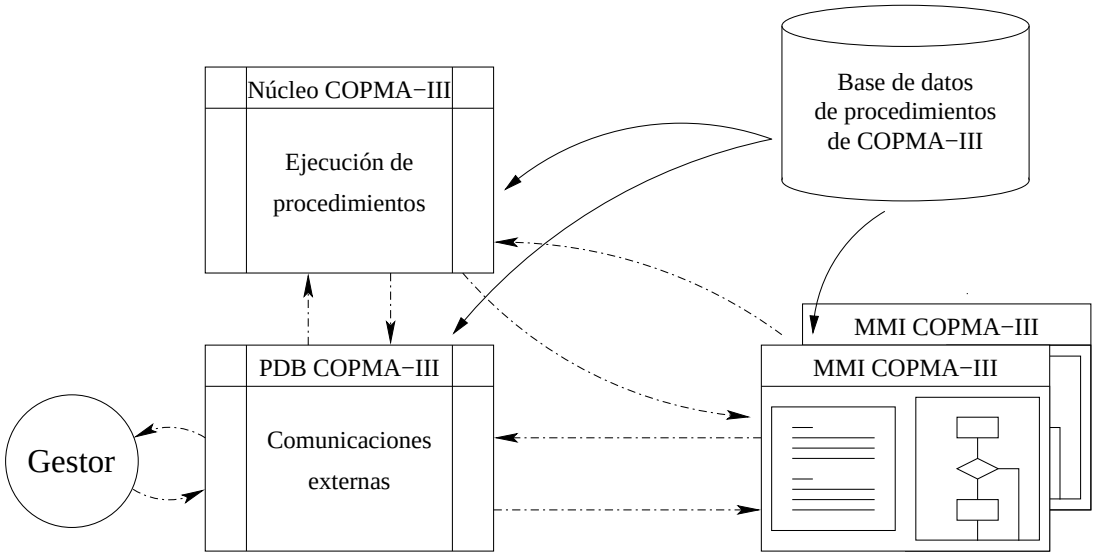


Figura 2.5: Esquema general del sistema COPMA-III.

(2005). En ningún caso se han realizado aplicaciones del sistema a la simulación automatizada de procedimientos, siendo este trabajo pionero en su alcance, aunque siempre se ha considerado como una de sus líneas de desarrollo, Berg y Nilsen (2002).

Los diferentes módulos que componen el sistema COPMA-III son, Figura 2.5:

Cliente o COPMA-III MMI.

El cliente emplea el explorador Internet Explorer de la plataforma Windows para mostrar la MMI de los procedimientos computerizados, Figura 2.6. Los procedimientos son transformados desde XML a HTML por medio de archivos de secuencias de comandos de XSL. El módulo presenta un conjunto de ficheros de configuración que dan flexibilidad a la hora de definir la apariencia de la MMI o como los mensajes enviados y recibidos del núcleo o de la base de datos de procesos son enviados e interpretados.

Este módulo del sistema COPMA-III tiene altas capacidades gráficas de visualización de procedimientos, mediante el uso de un módulo gráfico basado en el paso de XML a PGD-L y, finalmente, a gráficos SVG para su visualización, Alemberti et al. (1996).

Núcleo o COPMA-III *kernel*.

El núcleo es el responsable de asistir al operador en la ejecución del procedimiento. Dependiendo del grado de configuración, el núcleo puede presentar diferentes grados de automatización en el seguimiento del flujo lógico y estructural de los procedimientos. Normalmente, el núcleo mantiene el seguimiento de la posición actual en el procedimiento y notifica a otros procesos acerca de la siguiente parte a ser ejecutada. Además, el núcleo puede realizar la vigilancia de variables de proceso tal como se indique en el procedimiento XML. En el momento en que se cumpla la condición de vigilancia sobre

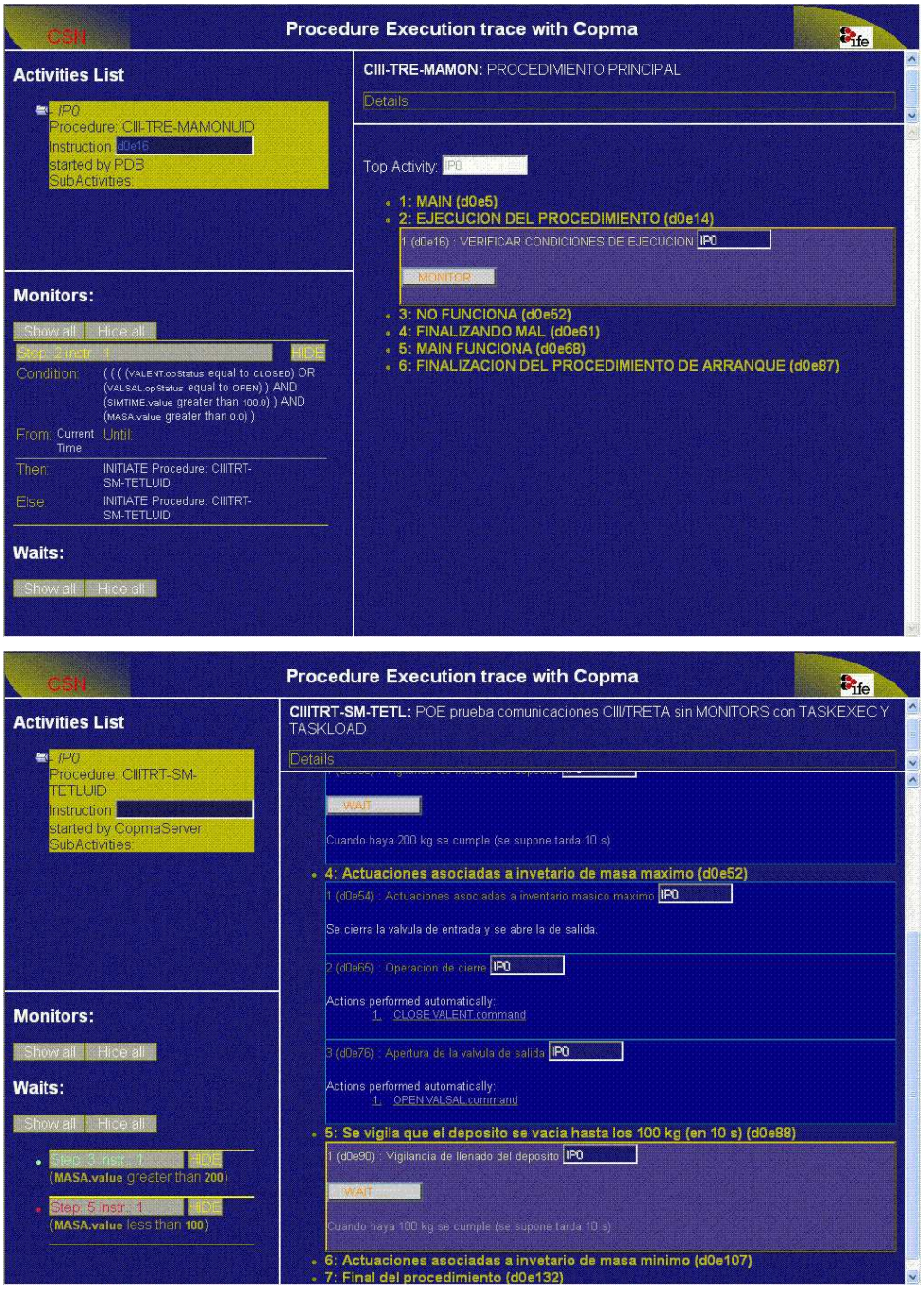


Figura 2.6: Ejemplos de MMI del cliente de COPMA-III.

cierta variable del proceso físico, el núcleo notifica a un proceso externo especificado el cumplimiento del criterio de vigilancia.

El núcleo posee, además, capacidades de ejecución simultánea de un conjunto de procedimientos. Esta capacidad se basa en el concepto de actividad, que permite distinguir entre instancias de un mismo procedimiento que se ejecutan simultáneamente. El concepto de actividad es, en realidad, mucho más amplio que la relación con la ejecución de procedimientos. Cada tarea que el núcleo debe supervisar, entendiendo como tarea la ejecución de un procedimiento, la vigilancia de condiciones específicas de parámetros físicos del proceso o la condición de espera de un procedimiento, suele tener asociada una o mas actividades. En este sentido, una actividad puede estar constituida por una o más instrucciones, uno o más pasos o un procedimiento completo. De hecho, el núcleo de COPMA-III maneja actividades y no procedimientos, lo que le dota de gran versatilidad.

Otra característica interesante del núcleo de COPMA-III es el concepto de sesión, relacionado con la idea de la simulación de diferentes operadores interactuando con un conjunto cerrado de procedimientos. Cada sesión está relacionada con un operador, pudiendo gestionarse el seguimiento de los procedimientos en función del tipo de operador y otros atributos del mismo.

En lo que respecta a la interpretación de los procedimientos, el núcleo de COPMA-III esta dotado de gran flexibilidad, correspondiéndose el cuerpo del módulo más con un intérprete de sintaxis que con un procesador de instrucciones. Por ello, los procedimientos empleados por el núcleo se caracterizan por estar implementados en un lenguaje de bajo nivel, cuyo léxico se corresponde con un conjunto de bloques constructores que proporcionan las funciones necesarias para interpretar los diferentes elementos del lenguaje de codificación de los procedimientos.

Base de datos de procesos o COPMA-III PDB (*Process Data Base*).

Es la responsable de las comunicaciones con procesos externos desde y hacia al sistema COPMA-III, estando diseñada para obtener información de la computadora de procesos de la CN.

Este módulo del sistema COPMA-III está basado en Java y usa una librería DLL que le proporciona las funciones necesarias para conectar con otros sistemas. Los lenguajes empleados en esta librería pueden ser C o Pascal, por ejemplo. La DLL puede usar por lo tanto una API (*Application Programming Interface*) a fuentes de datos externas para recuperar y enviar información, siendo la interfaz programable para establecer cualquier tipo de interacción con el núcleo del sistema COPMA-III. El grupo del HRP ha realizado una versión de la misma para implementar la API requerida para su integración con el código TRETA. En versiones futuras está previsto el desarrollo de una librería que permita el acceso a la PDB empleando diversos lenguajes de programación, Bisio et al. (2000).

En este trabajo, la ejecución de los procedimientos se realiza de forma automática por medio de funciones implementadas en el código TRETA y la programación específica de la DLL del sistema COPMA-III. Los detalles de esta implementación se explican en el Capítulo 4.

2.3 Interfase de comunicaciones de los sistemas de simulación TRETA/COPMA-III

La funcionalidad de la interfase de comunicaciones debe satisfacer como objetivos principales:

- La gestión de las comunicaciones entre ambos códigos debe realizarse mediante un proceso independiente, cuyas capacidades de intercambio de información requieran una implementación sencilla y conlleve pocas o nulas modificaciones en las especificaciones de ambos códigos de simulación.
- Permitir que el código de planta y de procedimientos establezcan comunicación de forma síncrona, es decir, todos los procesos involucrados deben intercambiar la información referente a un instante de tiempo de simulación de forma coherente y consistente, sin provocar demoras significativas del trabajo de simulación.
- Una misma instancia del proceso que gestione la interfase debe ser capaz de establecer comunicaciones entre varias instancias de ambos códigos de simulación, en una misma computadora o en una plataforma de computación distribuida.
- Debe posibilitar la invocación de las funciones de comunicación implementadas en la PDB de COPMA-III por parte de TRETA, o viceversa, permitiendo que tanto el código de simulación de planta como el de procedimientos puedan gestionar la ejecución de los procedimientos, es decir, las dependencias de ambos códigos no debe ser en ningún caso funcionales, sino de forma exclusiva relacionada con la información requerida por cada uno de los códigos de simulación.

La integración de la solución adoptada pasa por la implementación de sendas interfases de comunicaciones en los códigos TRETA y COPMA-III. Para ninguno de los casos, dicha implementación requiere de consideraciones especiales. Para el caso de COPMA-III, todo la funcionalidad de las comunicaciones corre a cargo del proceso específico PDB, diseñado especialmente para ello. En el caso del código TRETA, al poseer un carácter modular, es sencillo implementar dicha interfase en los módulos específicos de comunicaciones, que a partir de ahora denominaremos módulos *copma3* y *copmacrew*.

Para la implementación de dicha interfase se contemplaron tres posibilidades ya desarrolladas:

1. SWBus.
2. RMI-JNI.
3. IDL-CORBA.

A continuación se pasan a analizar las tres alternativas incluyendo una valoración de las ventajas y desventajas de cada una de ellas.

2.3.1 RMI-JNI

El sistema RMI (*Remote Method Invocation*) de Java, permite que un objeto que esté corriendo en una máquina virtual (*Virtual Machine*, VM) de Java pueda invocar métodos de otro objeto que este corriendo en otra VM de Java, Sun (2002d). La RMI permite la comunicación de diferentes programas que estén escritos en Java mediante un protocolo de comunicaciones denominado JRMP (*Java Remote Messaging Protocol*), específicamente diseñado para el uso de objetos Java remotos. El JNI (*Java Native Interface*) de Java es el interfaz para lenguajes nativos de Java, Sun (2002e). El JNI hace posible que un programa Java que esté corriendo en una VM de Java puedan trabajar y usar código y librerías que estén escritos en C/C++, y a través de estos en prácticamente cualquier lenguaje. Adicionalmente, la API permite incluir una VM de Java en códigos escritos en C/C++ usando objetos y métodos Java desde un módulo escrito en C/C++. En particular, con JNI y RMI es posible invocar métodos remotos de un objeto Java desde un modulo escrito en C/C++.

Para poder acceder al PDB de COPMA-III una posibilidad existente en la versión original del sistema COPMA-III es el uso de un interfaz RMI. Este interfaz RMI de la PDB permitiría que un modulo en C con funcionalidad JNI pudiese acceder a las variable internas de COPMA-III. El esquema de esta solución de interconexión entre COPMA-III y TRETA se muestra en la Figura 2.7.

Esta solución implicaría que el módulo *copma3* fuese escrito parcialmente en C, siendo necesario la inclusión de código Java con JNI para poder acceder al registro RMI del PDB. Por otro lado, de acuerdo a la documentación de COPMA-III, el registro RMI del PDB solo incluye funciones para poder modificar valores de variables en el PDB, no existiendo funcionalidad para soportar la lectura y suscripción de variables en el PDB, Sun (2002a) . Por todo ello, para la adopción de esta solución, además del desarrollo de *copma3* en Java/C sería necesario extender la funcionalidad actualmente existente del registro RMI de la PDB.

La inclusión de código JNI dentro de los módulos *copma3* y *copmacrew* haría necesario el disponer del entorno Java adecuado en el entorno de ejecución del código TRETA, lo que potencialmente puede implicar problemas de compatibilidad entre diferentes plataformas.

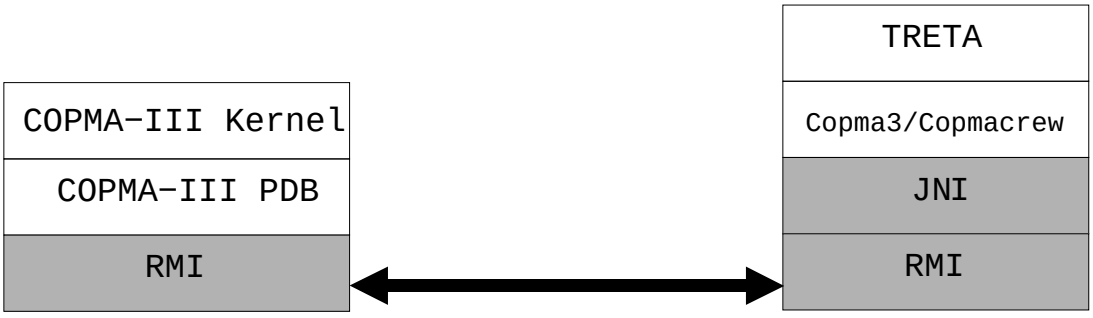


Figura 2.7: Configuración de la interfase de comunicaciones empleando el sistema RMI.

2.3.2 IDL-CORBA

La IDL (Interface definition Lenguage), Sun (2002b) y Sun (2002c), es una tecnología para objetos distribuidos, es decir, para poder comunicar objetos sobre diferentes plataformas a través de una red. IDL permite la interacción de objetos, es decir, la ejecución remota de métodos y el establecimiento de comunicaciones entre procesos, independientemente de si están escritos en Java, C/C++ o cualquier otro lenguaje. La tecnología IDL no es un lenguaje de programación sino mas bien un interfase para la puesta en común de los tipos de datos existentes en los diferentes lenguajes de programación, pudiendo definirse como un lenguaje de interfaz independiente del lenguaje nativo.

Usando IDL es posible comunicar procesos en diferentes plataformas gracias a que IDL está basado en la arquitectura CORBA (*Common Object Request Brokerage Architecture*), un estándar industrial para sistemas basados en objetos distribuidos, Sun (2002c). La característica clave de CORBA es el uso de la tecnología IDL. Todo lenguaje que soporta CORBA tiene su propio traductor IDL, también se suele hablar de compilador IDL, que hace posible el uso de la tecnología CORBA-IDL para el lenguaje nativo. Así se habla de Java IDL, C IDL, etc. Los detalles de cómo cada compilador IDL adapta el lenguaje nativo para usar CORBA dependen del lenguaje particular, dado que no es lo mismo trabajar con lenguajes interpretados como Java que con lenguajes compilados como C/C++.

RMI y Java IDL tienen características y capacidades similares, sin embargo hay dos diferencias importantes. La primera, es que RMI es una solución completamente basada en Java pero que solo permite comunicar entre sí objetos Java, mientras que Java IDL esta basado en un estándar, pero que sin embargo permite la comunicación entre objetos distribuidos escritos en diferentes lenguajes. La segunda diferencia son los protocolos de comunicación usados por ambas tecnologías. Java IDL usa el protocolo estándar de CORBA denominado IIOP (*Internet Object Request Broker Protocol*), que es el protocolo compartido por todas las aplicaciones que usen CORBA y el que finalmente permite que objetos residentes en diferentes plataformas y escritos en diferentes lenguajes puedan comunicarse entre sí. Por otro lado, Java RMI usa el protocolo JRMP (*Java Remote Messaging Protocol*) que está desarrollado específicamente para trabajar con objetos remotos Java. De cara al futuro, Sun e IBM han hecho públicos planes para permitir que RMI pueda usar IIOP, de manera que un objeto Java se pueda comunicar con cualquier otro objeto remoto que use CORBA.

La adopción de esta solución obligaría a desarrollar los módulos IDL necesarios para poder utilizar CORBA como interfaz entre COPMA-III y TRETA, Figura 2.8. Lo cual, como en el caso de la solución RMI, obligaría a desarrollar parte de los módulos *copma3* y *copmacrew* de forma mixta en C IDL y C, lo que implica un potencial riesgo a la hora de mantener en el futuro el sistema. Adicionalmente, la implementación de esta solución supondría un gran salto en el diseño actual de COPMA-III, que obligaría a hacer cambios substanciales.

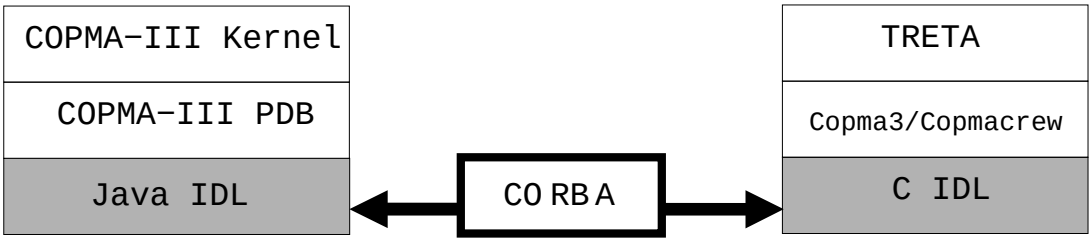


Figura 2.8: Configuración de la interfase de comunicaciones empleando la arquitectura CORBA.

2.3.3 Librería de comunicaciones *Software Bus*

La librería de comunicaciones *Software Bus* (SWBus) ha sido desarrollada por el HRP, HRP (2002a) y HRP (2002b). SWBus es un sistema de comunicaciones orientado a objetos capaz de gestionar un conjunto dinámico de objetos distribuidos, así como sus métodos. Las aplicaciones que usen objetos SWBus tienen la capacidad de compartir datos y métodos con otros procesos que estén corriendo en diferentes sistemas a través de la red utilizando el protocolo TCP/IP, facilitando de esta manera el desarrollo de sistemas distribuidos. La funcionalidad de SWBus se puede resumir en dos puntos:

1. El establecimiento de comunicaciones TCP/IP bidireccionales entre procesos.

2. La posibilidad de ejecutar métodos/funciones remotos.

En el marco del sistema TRETA/COPMA-III el esquema de la aplicación de SWBus se puede ver el la Figura 2.9. En su diseño original, la PDB de COPMA-III no tiene implementado el uso de SWBus, por lo tanto esta solución requiere la definición de un conjunto de métodos, o funciones de librería, para la lectura/escritura y suscripción de variables en el PDB, así como integrar la funcionalidad de SWBus en el PDB, Hortal y Nilsen (2002). En paralelo, sería necesario escribir los módulos de comunicaciones del código TRETA, *copma3* y *copmacrew*, con la funcionalidad de SWBus ya implementada.

Dado que físicamente SWBus esta implementado como una librería C, la solución basada en SWBus es la más ventajosa desde el punto de vista de la integración, ya que todos los módulos relacionados con este desarrollo del código TRETA están programados en C. Adicionalmente el desarrollo de *copma3* y *copmacrew* en lenguaje C aportaría grandes ventajas para su futuro mantenimiento quedando todo el proyecto TRETA basado en módulos programados en C. Este último aspecto se ve reforzado por el hecho de que la versión actual de SWBus es estable y está mantenida por el HRP, lo que evitaría depender de terceras partes en el futuro mantenimiento del sistema TRETA/COPMA-III. A su vez, la integración de SWBus en la PDB de COPMA-III tendría ventajas a la hora de diseminar el uso de COPMA-III como sistema computerizado de procedimientos.

Figura 2.9: Configuración de la interfase de comunicaciones empleando la librería SWBus.

2.3.4 Solución adoptada

La solución adoptada finalmente para establecer las comunicaciones entre TRETA y COPMA-III ha sido la función de librería Software Bus, SWBus. Las razones que más pesaron en la decisión fueron:

- Tanto la implementación de IDL o de RMI requerían la modificación extensiva de los módulos de comunicaciones de uno o ambos códigos.
- Ambas opciones están desarrolladas por un tercero, implicando una dependencia adicional a la hora de mantener el desarrollo de la herramienta y de llevar a cabo aplicaciones de la misma.
- Ambas opciones conllevaban la integración de fuente Java en el código TRETA.
- El uso de TCP/IP por parte de SWBus, ya que dota de gran versatilidad en cualquier plataforma de computación distribuida.

Para la implementación de SWBus en ambos códigos se han realizado las modificaciones necesarias en la PDB, ya que la primera versión de COPMA-III no tenia implementada la capacidad de comunicarse con otros procesos mediante SWBus, y la codificación de los módulos *copma3* y *copmacrew* de TRETA, Figura 2.10. Una de las tareas más importantes de este proceso consistió en la definición de la funcionalidad necesaria para estas comunicaciones. Todo los detalles referentes a esta tarea se comentan en el Capítulo 5.

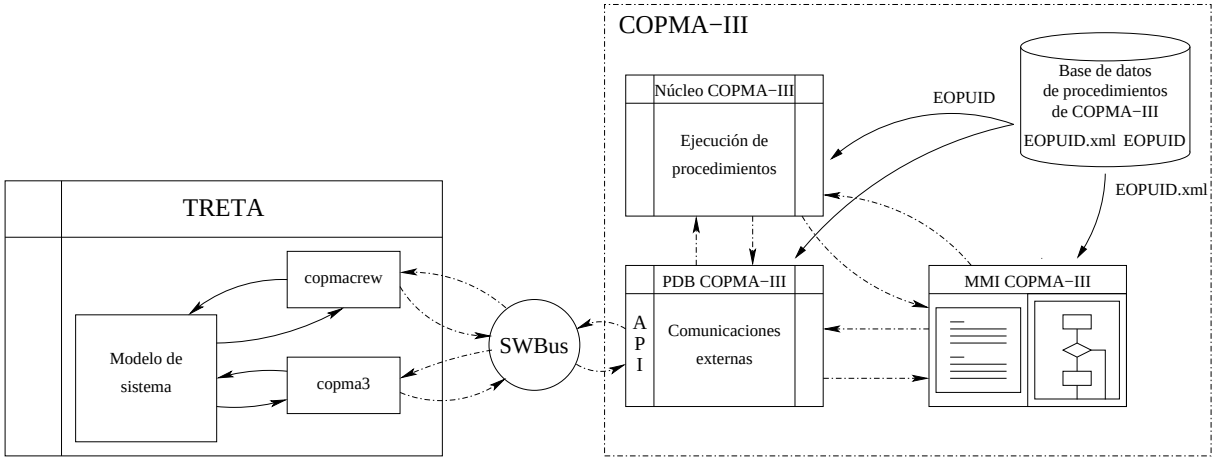


Figura 2.10: Implementación de la interfase de comunicaciones del simulador integral TRETA / COPMA-III.

Capítulo 3

Modelo de planta PWR-W para el código TRETA

Índice

En este capítulo detalla el trabajo realizado para la obtención del modelo de una central nuclear PWR-W genérica de tres lazos. El desarrollo del modelo se realizó a partir de una primera versión del mismo suministrada por el CSN, al cual se ha realizado un conjunto de mejoras, ampliando de forma considerable sus capacidades de simulación. El trabajo realizado se muestra en este capítulo siguiendo la siguiente estructura:

- Primeramente, se presenta su estado actual, Sección 3.1, llevando a cabo una descripción detallada del modelo de planta, de los modelos de sistemas de salvaguardias y protección, así como de las mejoras que se han realizado en el código para soportar ciertos aspectos de la simulación que no estaban considerados en los módulos del código TRETA.

- Posteriormente se presentará el esquema de cálculo del modelo, mostrando algunas de las mejoras implementadas en el mismo, Sección 3.2.

- Finalmente, se incluyen el conjunto de transitorios de validación del modelo, considerado de forma que sirva para comprobar la implementación de sistemas de salvaguardias y protección, sus tarados y parámetros de operación, así como determinar las capacidades de simulación del modelo desarrollado, Sección 3.3.

3.1 Descripción del modelo genérico de un PWR-W de tres lazos

El modelo genérico de un PWR-W de tres lazos que se describe en esta sección consta, principalmente, de las siguientes partes:

- Modelo de los lazos de refrigeración, que incluye las bombas de refrigerante y los tramos de ramas frías, calientes e intermedias, Sección 3.1.1.

- Modelo de vasija del reactor, considerando la generación de potencia y la transmisión de calor al refrigerante, Sección 3.1.2.

- Modelo del presionador y de los controles de nivel y presión relacionados, Sección 3.1.3.

- Modelo del secundario de la instalación, Sección 3.1.4

- Modelos del sistema de agua de alimentación normal y auxiliar (FWS y AFWS), Sección 3.1.5, del sistema de inyección de seguridad, Sección 3.1.6, del sistema de aislamiento de las líneas de vapor y de roturas localizadas en el secundario, Sección 3.1.7.

- Modelo del sistema de protección del reactor y de las señales de actuación de las salvaguardias tecnológicas, Sección 3.1.8.

3.1.1 Modelo de los lazos de refrigeración del reactor

Teniendo en cuenta la simetría de los lazos sin presionador, lazos 1/3 del RCS, Figura 3.2, se han considerado dos tipos de lazos, los dos lazos sin presionador y el lazo con presionador, modelándose los lazos 1/3 como uno sólo e introduciendo las propiedades del caudal obtenido por duplicado en el modelo de vasija, Figuras 3.3 y 3.5. La descripción del modelado de ambos lazos y de su nivel de detalle se realizará en los apartados siguientes, considerando los aspectos específicos de cada uno de ellos.

La nodalización realizada del primario del RCS tiene el suficiente nivel de detalle como para simular los transitorios operacionales más comunes de este tipo de plantas, Figura 3.1. Además, los sistemas, controles y componentes modelados permiten simular de forma realista un amplio conjunto de secuencias accidentales, tal como se puede comprobar en los resultados obtenidos para los transitorios considerados, Sección 3.3.

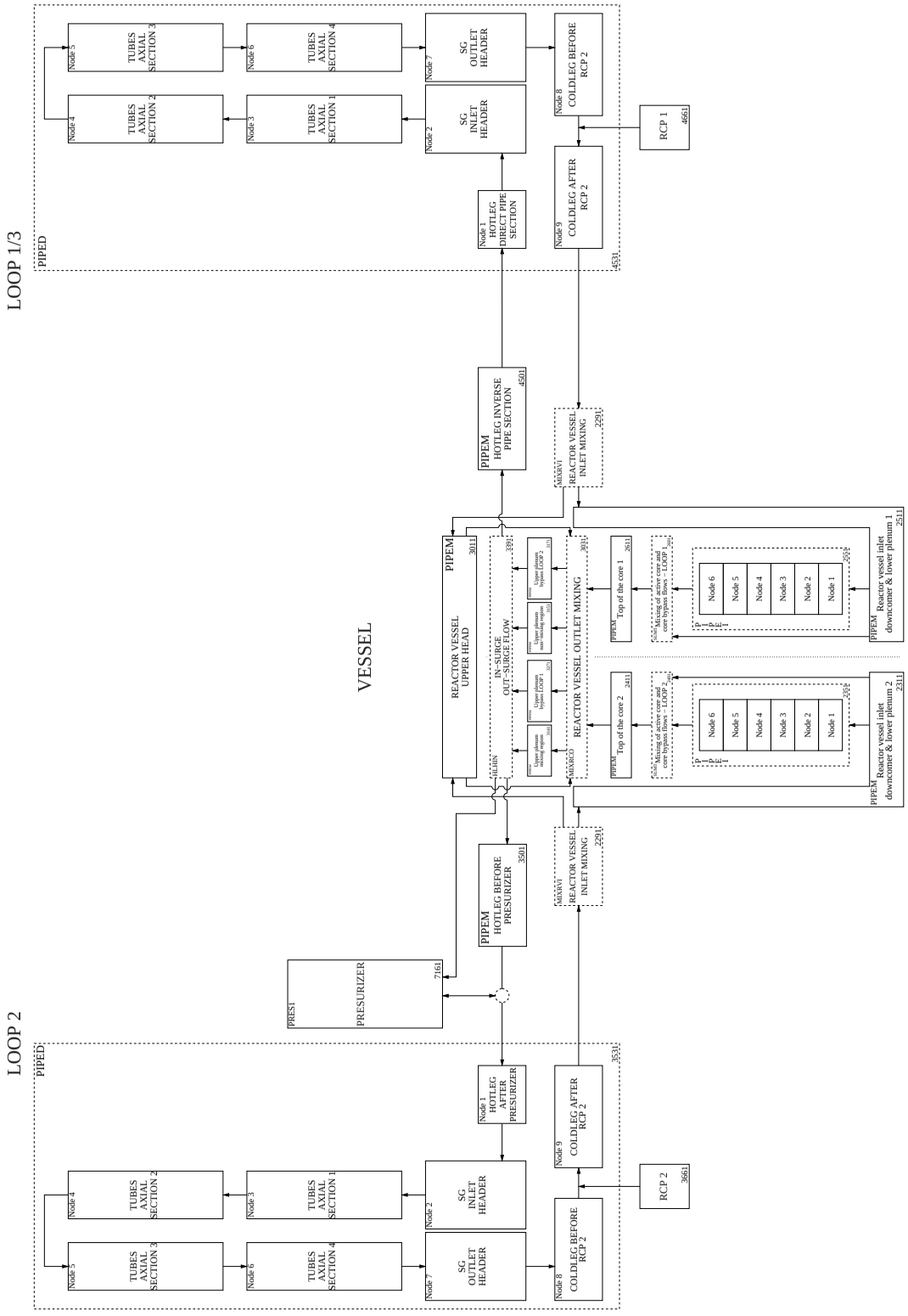


Figura 3.1: Esquema topológico del RCS del modelo de planta PWR-W para el código TRETA.

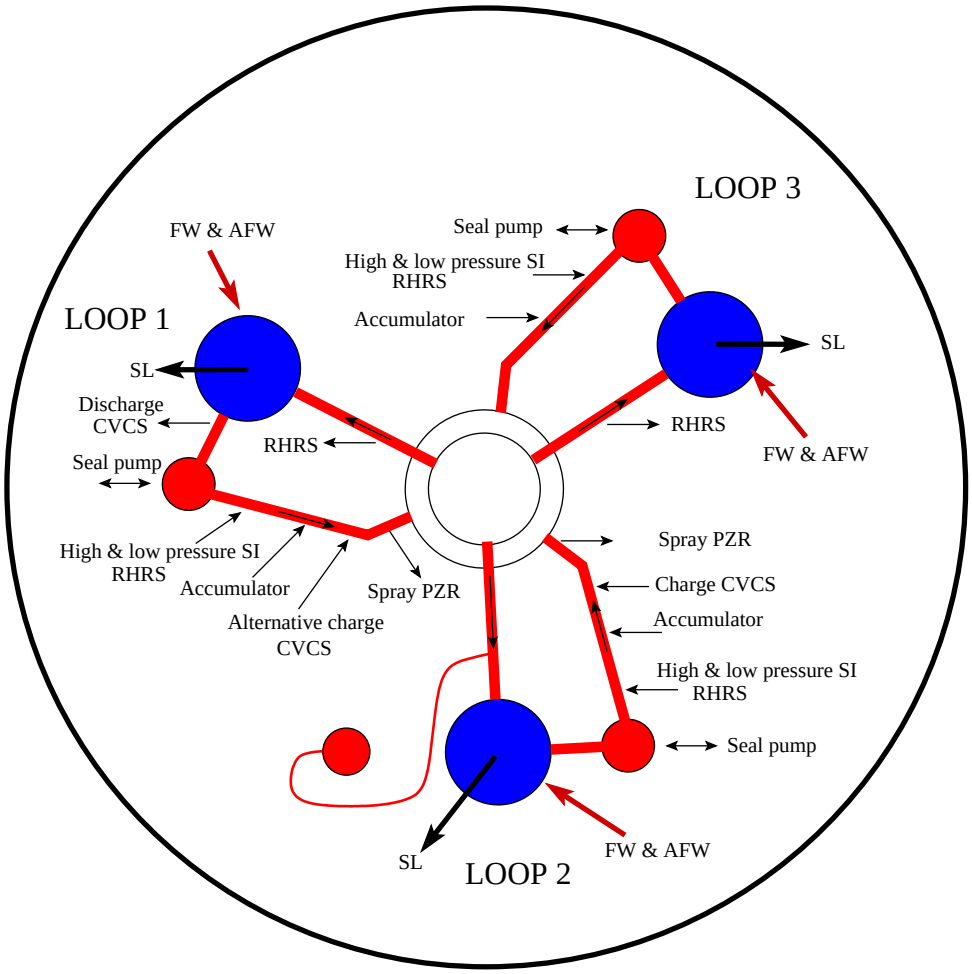


Figura 3.2: Esquema del RCS de una planta PWR-W.

3.1.1.1 Modelo del lazo con presionador

El lazo de refrigeración 2 consta de la rama caliente, distinguiendo dos tramos, el anterior y el posterior a la conexión con el presionador, lado primario del SG, rama intermedia, la bomba del lazo y la rama fría.

Rama intermedia del lazo 2

Las consideraciones relativas al modelado de la rama intermedia se asocian con el nodo 8 y 9 de la rama fría, Figura 3.3,. Así, en lo que respecta a la RCP del lazo, la potencia calorífica generada y el cálculo del punto de operación en la linealización de la curva característica, constantes C0 y C1, se realizan considerando la densidad y el caudal volumétrico de estos nodos, siendo las ramas 23, 3663 y 3664, respectivamente.

Rama caliente del lazo 2

Para el modelado del tramo anterior a la conexión al presionador se ha empleado un bloque 3501 (PIPEM), de forma que se obtiene la caída de presión en esta parte de la tubería. Esta caída presión, añadida a la caída de presión total en la vasija en el bloque 3521, se emplea como condición de contorno para el bloque 3531 (PIPED) donde se modela el resto del lazo, incluido el tramo de rama caliente posterior al presionador, hasta la entrada a la vasija.

En la conexión existente en la rama caliente con el presionador se deben considerar los flujos de entrada/salida de caudal desde el presionador al lazo de refrigeración, calculándose el caudal neto al o desde el presionador en el bloque 3391 (HLHIN). La entalpía de entrada al bloque 3531 (PIPED) se cacula considerando el caudal de la tubería de conexión del presionador, rama 3391 del bloque 3391 (HLHIN), y la entalpía correspondiente a flujos de salida del presionador, entalpía calculada por el bloque 7161 (PRES1) rama 7163, entalpía correspondiente a la región de líquido de la parte inferior del presionador.

Lado primario del SG del lazo 2

Se corresponde con los nodos 2 a 7 del bloque 3531 (PIPED), modelando:

- La caja de aguas de entrada al SG.
- Dos nodos asociados al tramo ascendente de tubos en U.
- Los dos nodos correpondientes al tramo descendente de los tubos.
- La caja de aguas de salida del SG.

Tanto de la caja de aguas de entrada al SG como de los nodos asociados a los tubos en U, parten las ramas 3543 (caudal de tubos), 3555, 3562, 3569 y 3576 (temperaturas de los nodos de tubos) que aportan las dependencias de caudal de tubos y temperaturas al

bloque 1951 (UASG), encargado de calcular la transferencia de calor al secundario. Las ramas correspondientes al flujo de calor calculado por este bloque son suministradas a los nodos de tubos para cerrar el cálculo de transmisión de calor primario-secundario.

Todas las dependencias del secundario de los lazos modelados cuentan con inicialización de estacionario, pudiéndose realizar la convergencia del estacionario de esa parte del modelo de forma independiente.

Rama fría del lazo 2

Como ya se ha comentado previamente, la rama intermedia ha sido incluida en el nodo 8 del bloque 3531, primer nodo de rama fría, en el cual se consideran la aportación de la potencia calorífica y los parámetros de la linealización de la curva característica para el caudal de paso por el nodo 9, ambos de la RCP del lazo, ramas 3663, 3664 y 23, respectivamente.

En la rama fría se localizan las conexiones, todas ellas de carga, del CVCS y del HPIS. Para este tipo de conexiones, el modelo cuenta con entradas de caudal y entalpía para aporte del CVCS y el HPIS independientes para cada uno de los lazos en el bloque 2291 (MIXRVI), bloque de mezcla de los caudales de entrada a la vasija.

A continuación se comentan las características principales del modelo de lazo 2.

Dependencias del modelo del lazo 2 con otros modelos

- **Modelo de la vasija**. Presenta dos dependencias. Por un lado, obtiene la distribución de flujos tanto para cada lazo como para la línea de conexión del presionador, bloque 3391 (HLHIN). Y, por el otro, calcula la caída de presión del lazo sumando las caídas de cada bloque de la parte azimutal de la vasija correspondiente al lazo 2, añadiendo el tramo de la rama caliente desde la salida de la vasija hasta la conexión con el presionador, bloques 2311, 2351, 2411, 3171 y 3501 (PIPEM).
- **Modelo del presionador**. La presión del primario se obtiene del modelo del presionador, bloque 7161 (PRES1), corrigiéndola con la caída de presión correspondiente a la tubería de conexión con el lazo 2 del RCS, bloques 7181 - 7185.
- **Modelo del secundario correspondiente al lazo de refrigeración 2**. La dependencia es recíproca, con el objeto de calcular el coeficiente de transmisión de calor en el generador de vapor, bloque 1951 (UASG). Este bloque requiere las temperaturas de los nodos de tubos y el caudal de paso, obteniéndolos del bloque 3531 (PIPED).
- **Modelo de la bomba de primario correspondiente al lazo de refrigeración 2**. Proporciona los parámetros de la linealización de la curva característica de la bomba del primario, bloque 3661 (CENTRIFU) ramas 3663 y 3664, y el calor aportado por la bomba, bloque 23 (CTE), con un valor de 3.333333e+06 W, Figura 3.4.

- **Modelo del SIS**. El modelo debe suministrar el caudal y la entalpía correspondientes a la actuación de la inyección de seguridad directamente al bloque 2291 (MIXRVI) de entrada a la vasija.

Bloques relevantes

El modelo termohidráulico del lazo se corresponde, principalmente, con los bloques 3501 (PIPEM) correspondiente al tramo de la rama caliente anterior a la conexión del presionador, y el bloque 3531 (PIPED) que modela el resto del lazo. En estos bloques se efectúa el cálculo de las ecuaciones de conservación del fluido, siendo la única diferencia entre ambos la forma de la resolución de la ecuación del momento. El bloque 3501 se corresponde con un módulo PIPEM, que aplica la ecuación del momento de forma directa, partiendo del caudal volumétrico, mientras que el bloque 3531 se resuelve la ecuación del momento de forma inversa, tomando como condición de contorno la caída de presión en el lazo y obteniendo el caudal de entrada a la vasija.

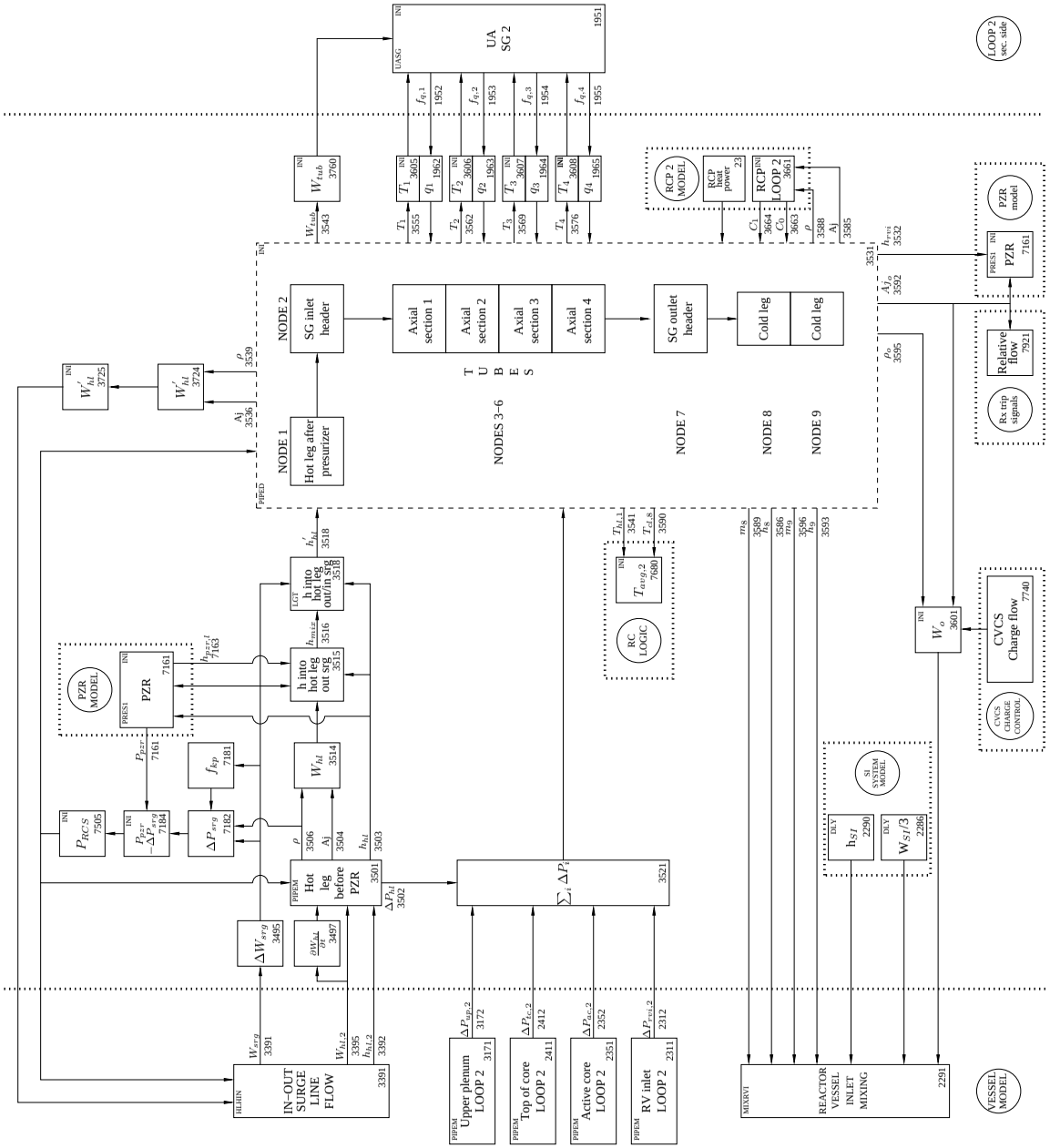


Figura 3.3: Modelo termohidráulico del lazo con presionador.

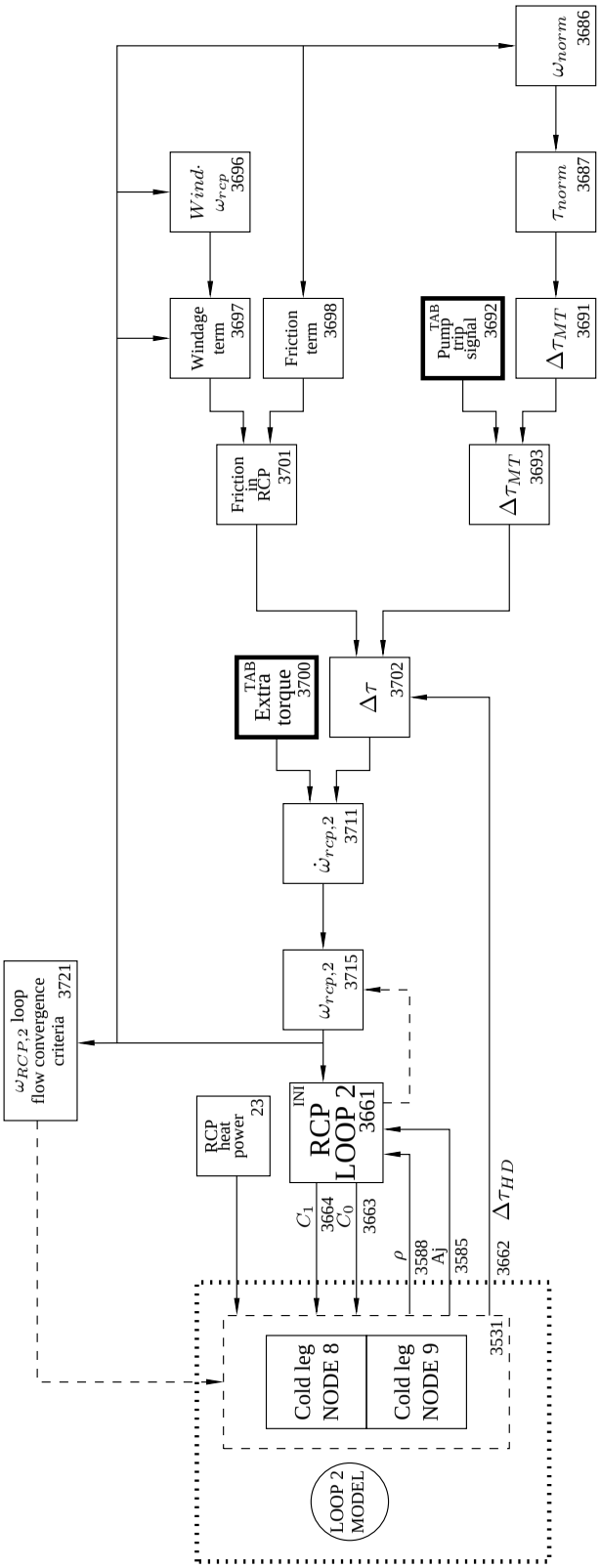


Figura 3.4: Modelo de la bomba del lazo con presionador.

3.1.1.2 Modelo de los lazos sin presionador

El modelo de los lazos 1/3 es similar al correspondiente al lazo 2, siendo la única diferencia que en este caso no hay conexión con el presionador. Por lo demás, el modelo es idéntico, trasladándose la numeración de los bloques.

Rama caliente de los lazos 1/3

Idéntico al modelo de lazo 2, exceptuando las referencias a la dependencia del modelo del presionador. La estructura de bloques PIPED y PIPEM se conserva respecto al lazo 2.

Lado primario del SG de los lazos 1/3

Idéntico al modelo de lazo 2.

Rama fría de los lazos 1/3

Los lazos 1/3 presentan diferentes conexiones a otros sistemas y respecto al lazo 2, Figura 3.2:

- El lazo 1 presenta la descarga del CVCS en la rama intermedia, bloque 7736.
- El lazo 3 no presenta ni carga ni descarga del CVCS.
- Ambos lazos tienen conexiones relacionadas con la inyección del SIS, bloques 2286 y 2290.

A continuación se comentan las características principales del modelo de lazo 1/3.

Dependencias

- **Modelo de vasija**. Calcula la caída de presión del lazo sumando las caídas de cada bloque de la parte azimutal de la vasija correspondiente al lazo 1/3, añadiendo el tramo de la rama caliente modelado mediante un módulo PIPEM, bloques 2511, 2551, 2611, 3271 y 4501 (PIPEM).
- **Modelo del secundario correspondiente a los lazos de refrigeración 1/3**. La dependencia es recíproca, con el objeto de calcular el coeficiente de transmisión de calor en el generador de vapor, bloque 2001 (UASG). Este bloque requiere las temperaturas de los nodos de tubos y el caudal de paso, obteniéndolos del bloque 3531 (PIPED).
- **Modelo de la bomba de primario de los lazos de refrigeración 1/3**. Obtiene los parámetros de la linealización de la curva característica de la bomba del primario, bloque 4661 (CENTRIGFU) ramas 4663 y 4664, y el calor aportado por la bomba, bloque 23 (CTE), con un valor de 3.333333e+06 W, Figura 3.6.

- **Modelo del SIS**. El modelo debe suministrar el caudal y la entalpía correspondientes a la actuación de la inyección de seguridad directamente al bloque 2291 (MIXRVI) de entrada a la vasija.

Bloques relevantes

Similar a lo comentado para el modelo del lazo 2.

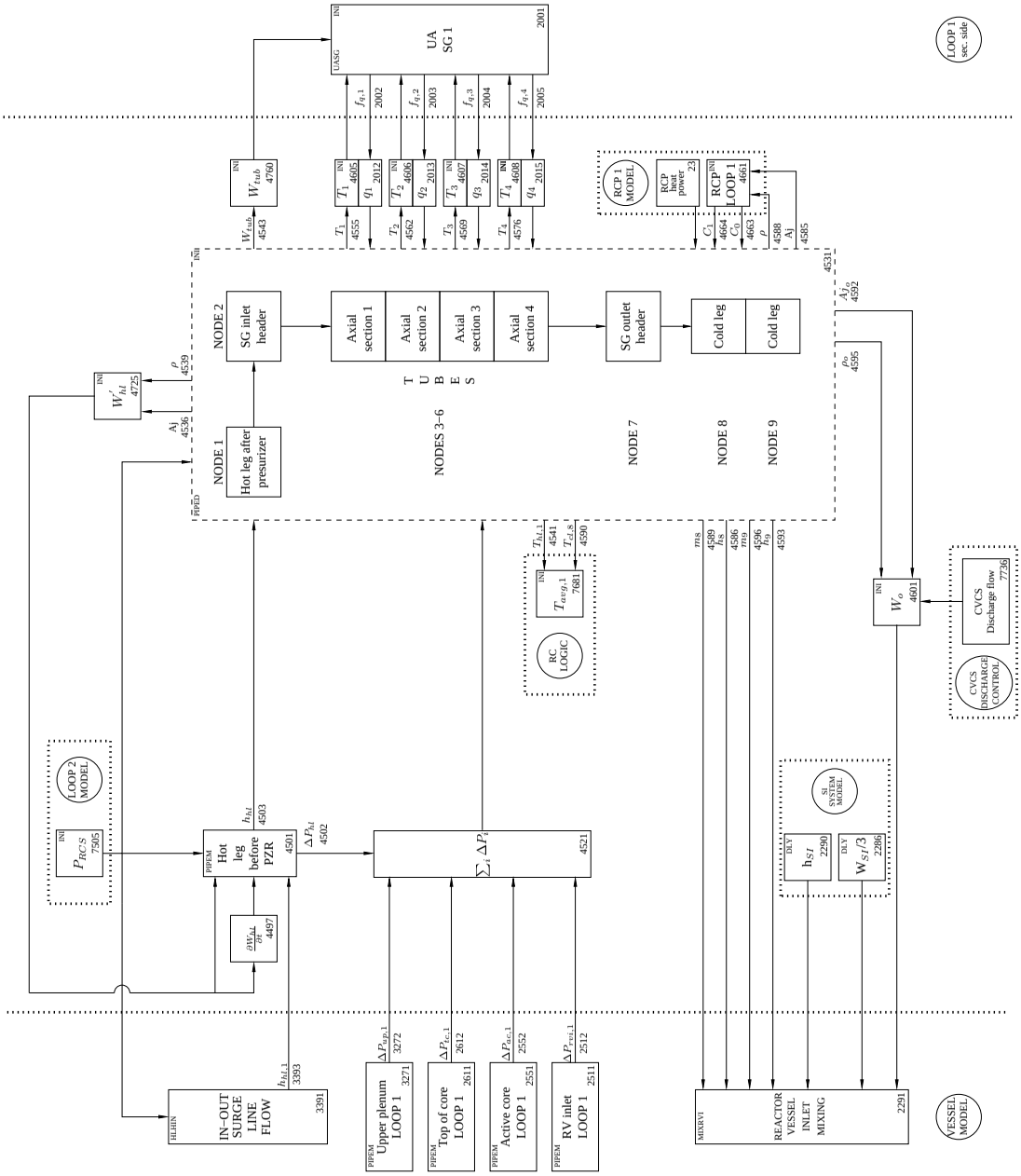


Figura 3.5: Modelo termohidráulico de los lazos sin presionador.

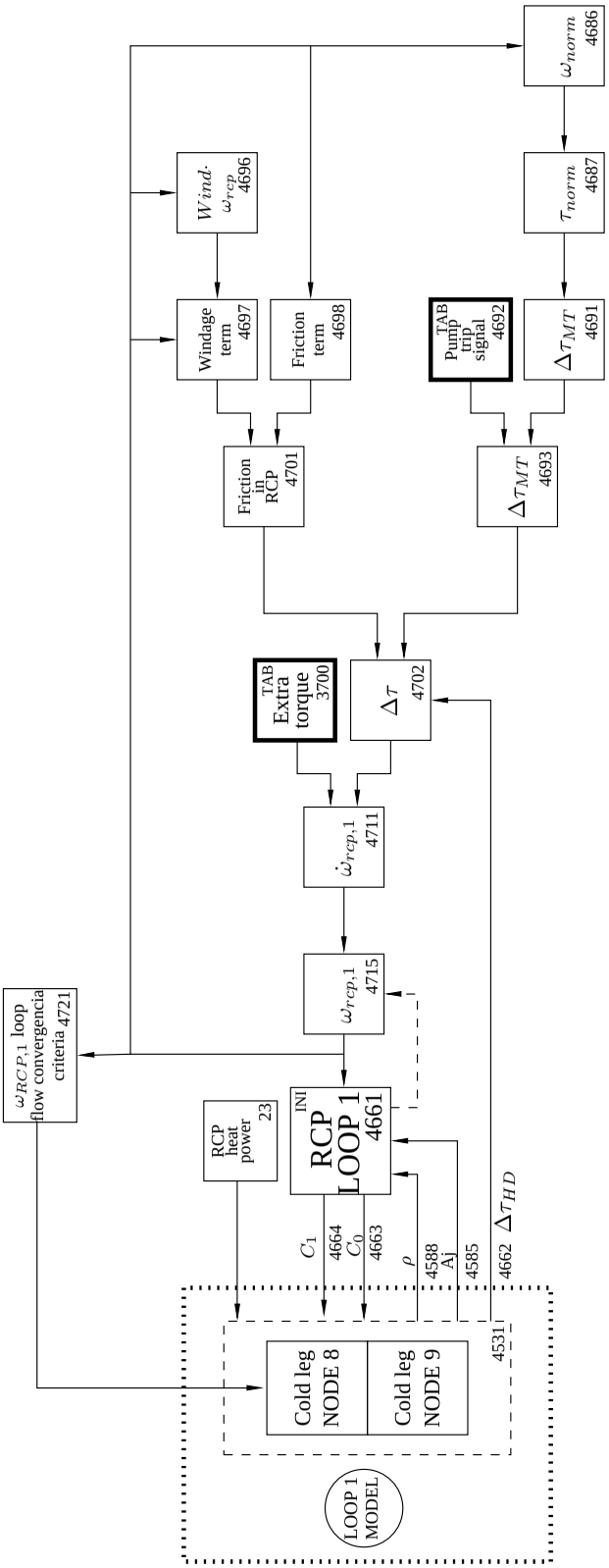


Figura 3.6: Modelo de la bomba de los lazos sin presionador.

3.1.2 Modelo de la vasija del reactor

Dentro del modelo de la vasija del reactor se puede distinguir entre el modelado de la termohidráulica de la vasija y la cinética del núcleo. Ambos se acoplan mediante la densidad del refrigerante/moderador y la transmisión de calor combustible-vaina-refrigerante.

3.1.2.1 Modelo de la termohidráulica de la vasija

El modelo se realiza considerando secciones azimutales del núcleo, una por cada lazo de refrigeración. En este modelo, al considerar tres lazos tomando dos de ellos simétricos, podremos reducir el núcleo a dos secciones azimutales.

Todo el modelado termohidráulico de la vasija se basa en módulos PIPEM, siendo la condición de contorno del modelo el caudal volumétrico de entrada a la vasija.

Los bloques más relevantes que conforman el modelo de la vasija se pueden clasificar en dos tipos:

- Los bloques encargados de simular la mezcla de caudales, MIXRVI, MIXRCO y SUMT.
- Los bloques correspondientes a tramos termohidráulicos, módulos tipo PIPEM, que realizan la resolución inversa de la ecuación del momento partiendo del caudal y de los coeficientes de fricción, obteniendo la caída de presión correspondiente en cada región de la vasija modelada.

Los bloques encargados de realizar el mezclado de caudales son:

- El mezclado de caudales a la entrada de la vasija, bloque 2291 (MIXRVI), que se encarga de simular el mezclado del caudal de los lazos de refrigeración en la bajante y el plenum inferior. La eficiencia del mezclado se especifica para cada bloque en el archivo de entrada.
- El mezclado en la parte superior de cada sección azimutal del núcleo del caudal del núcleo activo y el de *bypass*, bloques 2401 y 2601 (SUMT).
- El mezclado en el plenum superior de los caudales provenientes de cada sección azimutal del núcleo y de la cabeza de la vasija, bloque 3031 (MIXRCO).

Los bloques de la red termohidráulica de la vasija, módulos de tipo PIPEM/I, son:

- El bloque que modela los volúmenes de la bajante, o *downcomer*, y el plenum inferior. Se considera un bloque independiente para cada sección azimutal del núcleo, bloques 2311 y 2511 para los lazos 2 y 1/3. La mezcla de caudales en esta región del núcleo se modela mediante el bloque 2291 (MIXRVI).

- Las regiones activas de cada núcleo, bloques 2351 y 2551 para los lazos 2 y 1/3, donde se modelan los canales termohidráulicos correspondientes a los elementos combustibles.
- La parte superior de cada núcleo activo, bloques 2411 y 2611, volumen en el que se produce el mezclado del caudal activo y el de *bypass*, mezclado modelado en los bloques 2401 y 2601. En estos bloques se estiman a su vez las calidades dinámicas de salida, suministrándolas como datos al bloque 3031 (MIXRCO).
- La parte superior del núcleo, UPPER PLENUM.

Entrada de la vasija, bajante y plenum inferior

La entrada del caudal se produce a través de las ramas frías de los lazos a la vasija, en la cota de la placa soporte superior. Los caudales entran en un volumen formado por la bajante o *downcomer*, volumen de descenso hasta alcanzar la parte inferior de la vasija, y el plenum inferior produciéndose cierto mezclado de los caudales.

El bloque 2291 (MIXRVI) es el encargado de suministrar los caudales másicos y las entalpías a cada sección azimutal del núcleo, realizando el mezclado de los caudales. Este mezclado depende del parámetro de mezcla denominado *reactor vessel inlet mixing coefficient,* especificado en el archivo de entrada. Además, el bloque 2291 determina el caudal másico que se desvía a la cabeza de la vasija y su correspondiente entalpía.

El cálculo de las ecuaciones de conservación se realiza en los bloques 2311 y 2511, módulos tipo PIPEM donde se modelan de forma separada los volúmenes de la bajante y el plenum inferior de las secciones azimutal del núcleo para el lazo 2 y 1/3. De este cálculo se obtiene la caída de presión en ambos volúmenes para cada lazo de refrigeración. A partir de los caudales de paso por cada sección azimutal del núcleo, ramas 2314 y 2515 para cada sección azimutal, se calcula el caudal de *bypass* (no calentado) mediante una relación de proporcionalidad y el caudal activo, caudal que atraviesa la región calentada del núcleo. En la separación de caudales de *bypass* y activo solamente se considera el balance entálpico de la distribución de caudales, despreciando efectos hidráulicos como el ajuste de las caídas de presión.

Núcleo activo

La termohidráulica de cada sección azimutal del núcleo activo se modela con los bloques 2351 y 2551, para los lazos 2 y 1/3 respectivamente. Son módulos tipo PIPEI, con una nodalización similar a la empleada para el perfil axial de potencia. El perfil axial de potencia se comenta en detalle en el modelo del núcleo, Sección 3.1.2.2.

Cada sección azimutal modela un canal termohidráulico sin considerar posibles flujos cruzados entre ellos. La transferencia de calor al refrigerante se calcula en función del gradiente de temperaturas refrigerante-combustible con un coeficiente de transmisión global calculado en el modelo térmico del núcleo, bloques 2151 y 2191 (QCALC) para los lazos 2 y 1/3.

Parte superior del núcleo

A la salida de cada sección azimutal del núcleo activo, en la cota correspondiente a la placa soporte superior, se produce la mezcla del caudal activo con el caudal de *bypass*, bloques 2401 y 2601 (SUMT), para las secciones azimutales del lazo 2 y 1/3.

Dependencias

- **Modelo de los lazos de refrigeración 1/3**. Requiere como entradas para el bloque 2291 (MIXRVI), de mezclado a la entrada de la vasija y distribución de caudales de las secciones azimutales del núcleo, la masa y entalpía del refrigerante de los dos nodos correspondientes a la rama fría de cada lazo, ramas 4589, 4586, 4596 y 4593.
- **Modelo del lazo de refrigeración 2**. Requiere como entradas para el bloque 2291 (MIXRVI), de mezclado a la entrada de la vasija y distribución de caudales de las secciones azimutales del núcleo, la masa y entalpía del refrigerante de los dos nodos correspondientes a la rama fría de cada lazo, ramas 3589, 3586, 3596 y 3593.

  La presión del RCS, rama 7505, se suministra a todos los bloques de la vasija que se corresponden con módulos PIPEM/I, para posibilitar el cálculo de las propiedades del fluido.
- **Modelo del SIS**. Como entradas para el bloque 2291, de mezclado a la entrada de la vasija y distribución de caudales de las secciones azimutales del núcleo, se requieren la entalpía y el caudal del modelo del sistema de SI, ramas 2290 y 2286, respectivamente.
- **Modelo del núcleo**. La dependencia es recíproca, debido a las realimentaciones existentes entre la neutrónica y la termohidráulica del núcleo. Por ello, el modelo neutrónico requiere del bloque 2351 (PIPEI), canal termohidráulico del núcleo activo, las densidades del moderador/refrigerante en cada nodo axial del núcleo activo, ramas 2360 a 2395 (n+7). Además, al realizarse el cálculo de la transmisión de calor en el modelo del núcleo, requiere la temperatura del refrigerante en cada nodo, ramas 2362 a 2397 (n+7). Finalmente, comentar que las entradas de flujo calorífico en cada nodo termohidráulico del núcleo activo se corresponden con las ramas 2181 a la 2186 para el bloque 2351 y de la 2221 a la 2226 para el bloque 2551 del modelo de la vasija, lazos 2 y 1/3 respectivamente.

Bloques relevantes

Debido a que el modelo ya ha sido comentado en suficiente detalle en las secciones anteriores, aquí sólo se muestra, a modo de resumen, una lista de los bloques que lo componen.

Así, para los bloques de mezclado de caudal tenemos:

- Mezclado de caudal a la entrada de la vasija y distribución de caudales a secciones azimutales del núcleo y cabeza de la vasija, bloque 2291 (MIXRVI).

- Mezclado de los caudales provenientes del núcleo activo y del *bypass* en la parte superior del núcleo, bloques 2401 y 2601 (SUMT) para los lazos 2 y 1/3.
- Mezclado y distribución de caudales en las distintas regiones de la parte superior de la vasija, bloque 3031 (MIXRCO).

Para los bloques relacionados con el modelo termohidráulico se tiene:

- Los volúmenes relacionados con el *downcomer* y el plenum inferior de la vasija, bloques 2311 y 2511 para los lazos 2 y 1/3.
- Núcleos activos de las dos secciones azimutales del núcleo, bloques 2351 y 2551 para los lazos 2 y 1/3.
- Parte superior del núcleo, donde se modela la termohidráulica de elementos estructurales, bloques 2411 y 2611 para los lazos 2 y 1/3.
- Los bloques correspondientes a los diferentes tipos de volúmenes en que se ha divido el plenum superior de la vasija, bloques 3141, 3151, 3171 y 3271.

Los bloques encargados de modelar la termohidráulica de la vasija, módulos PIPEM/I, calculan la caída de presión asociada al paso del fluido por los elementos estructurales que se incluyen en el volumen modelado. Esta caída es suministrada a los bloques 3521 y 4521, modelo del lazo 2 y de los lazos 1/3, para obtener la caída de presión total del lazo.

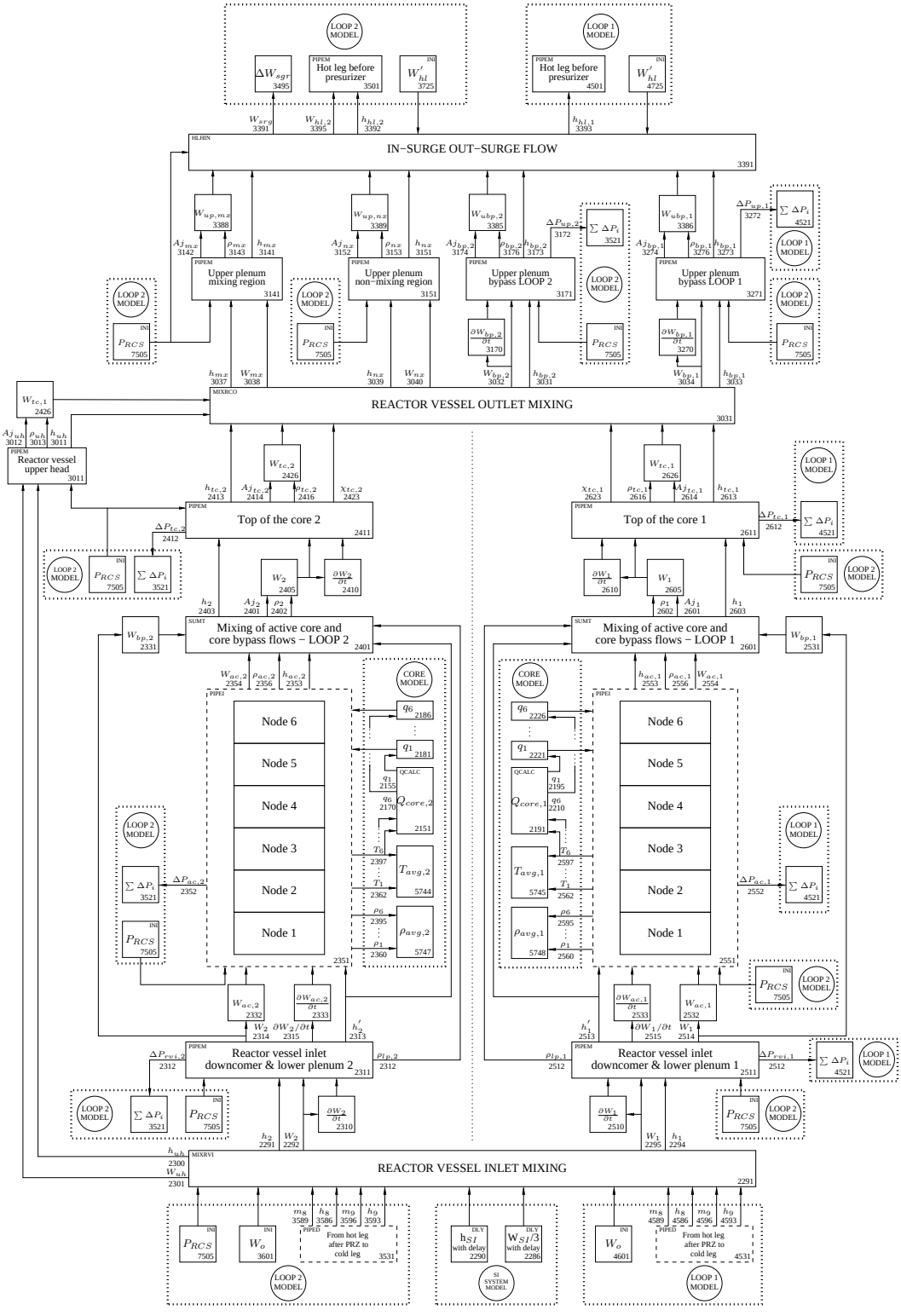


Figura 3.7: Modelo termohidráulico de la vasija.

3.1.2.2 Modelos de cálculo de potencia y de transmisión de calor

El modelo del núcleo se ha realizado considerando un modelo colapsado de transferencia de calor, un modelo neutrónico de cinética puntual y un modelo para el calor residual, Figura 3.8.

En el **modelo de cinética** se usan seis grupos de neutrones diferidos, un término fuente y la vida media de los neutrones, bloque 2105. El modelo considera cambios de la reactividad provocados por:

- la variación de la temperatura del moderador,
- el efecto Doppler,
- concentración de boro (bloque 2088),
- y por posición de las barras de control y valores de reactividad debidos al disparo del reactor (bloques 2085 y 2084), Figuras 3.9 y 3.10.

Los asociados a boro y factores externos no están modelados, estando actualmente con valor nulo constante. El coeficiente del moderador, el coeficiente Doppler y el defecto integral Doppler función de la potencia con corrección para variaciones de la temperatura del refrigerante, se especifican en el archivo de entrada en el bloque 2088. La función de la reactividad insertada por disparo del reactor en función del tiempo puede ser especificada por el usuario en el bloque 2083 y la reactividad aportada por la inserción de las barras de control frente a su posición en el bloque 2085.

Para simular el **calor residual**, se usa un modelo de cinco grupos de precursores, similar al empleado para los precursores de neutrones diferidos, aunque puede ser empleado el estándar del ANSI-51.1, bloque 2110 (CONVEX), Figura 3.8

El **modelo de transferencia de calor**, Figura 3.8, usa un número fijo de nodos axiales especificado por el usuario, y un solo nodo azimutal por cada lazo. Dentro del modelo se calcula el coeficiente promediado de transferencia de calor al refrigerante (UA) como función del promediado de la temperatura radial del combustible, aunque puede ser especificada una función parabólica para su estimación. A su vez, se emplea otro ajuste parabólico para estimar la capacidad calorífica del combustible en función de su temperatura, bloques 2151 y 2191 (QCALC) para los lazos 2 y 1/3. El perfil axial de potencia sigue una distribución parabólica, con una relación 1.5 del máximo con el valor promedio, bloques 2147, 2148 y 2149. Se supone que un 2.6 % de la potencia se deposita directamente en el refrigerante, bloque 2146, el resto se transfiere vía combustible-refrigerante, siendo los bloques del 2181 hasta el 2186 para el lazo 2 y los bloques del 2221 hasta el 2226 para los lazos 1/3 los que estiman el flujo calorífico para cada nodo axial. Se obtienen el coeficiente global de transferencia de calor del núcleo, bloque 2268, y la constante de tiempo global de transferencia de calor en el núcleo, bloque 2269.

Dependencias

- **Modelo de la vasija**. La dependencia es recíproca, debido a las realimentaciones existentes entre la cinética y la termohidráulica del núcleo. Por ello, el modelo neutrónico requiere de los bloques 2351 y 2551 (PIPEI) las densidades del moderador/refrigerante en cada nodo axial de los núcleos activos, ramas 2360 a 2395 y 2560 a 2595(n+7). Además, al realizarse el cálculo de la transmisión de calor en este parte del modelo, requiere la temperatura del refrigerante en cada nodo, ramas 2362 a 2397 y 2562 a 2597(n+7). Finalmente, resta comentar las salidas de flujo calorífico en cada nodo termohidráulico del núcleo activo, ramas de la 2181 a la 2186 para el bloque 2351 y de la 2221 a la 2226 para el bloque 2551 del modelo de la vasija, lazos 2 y 1/3 respectivamente.
- **Modelo del sistema de barras de control**. El sistema de control de las barras de control suministra al modelo de la cinética, Figuras 3.9 y 3.10:
  - la posición efectiva de las barras de control en operación normal, bloque 8033, para el cálculo de la reactividad insertada por las barras,
  - y la señal de disparo de reactor, bloque 8021, para que a partir de la función de disparo de barras del modelo, es decir, la posición de los bancos de parada en función del tiempo, bloque 2083, estimar la reactividad insertada en caso de producirse el disparo del reactor.
- **Modelo de la lógica de los disparos del reactor**. La lógica de disparos del reactor requiere del modelo neutrónico el flujo neutrónico calculado por el bloque 2105 para las entradas de las diferentes señales de los disparos.

Bloques relevantes

Como ya se ha comentado en la descripción del **modelo de transferencia de calor**, se obtienen el coeficiente global de transferencia de calor del núcleo, bloque 2268, y la constante de tiempo global de transferencia de calor en el núcleo, bloque 2269, de especial relevancia a la hora de realizar el balance de reactividad total del núcleo. En lo que respecta para el **modelo de cinética puntual**, destacar el bloque que ejecuta el balance global de reactividad, bloque 2088, basándose en los coeficientes de moderador y Doppler, barras de control frente a su posición y el defecto integral Doppler en función de la potencia con corrección para variaciones de la temperatura del agua suministrados en el archivo de entrada.

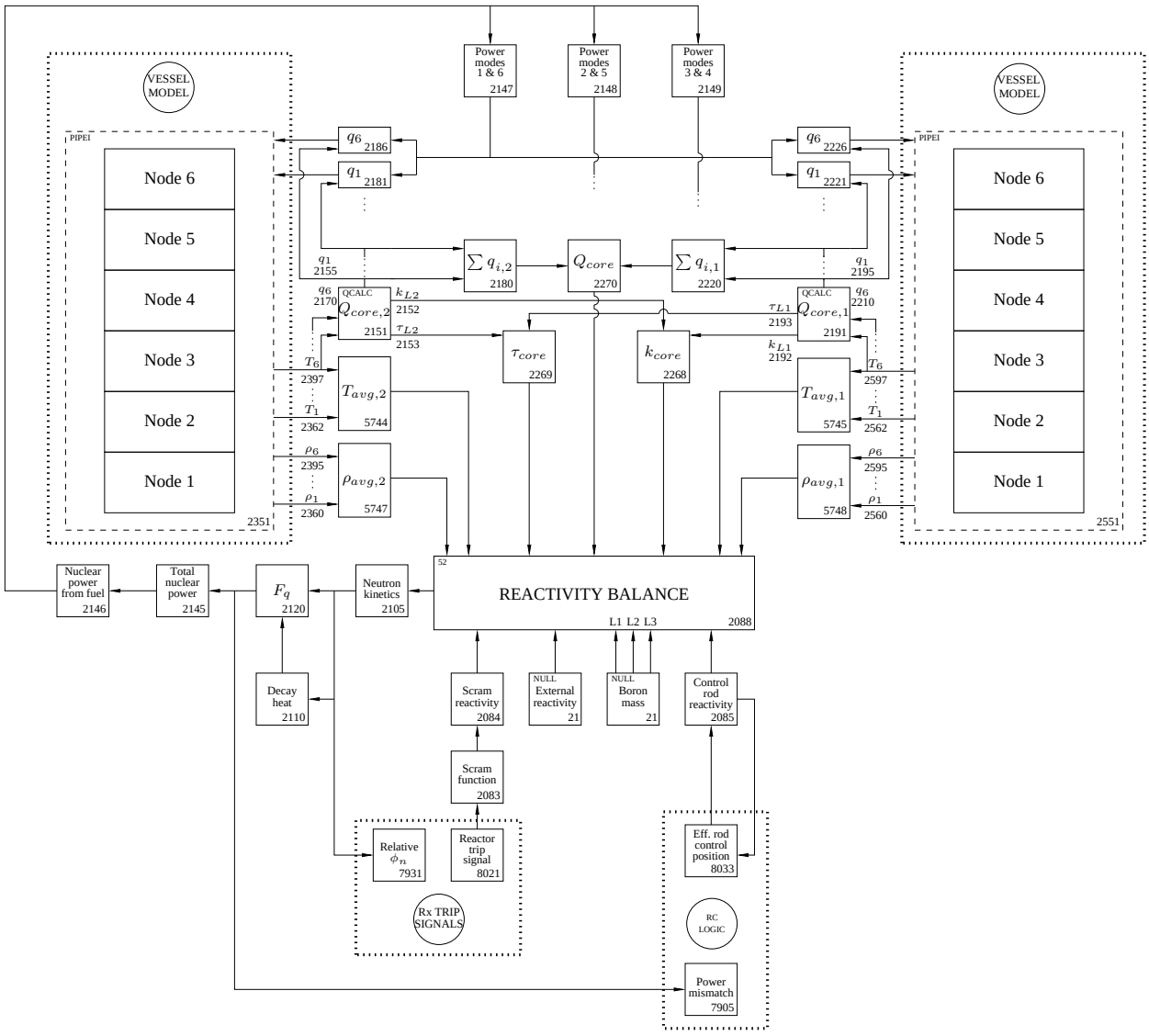


Figura 3.8: Esquema de cálculo de la potencia y de la transferencia de calor del núcleo.

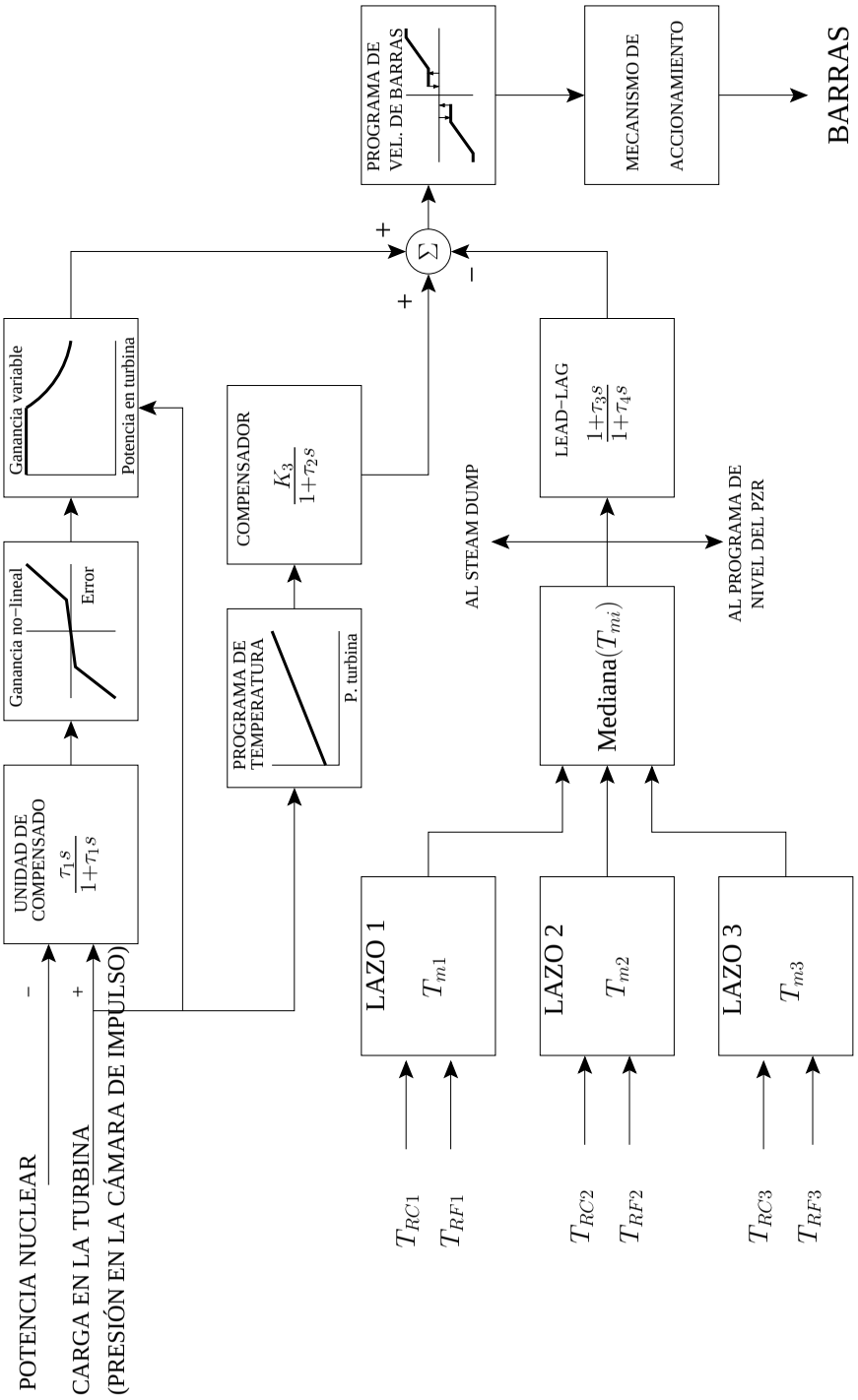


Figura 3.9: Esquema del sistema de barras de control.

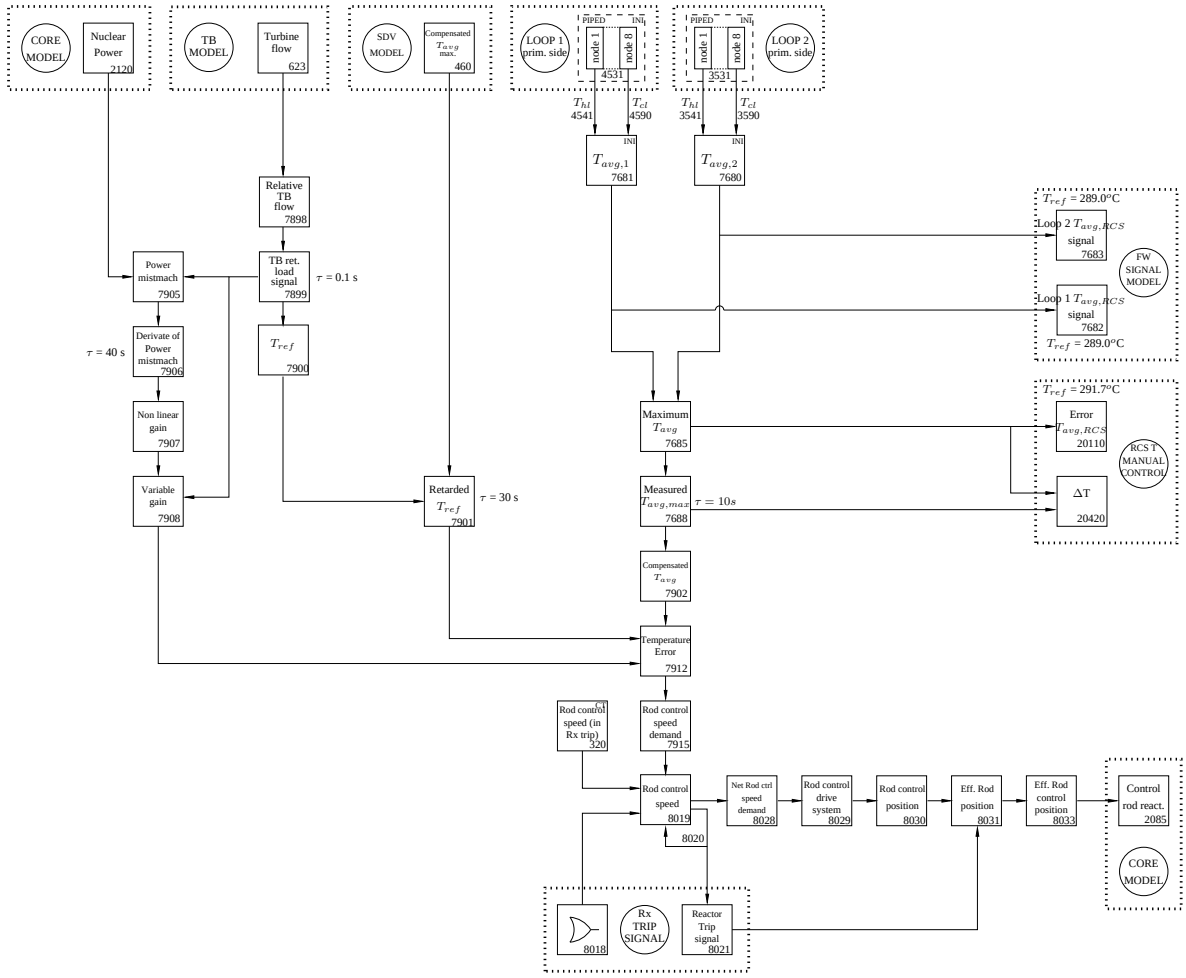


Figura 3.10: Modelo del sistema de las barras de control.

3.1.3 Modelo del presionador y de los controles relacionados

En el **modelo termohidráulico del presionador** se realiza el balance de masa y energía empleando dos regiones, de líquido y vapor, con un esquema de volúmenes de control variable de forma que se puede modelar el cambio de nivel del presionador en condiciones de transitorio. Se suponen volúmenes de mezcla perfecta, considerando condensación y sobrecalentamiento en la región de vapor y evaporación y subenfriamiento en la región líquida. Las burbujas y las gotas se modelan considerando modelos de velocidad constante, bloque 7161, Figura 3.11. Estos volúmenes de control conforman un cilindro que incluye, con idéntica sección, el volumen de la línea de conexión con el lazo 2.

Se considera en el modelo:

- el efecto de calentadores, tanto proporcionales como de apoyo,
- y la actuación de las válvulas de alivio, seguridad y rociado.

Por ello, al bloque 7161 (PRES1) entran las ramas 7100 y 450, asociadas con los calentadores y las pérdidas de calor en el presionador, éstas últimas modeladas con una constante, bloque 450. Las ramas 7050 y 3532 (bloque 3531, PIPED del lazo 2) proporcionan el caudal de rociado y la entalpía del mismo y, finalmente, las ramas 7150 y 7130 asociadas al caudal y la entalpía de las válvulas de alivio de vapor.

El **sistema de control de presión del presionador** obtiene las demandas para el rociado, las válvulas de alivio y seguridad y los calentadores, Figuras 3.12 a 3.14. El error en presión, calculado a partir de la presión y su valor nominal, se emplea para controlar el rociado proporcional y los calentadores, tanto de apoyo como proporcionales. Los caudales másicos de las válvulas de alivio y seguridad son modelados mediante tablas en función de la presión del presionador, bloques 7145 y 7140 para los caudales volumétricos. Para determina si el caudal evaucado por las válvulas es líquido o vapor se tomando como origen la cota de calentadores y se calcula la cota de la interfase de ambos fluidos para saber si alcanza la cota de las válvulas de descarga. A su vez, considerando dicho nivel, se anula la demanda de calentadores en caso de posible descubrimiento de los mismos, señal de bajo nivel en el presionador, bloque 7090. El caudal de las válvulas de alivio y seguridad de líquido o vapor se calcula de forma directa en función de la presión y la dependencia debe ser suministrada por el usuario en el archivo de entrada.

El **control de nivel del presionador** conecta con el bloque 7740, Figuras 3.15 a 3.17, realizando los ajustes necesarios en el caudal de carga del CVCS para mantener en nivel en el valor de referencia obtenido considerando la temperatura media del refrigerante.

Dependencias

Modelo del lazo de refrigeración 2. La presión del primario se obtiene del modelo del presionador, bloque 7161, corrigiéndose con la caída de presión correspondiente a la tubería de conexión con el lazo 2 del RCS, bloques 7181 - 7185.

Las dependencias que presenta del modelo del lazo 2 son:

- El caudal de entrada o salida al presionador desde la rama caliente, rama 3495. Es positivo en caso de corresponderse con la entrada de caudal, *in-surge flow*, y negativo en caso de ser de salida, *out-surge flow*. Este caudal tiene un limitador a $\pm$ 1000 kg/s, bloque 3496.
- La entalpía del fluido en la región de líquido del presionador para el caso en que se produzca salida de caudal del presionador a la rama caliente del lazo 2, rama 7166.
- Para el caso en que se produzca entrada de caudal al presionador desde la rama caliente del lazo 2, requiere la entalpía del fluido de la rama caliente, rama 3503.
- El caudal de la válvula de rociado requiere el caudal volumétrico que circula por la rama fría, rama 3592, y su entalpía, rama 3532.

Bloques relevantes

El bloque central es el 7161 (PRES1), ya comentado en la descripción del modelo.

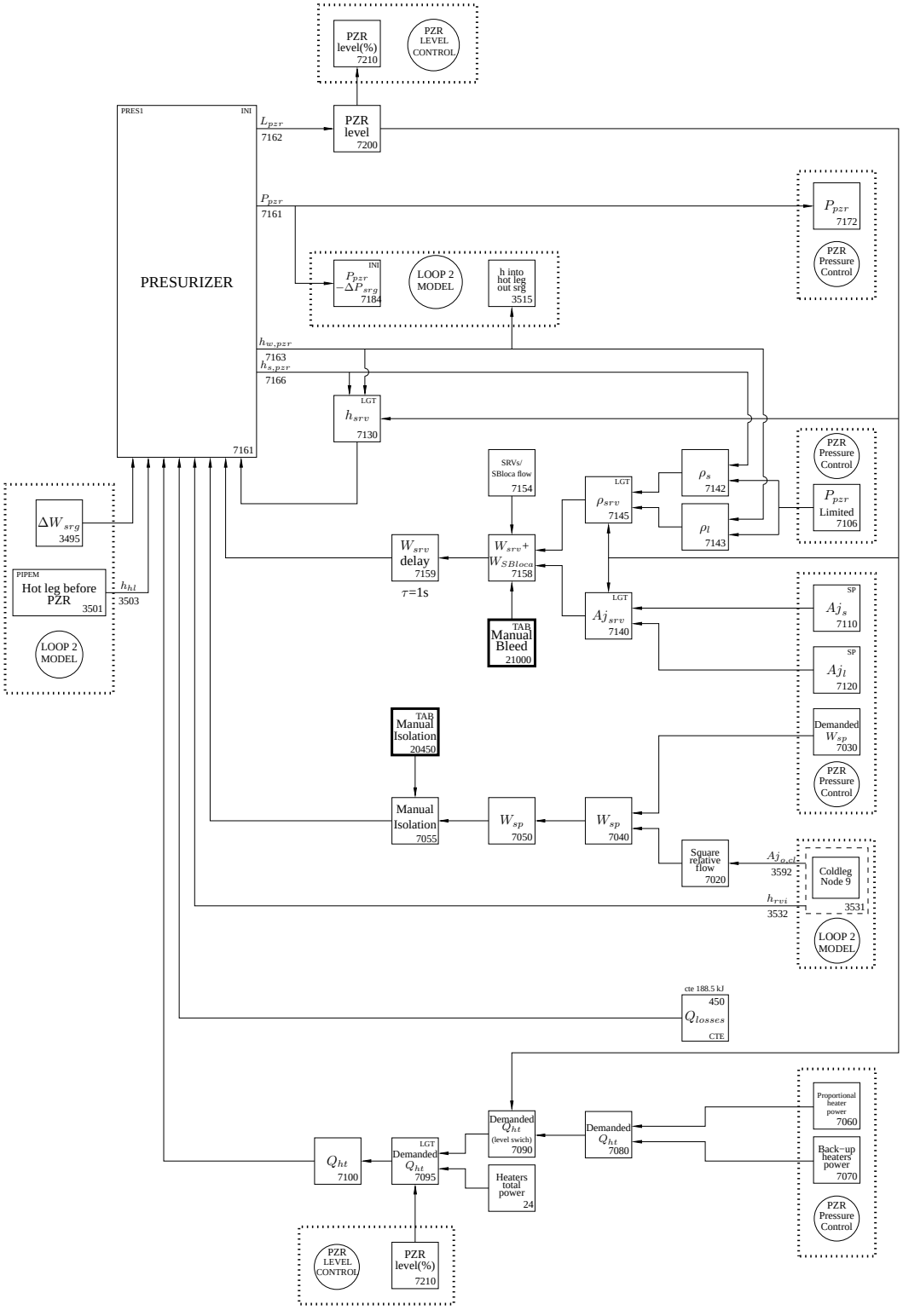


Figura 3.11: Modelo del presionador y sistemas asociados.

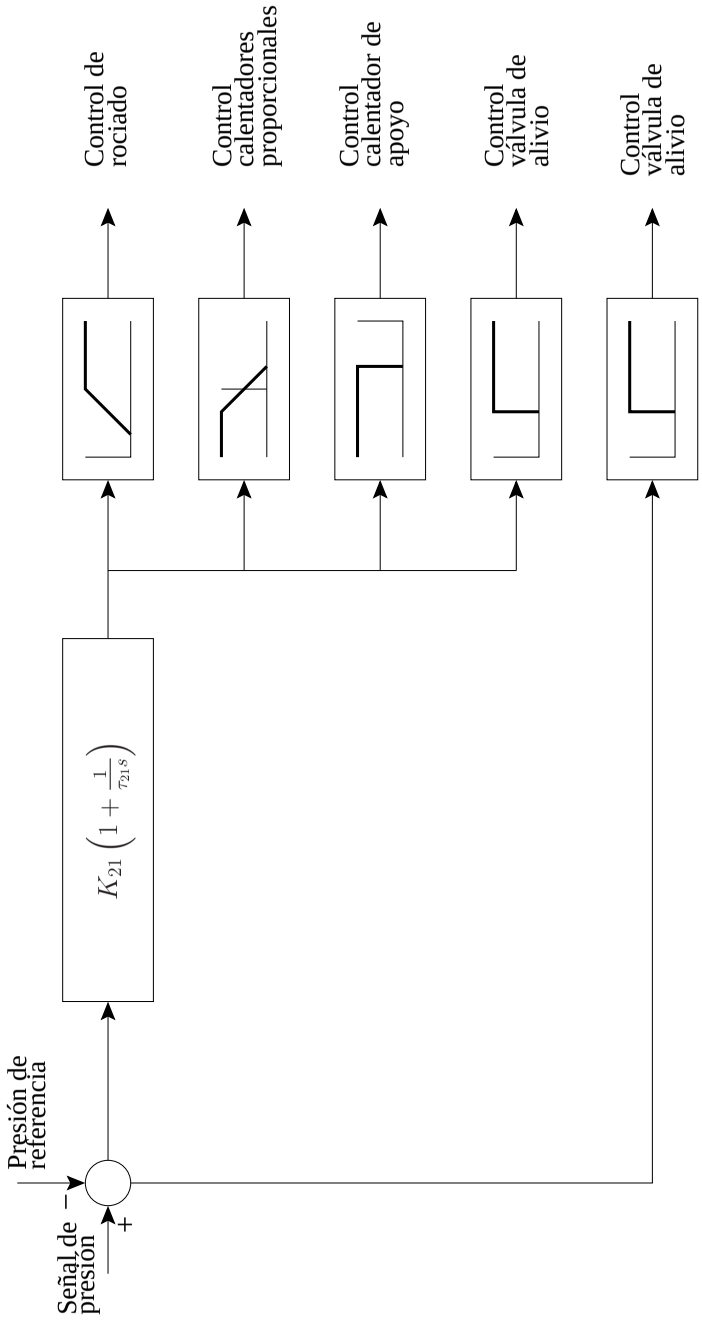


Figura 3.12: Esquema del control de presión del presionador.

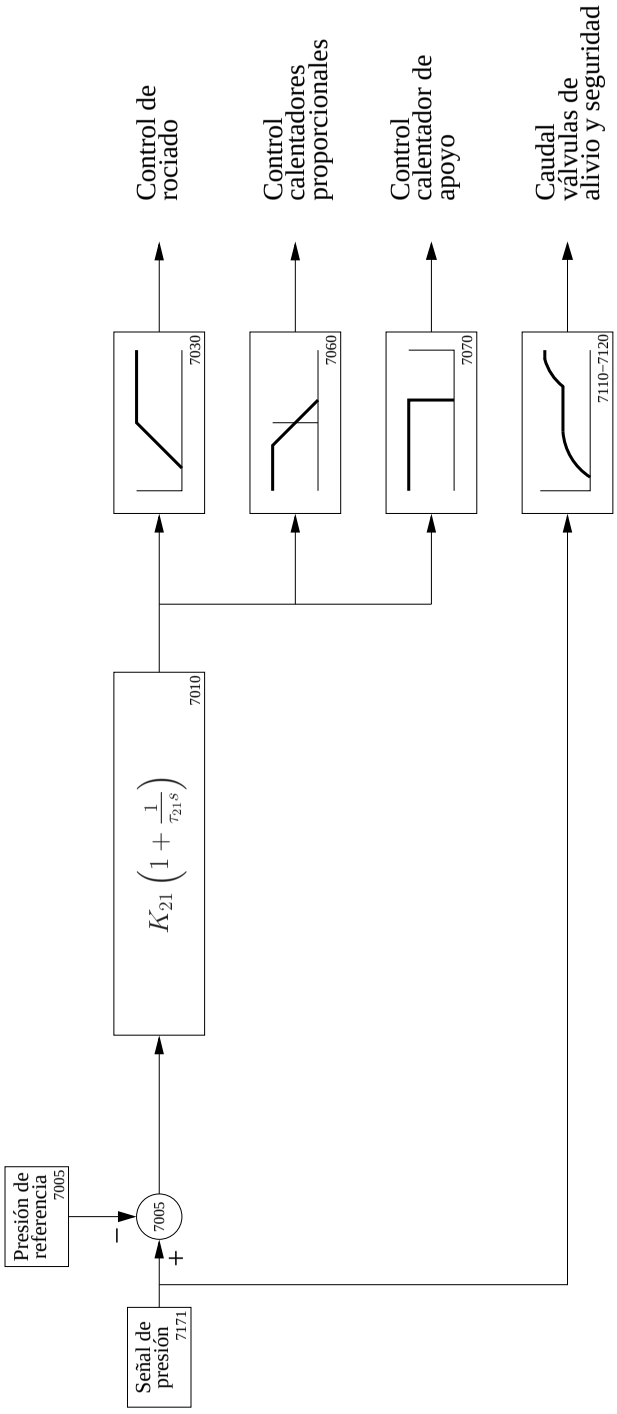


Figura 3.13: Esquema del modelo del control de presión del presionador usado en el modelo de planta.

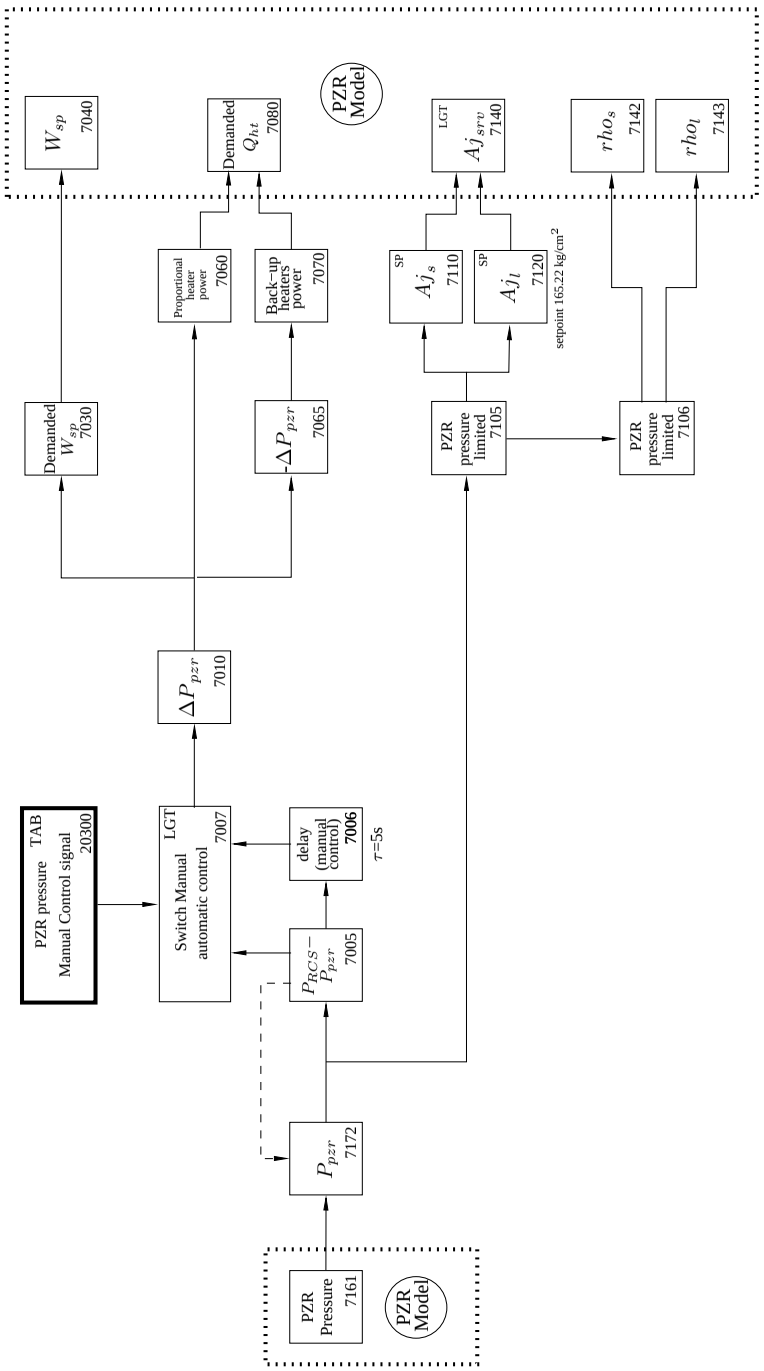


Figura 3.14: Modelo del control de presión del presionador.

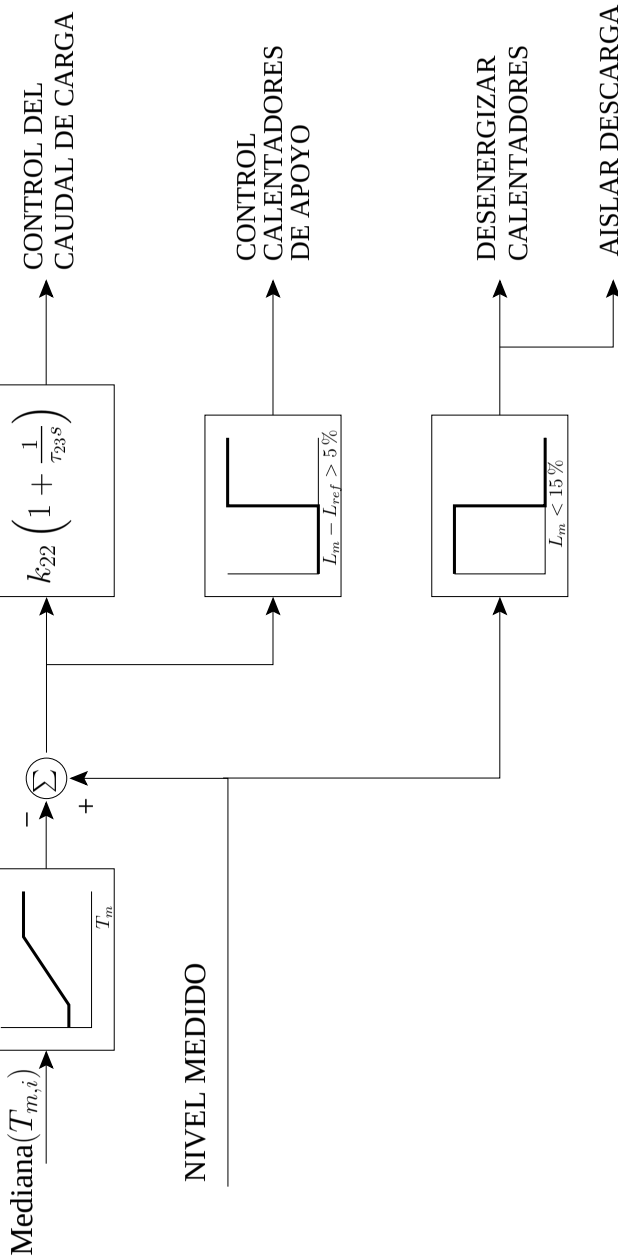


Figura 3.15: Esquema del modelo del control de nivel del presionador.

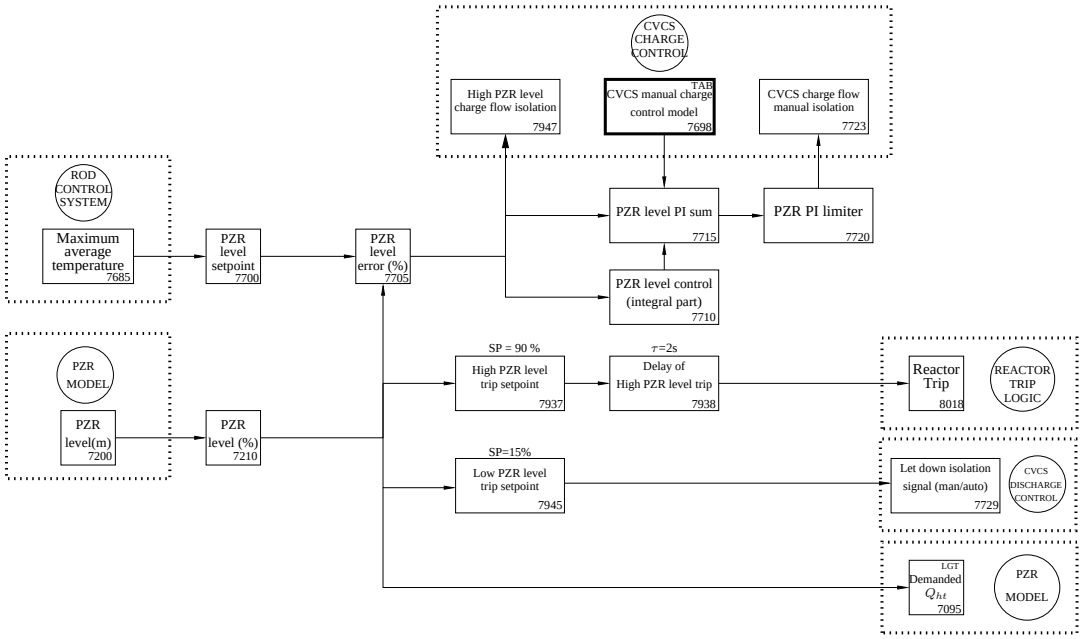


Figura 3.16: Modelo del control de nivel del presionador.

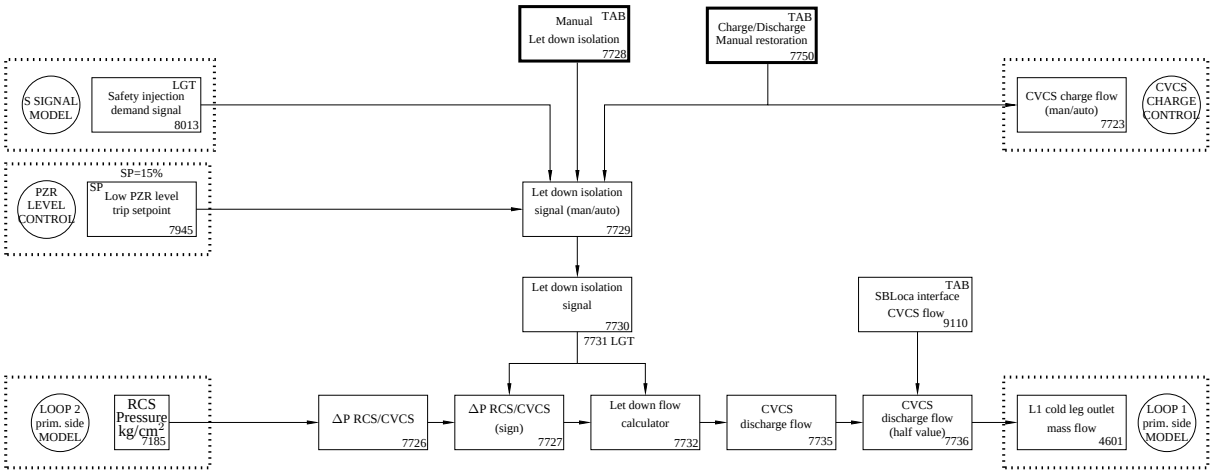


Figura 3.17: Modelo del control de descarga del CVCS.

3.1.4 Modelo del secundario

Para cada modelo de lazo de refrigeración se ha modelado su correspondiente generador de vapor y la línea de vapor hasta el colector, Figuras 3.18 y 3.19. Además de comentarse en detalle estos modelos, se incluyen esquemas de los modelos de turbina y de alivio de vapor al condensador en sus diferentes modos de operación, Figuras 3.20 a 3.23.

3.1.4.1 Parte del secundario correspondiente al lazo con presionador

Esta parte del modelo se compone del modelo del generador de vapor asociado al lazo 2 y la línea de vapor hasta el colector de la línea de vapor principal.

El modelo del generador de vapor se ha realizado considerando el nodalizado correspondiente al lado primario de tubos, bloques 3531 y 4531 (PIPED), para los lazos 2 y 1/3, y para el lado de tubos del SG, bloques 1951 y 2001 (UASG).

La transmisión de calor se calcula empleando el coeficiente de transmisión promediado (UA) calculado en los bloques 1951 y 2001 (UASG). La región de transmisión se divide en tres partes:

- Transmisión en película para la zona primaria. Donde se emplea el modelo de transmisión de calor por convección forzada de Dittus-Boelter con un coeficiente de transmisión dependiente del caudal de tubos, bloque 3760.
- Trasmisión por el tubo metálico.
- Transmisión en película con ebullición para el lado secundario de los tubos. Donde se emplea el modelo de Jens-Lottes para ebullición nucleada, con dependencia del flujo calorífico y la presión en el SG.

El promediado de la resistencia térmica total se realiza en los bloque 1951 y 2001 (UASG) para cada lazo, fijando el peso de cada región en el promediado con parámetros de entrada de estos bloques fijados por el usuario. Además, se da la posibilidad de simular la degradación de la transmisión de calor en los tubos por pérdida de inventariado en los SG y descubrimiento de los mismos. Así, se suministra el inventario de carcasa del SG, bloques 1995 y 1945 para los SG 1/3 y 5 respectivamente, a partir de su cálculo volumétrico. Si el inventariado existente es inferior al considerado se simula de forma lineal el efecto de la degradación de la transmisión de calor por el secado de los tubos, bloque 1951 (UASG).

El lado secundario del SG se modela como un solo volumen colapsado donde se calculan las propiedades del fluido, considerado como una mezcla de vapor y líquido saturado. La presión del vapor, su entalpía y la densidad son evaluadas en función de la temperatura del fluido. Las estructuras de calor del SG se suponen a la temperatura del vapor saturado, obteniendo así la capacidad calorífica del sistema, bloques 1282 y 1482 (FUNIN).

El caudal de vapor de salida de cada SG se obtiene realizando el balance de masa en el colector de la línea de vapor principal, bloque 630, calculando la densidad del vapor en el colector, bloque 632, y ajustando la caída de presión en la línea de vapor de cada SG, bloque 610, mediante la ecuación:

$$P_2 - P_h = K \cdot \frac{W_s^2}{\rho_s}$$

donde la constante de pérdidas, *K*, se calcula para ajustar las pérdidas de la línea de vapor en condiciones nominales de potencia.

Dependencias

- **Modelo del lazo de refrigeración 2**.

  La dependencia es recíproca, con el objeto de calcular el coeficiente de transmisión de calor en el generador de vapor, bloque 1951 (UASG). Este bloque requiere las temperaturas y el caudal de tubos, obteniéndolos del bloque 3531 (PIPED) del modelo del lazo de refrigeración, y da el flujo calorífico para cada nodo de la región de tubos del SG.

- **Modelo del secundario de los lazos de refrigeración 1/3**.

  Para realizar el balance másico en el colector de vapor principal, bloque 630, requiere el caudal de vapor aportado por los lazos restantes, bloque 618.

- **Modelo de la válvula de alivio de vapor de la línea de vapor**.

  Este modelo, basándose en la presión medida en el SG, bloque 1320, simula la apertura de las válvulas de alivio, bloque 349, y calcula el caudal crítico de salida por ellas, bloque 600, suministrándolo al cálculo del caudal total de vapor que circula por la línea del modelo de secundario del lazo 2, bloque 649.

- **Modelo de las válvulas de alivio al condensador**.

  Requiere el caudal de turbina, bloque 623, para estimar el balance de carga-potencia, y proporciona al modelo la apertura de las válvulas de descarga al condensador, bloque 540, de forma que puede estimar el caudal de descarga de vapor, bloque 621, e incluirlo en el balance másico del colector de vapor principal, bloque 630, Figura 3.23. El modelo cuenta con la implementación del modo de operación en temperatura en condiciones de disparo de turbina y rechazo de carga, cuyo funcionamiento está representado de forma esquemática en las Figuras 3.22 y 3.21, respectivamente.

- **Modelo de la turbina**.

  Proporciona al modelo la apertura de las válvulas de control de turbina, bloque 210, de forma que puede estimar el caudal de vapor demandado por la turbina, bloque 623, e incluirlo en el balance másico del colector de vapor principal, bloque 630, Figura 3.20.

- **Modelo de cálculo del nivel del SG**.

  El cálculo del nivel de los SG se realiza a partir del balance de masa del lado secundario del SG, bloque 1219. Para una descripción en detalle consultar la Sección 3.1.5.2.

- **Modelo del FWS**.

  El caudal de agua de alimentación y su entalpía se obtienen del modelo del FWS, siendo los bloques 1115 y 715 los correspondientes a los caudales de FW de ambos SG, lazo 1/3 y lazo 2, y el bloque 1180 el correspondiente a la entalpía del FW.

- **Modelo de roturas de secundario**.

  El modelo de roturas de secundario, comentado en de detalle en la Sección 3.1.7, aporta al modelo el caudal de la rotura, bloques 63 y 65 según se simule la rotura en la línea de vapor del lazo 2 o en el colector de vapor de las líneas de vapor, de forma que se considera en la obtención del caudal de vapor de los SG.

- **Modelo de aislamiento de las líneas de vapor**.

  La señal de aislamiento de la línea de vapor, bloque 8065, se combina con el cálculo del caudal de vapor de cada SG de forma que anule su valor en caso de producirse, bloques 618 y 613 de los lazos 1/3 y 2, respectivamente. El modelo se ha implementado de forma que en caso de rotura no aislable, ver modelo de roturas de secundario en la Sección 3.1.7, el caudal del SG del lazo afectado resulte ser el caudal saliente por la rotura.

Bloques relevantes

Los bloques centrales del modelo son el 1951 (UASG) y el 1282 (FUNIN). El bloque 1951 se encarga de calcular el coeficiente de transmisión de calor global del SG, aportando los flujos caloríficos en cada nodo de tubos y el calor total extraído del primario para el bloque 1282 (FUNIN). Este bloque realiza el balance térmico del SG, obteniendo la energía acumulada en el SG, rama 1282, de forma que se puede estimar la temperatura del sistema, bloque 1300 (VALCT), y suponiendo condiciones de saturación, obtener la presión del SG en el lado de carcasa, bloque 1320 (FUNIN).

3.1.4.2 Parte del secundario correspondiente a los lazos sin presionador

Similar al modelo del lazo con presionador, lazo 2.

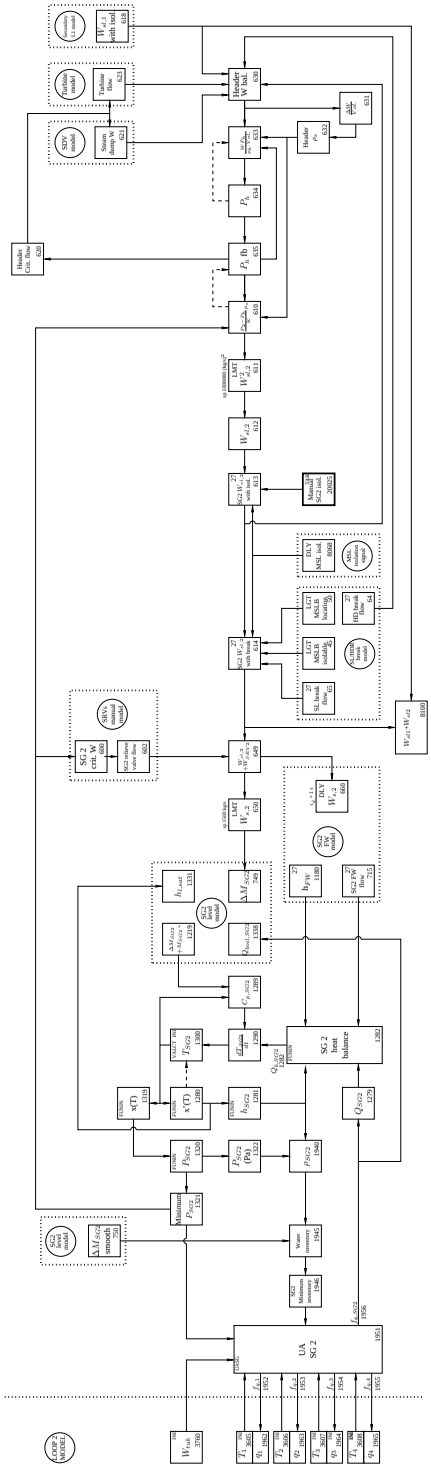


Figura 3.18: Modelo termohidráulico del secundario del lazo con presionador.

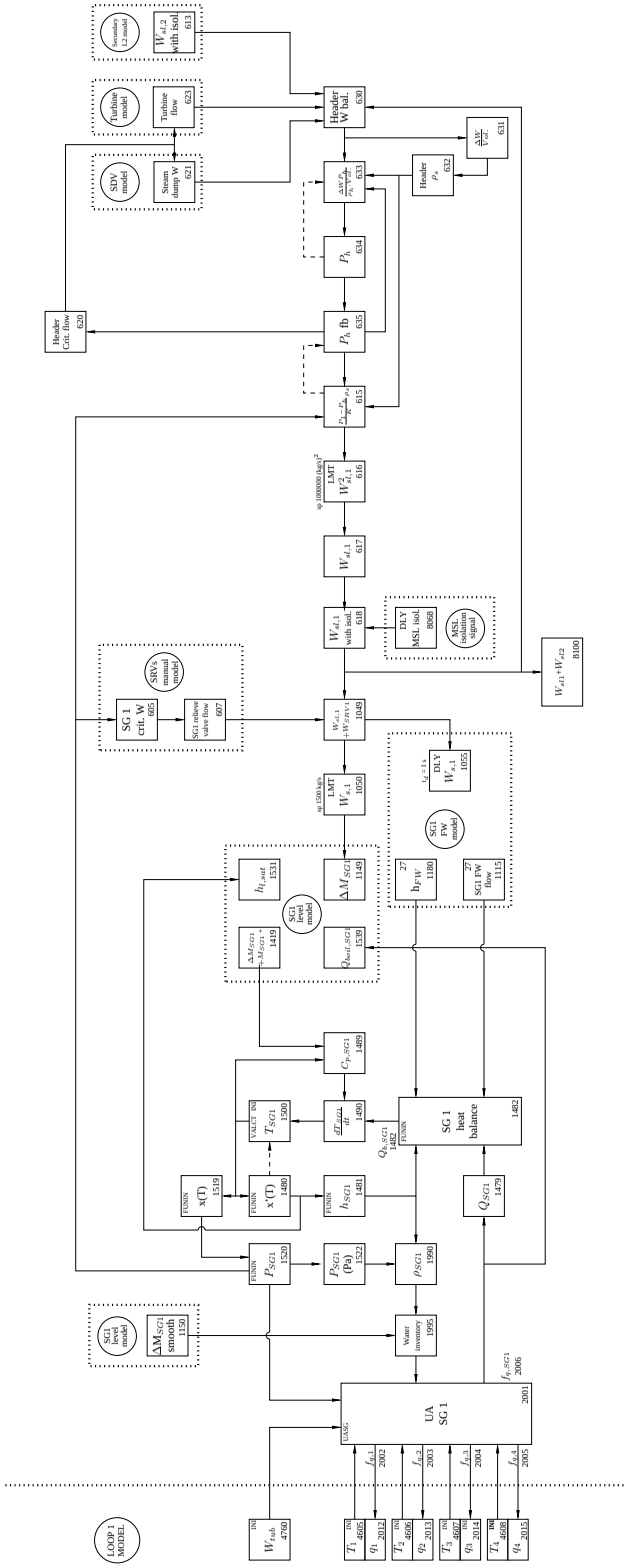


Figura 3.19: Modelo termohidráulico del secundario de los lazos sin presionador.

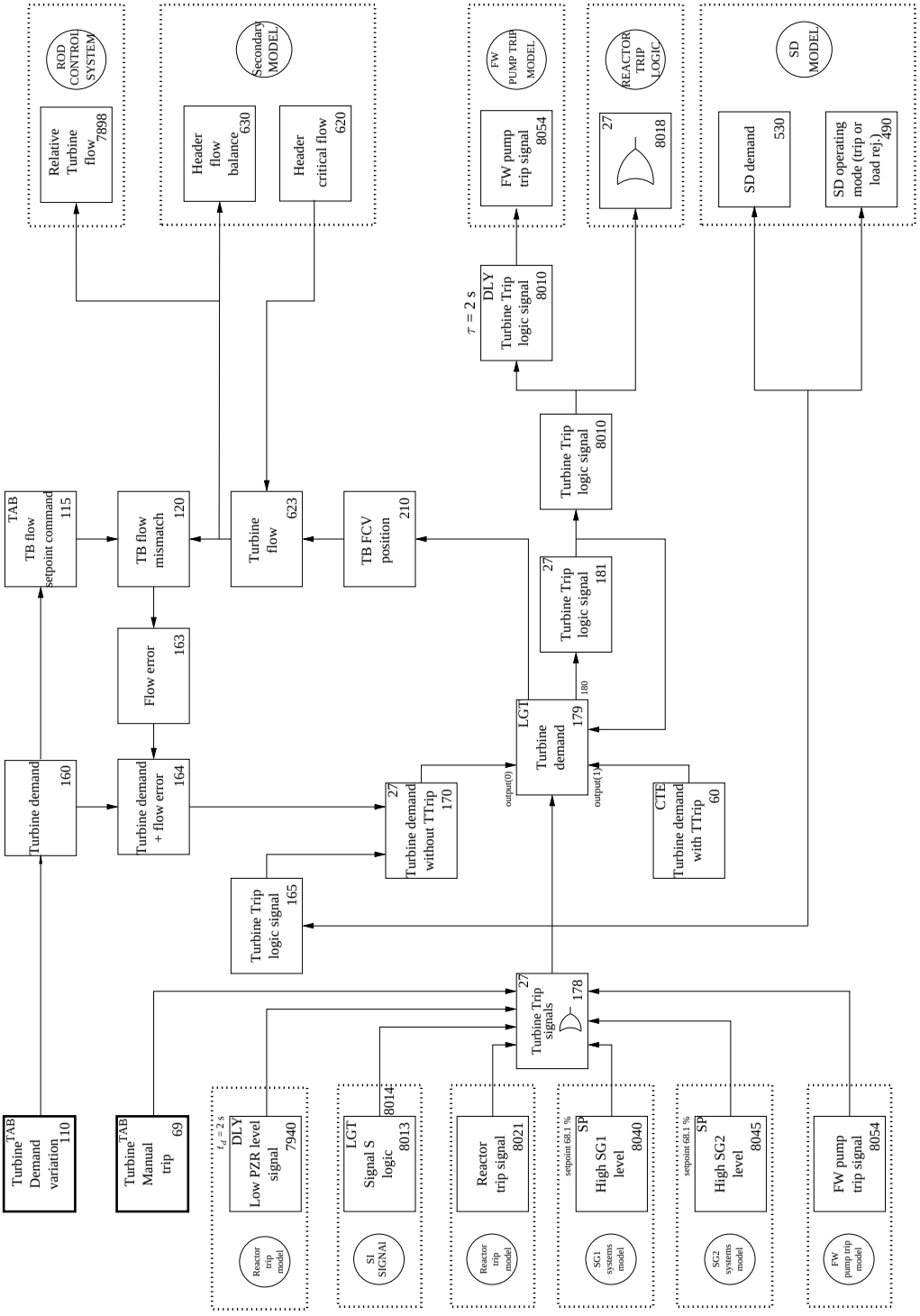


Figura 3.20: Modelo de turbina.

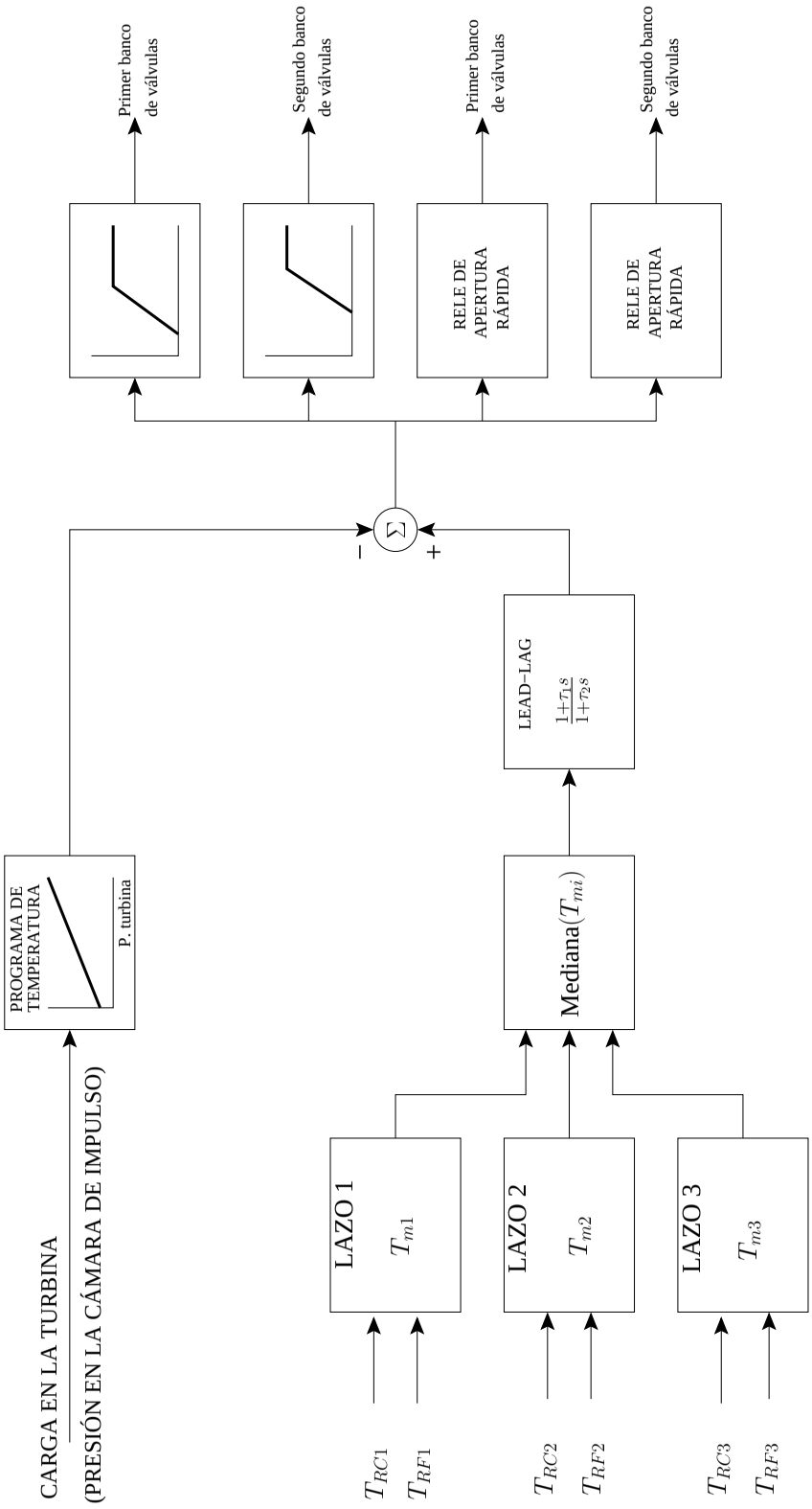


Figura 3.21: Esquema del alivio de vapor al condensador: modo temperatura en condiciones de rechazo de carga.

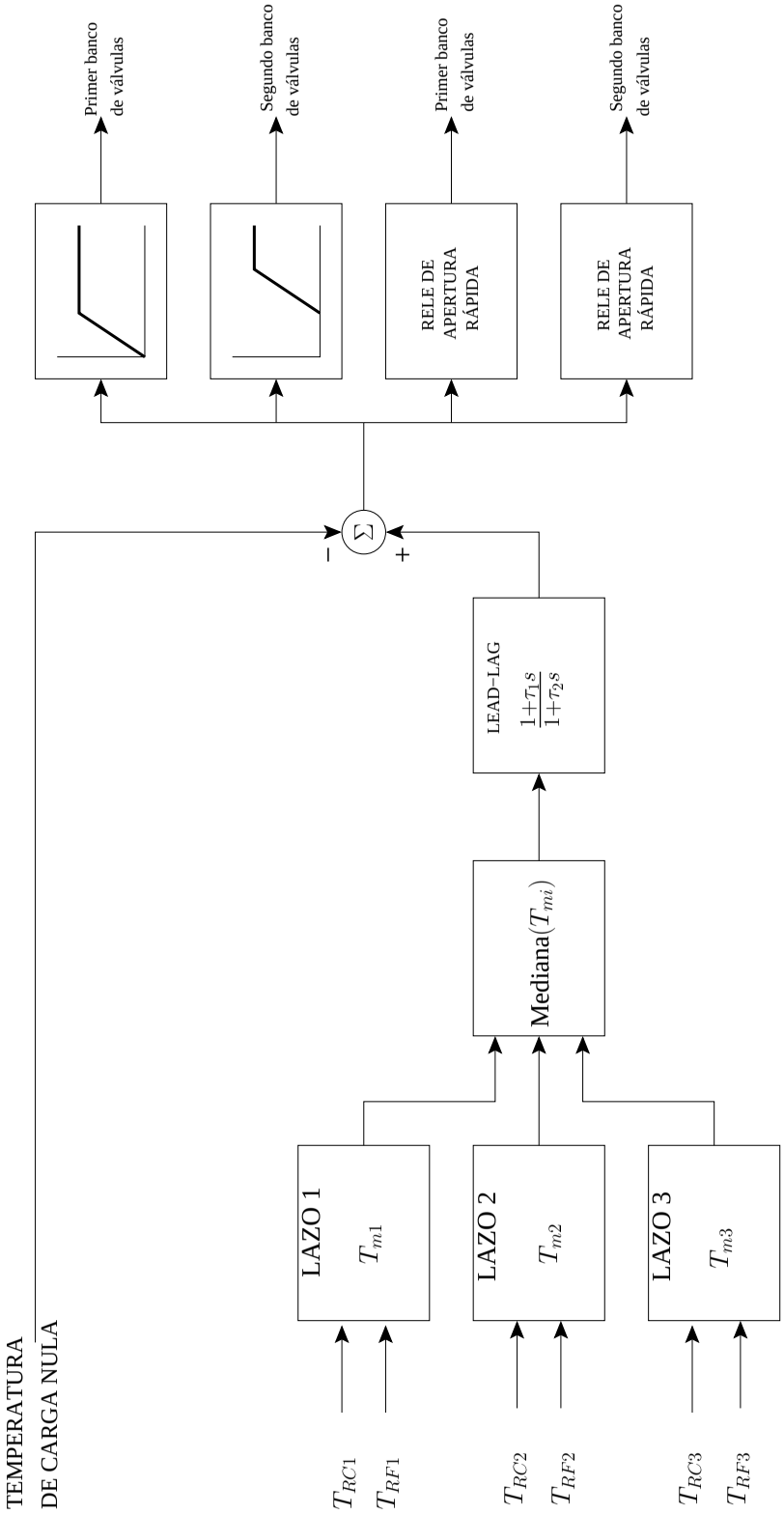


Figura 3.22: Esquema del alivio de vapor al condensador: modo temperatura en condiciones de disparo de turbina.

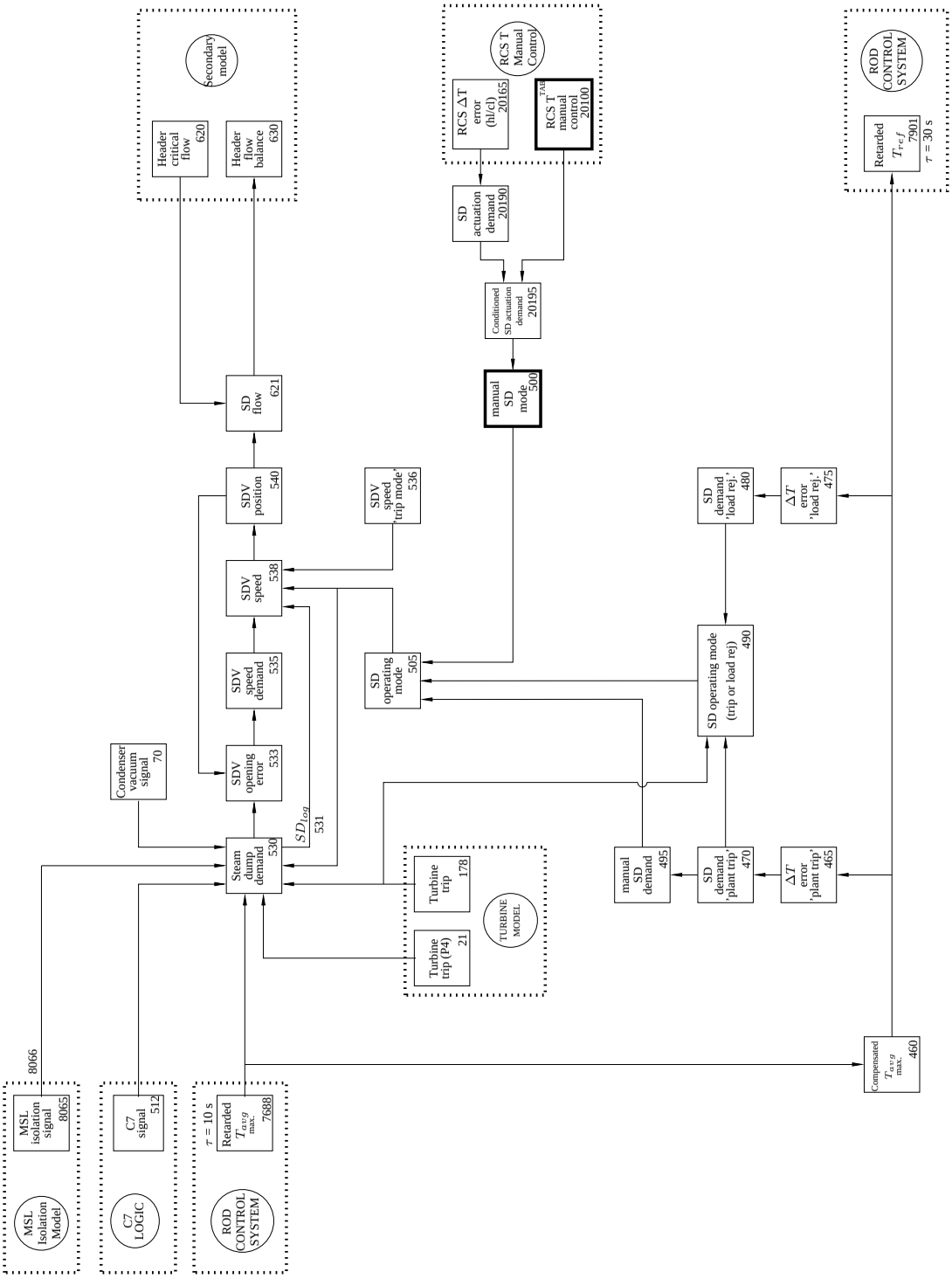


Figura 3.23: Modelo de alivio de vapor al condensador: modo temperatura en condiciones de disparo de turbina y rechazo de carga.

3.1.5 Modelo del FWS, del AFWS y de los controles relacionados

Dentro de este modelo se han incluido:

- El sistema de agua de alimentación normal.
- El sistema de agua de alimentación auxiliar.
- El modelo de cálculo del nivel de los generadores de vapor.
- El control de nivel de los generadores de vapor.

El modelado de cada sistema se comenta a continuación.

3.1.5.1 Modelo de los sistemas de agua de alimentación normal y auxiliar

El modelo de agua de alimentación normal (FWS) y auxiliar (AFWS) ha sido desarrollado tomando como referencia el modelo existente para la CN de Almaraz (CNA), Queral et al. (2002b). La implementación realizada del control de nivel del SG y del caudal de agua de alimentación normal y auxiliar se muestra en las Figuras 3.25 y 3.26. Los datos principales del modelo se resumen en la Tabla 3.1.

Para el FWS se han considerado los caudales y entalpías empleados en el modelo de la CNA, bloques 1100 y 1170 para el SG del lazo 1 y bloques 695 y 1170 para el correspondiente al lazo 2, Queral et al. (2002b). El caudal nominal del FWS se corresponde con una apertura del 59.9254 % que es el valor de referencia de planta. Sin embargo, para el modelo del AFWS se ha considerado un caudal de 24 kg/s, condición de caudal obtenida del FSAR de la CNA para el caso de pérdida de FW con inyección de las dos motobombas (86.4 m^3/h en condiciones de presión y temperatura del RWST, es decir, temperatura media de 25 ^oC y presión atmosférica), y una entalpía de 114.0 kJ/kg, obtenida para el agua líquida en las condiciones del RWST antes citadas, Queral et al. (2002b).

La actuación del AFWS se somete a un retraso de 26 s, siendo el tiempo correspondiente al arranque de las motobombas del sistema en transitorios sin pérdida de suministro eléctrico, Queral et al. (2002b).

	Entalpía [kJ/kg]	**Caudal** [kg/s]
NFW	de 593.43 a 962.997 según demanda en turbina	828.7387
AFW	constante a 114.0	24.0

Tabla 3.1: Parámetros del modelo de NFW y AFW.

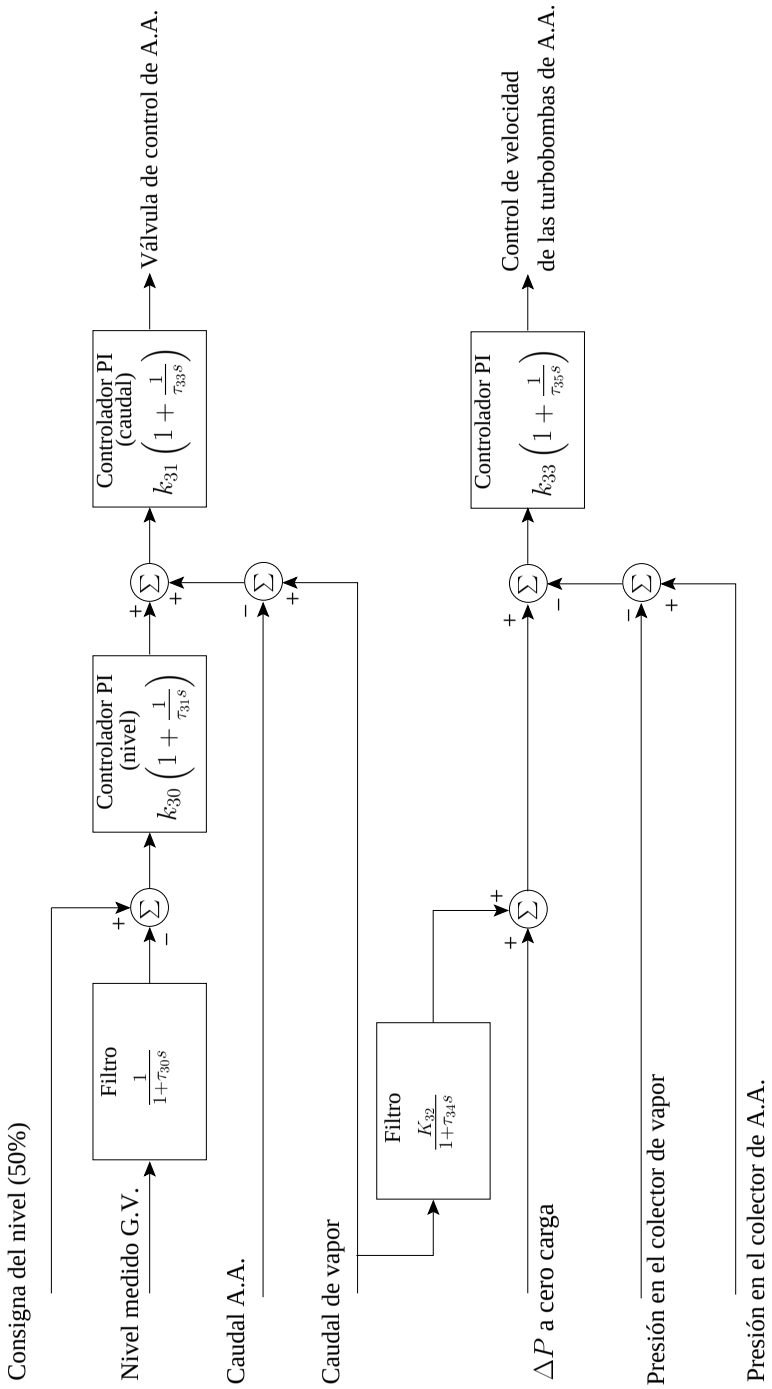


Figura 3.24: Esquema del control de nivel del generador de vapor.

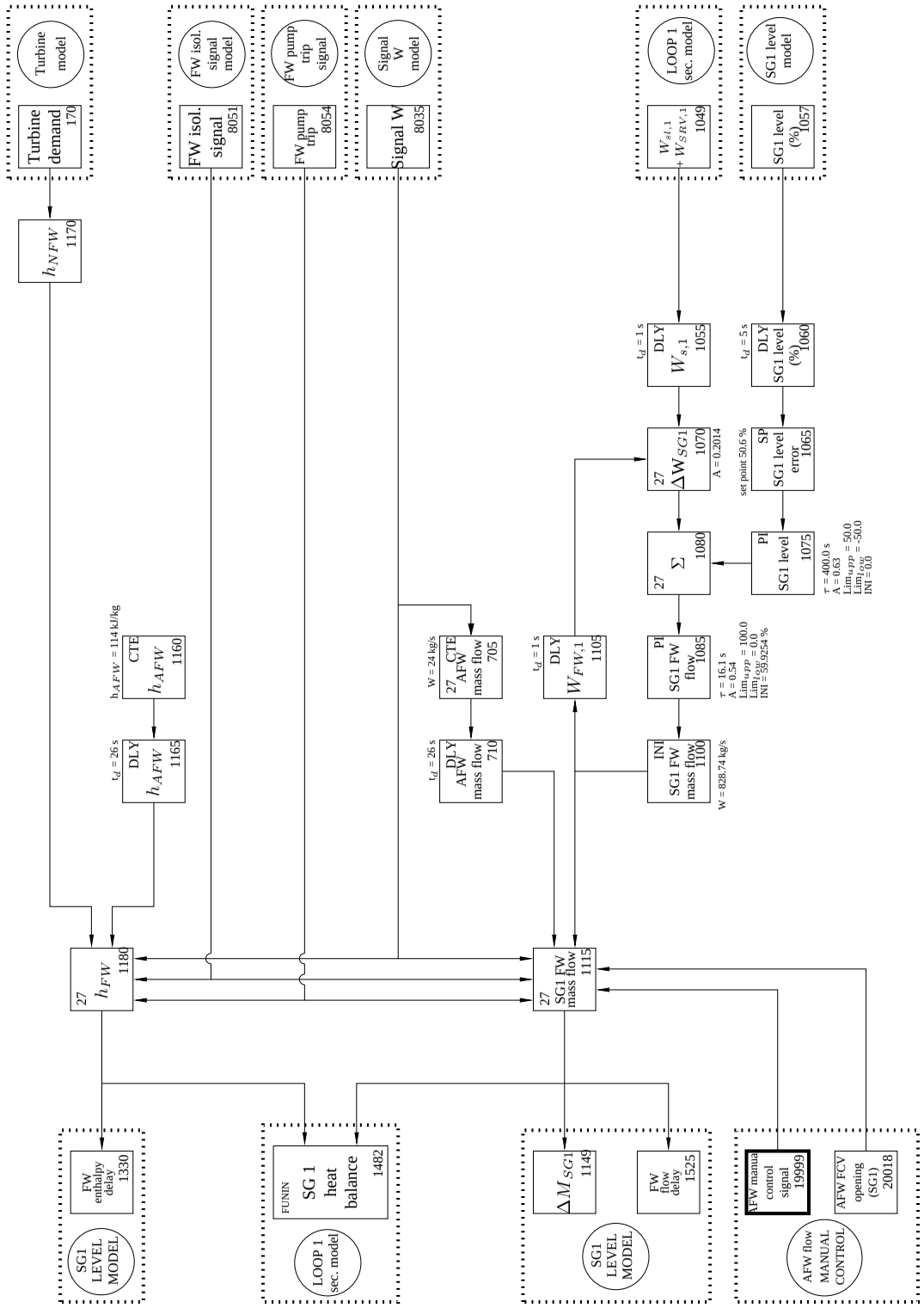


Figura 3.25: Modelo del FWS del generador de vapor de los lazos sin presionador.

3.1.5.2 Cálculo del nivel en los generadores de vapor

Para el cálculo de nivel se ha considerado como referencia el 17.6 % de señal de bajo nivel en SG equivalente a una masa de 7295.7 kg de inventario. Tomando como referencia este valor, el resto se obtienen mediante relación lineal kg - %.

El nivel se calcula en tres unidades de medida:

- Nivel del span (tpu), bloques 1545 y 1345.
- Nidel de rango estrecho porcentual, bloques 1057 y 663.
- Inventario másico del SG, bloques 1419 y 1219.

En el cálculo incorporado para el control de nivel del SG, se emplea el nivel porcentual. Resaltar que este nivel porcentual no considera el aumento de nivel por hinchamiento, siendo el nivel en tpu el que lo hace.

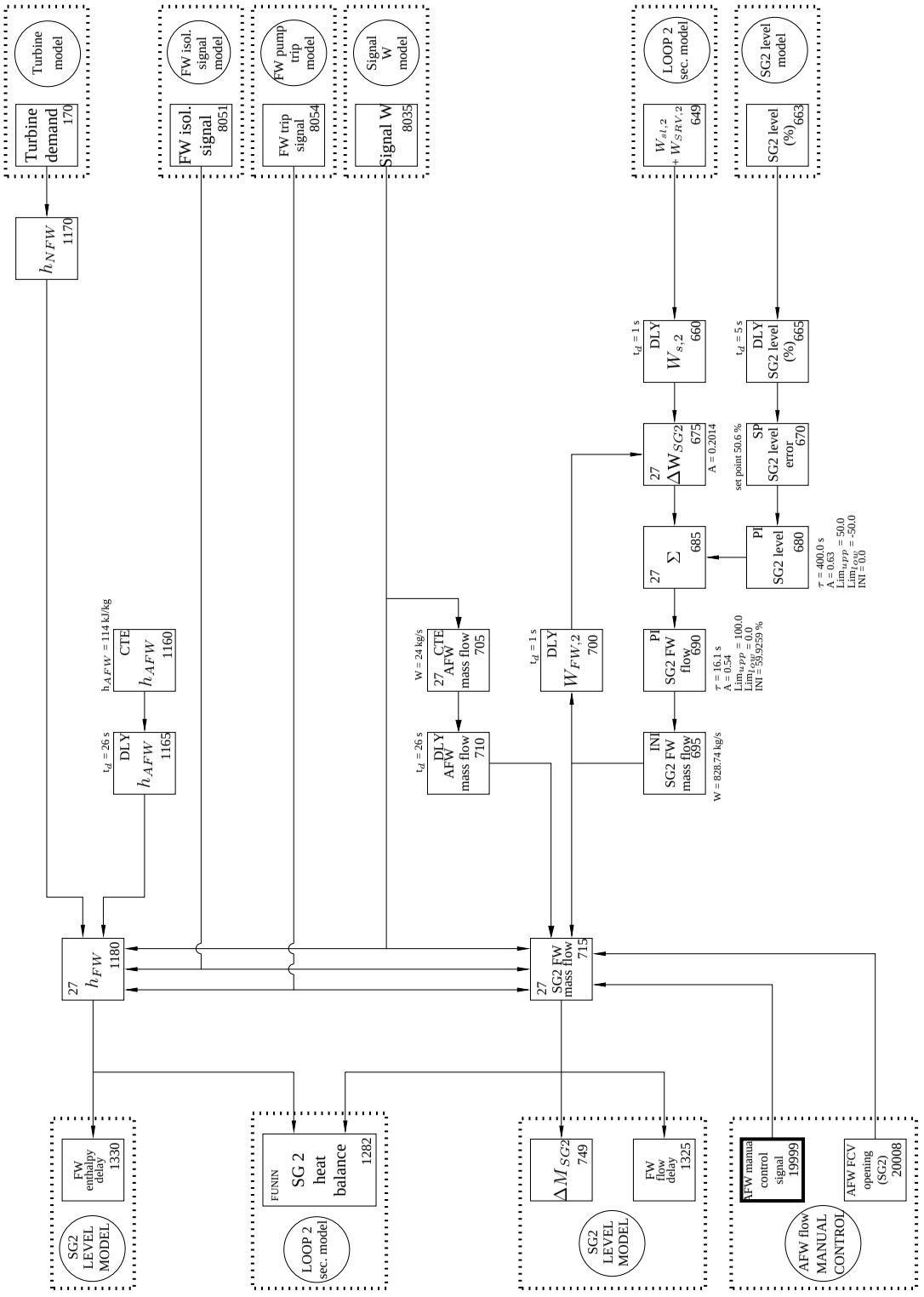


Figura 3.26: Modelo del FWS del generador de vapor del lazo con presionador.

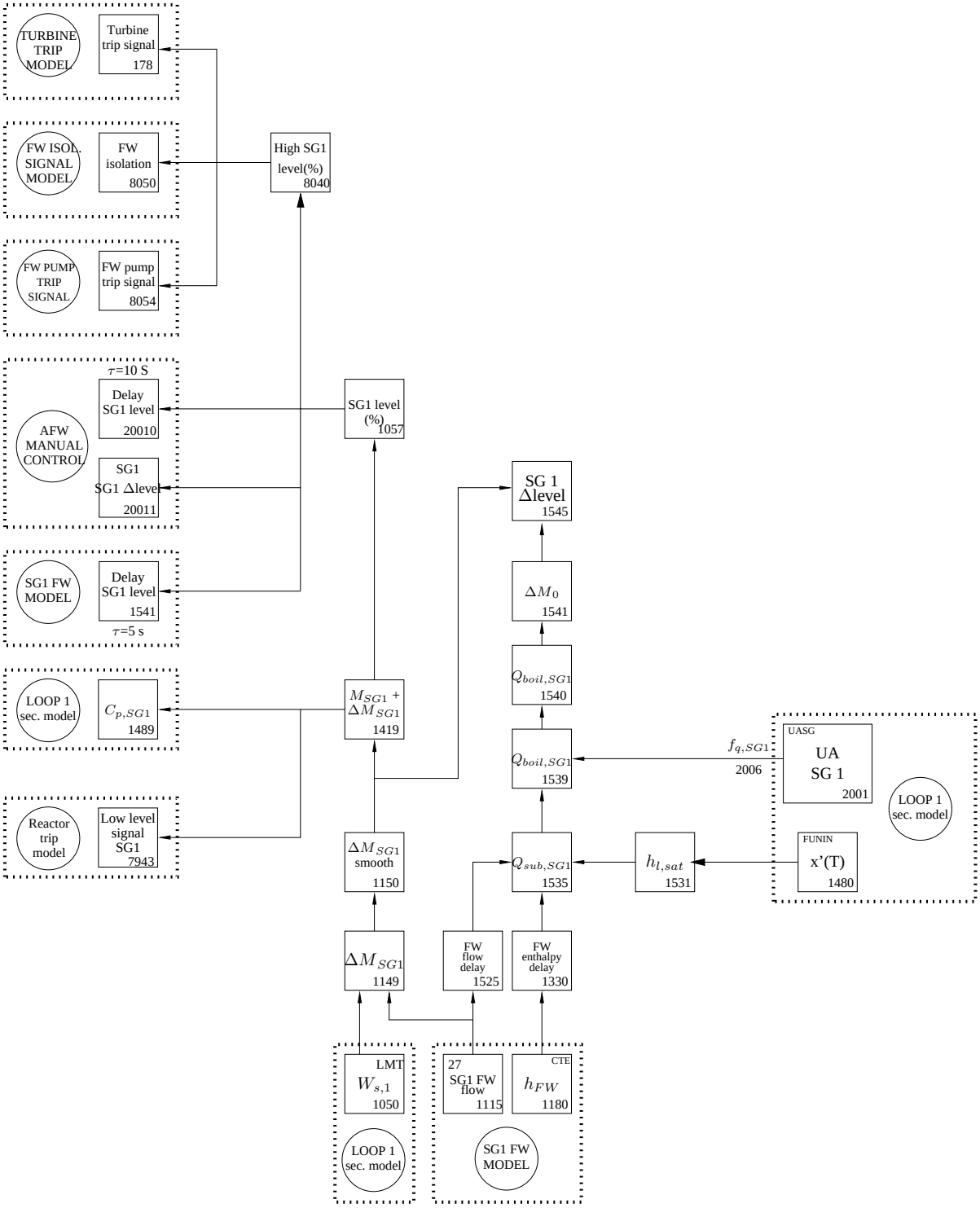


Figura 3.27: Esquema del cálculo del nivel del generador de vapor de los lazos sin presionador.

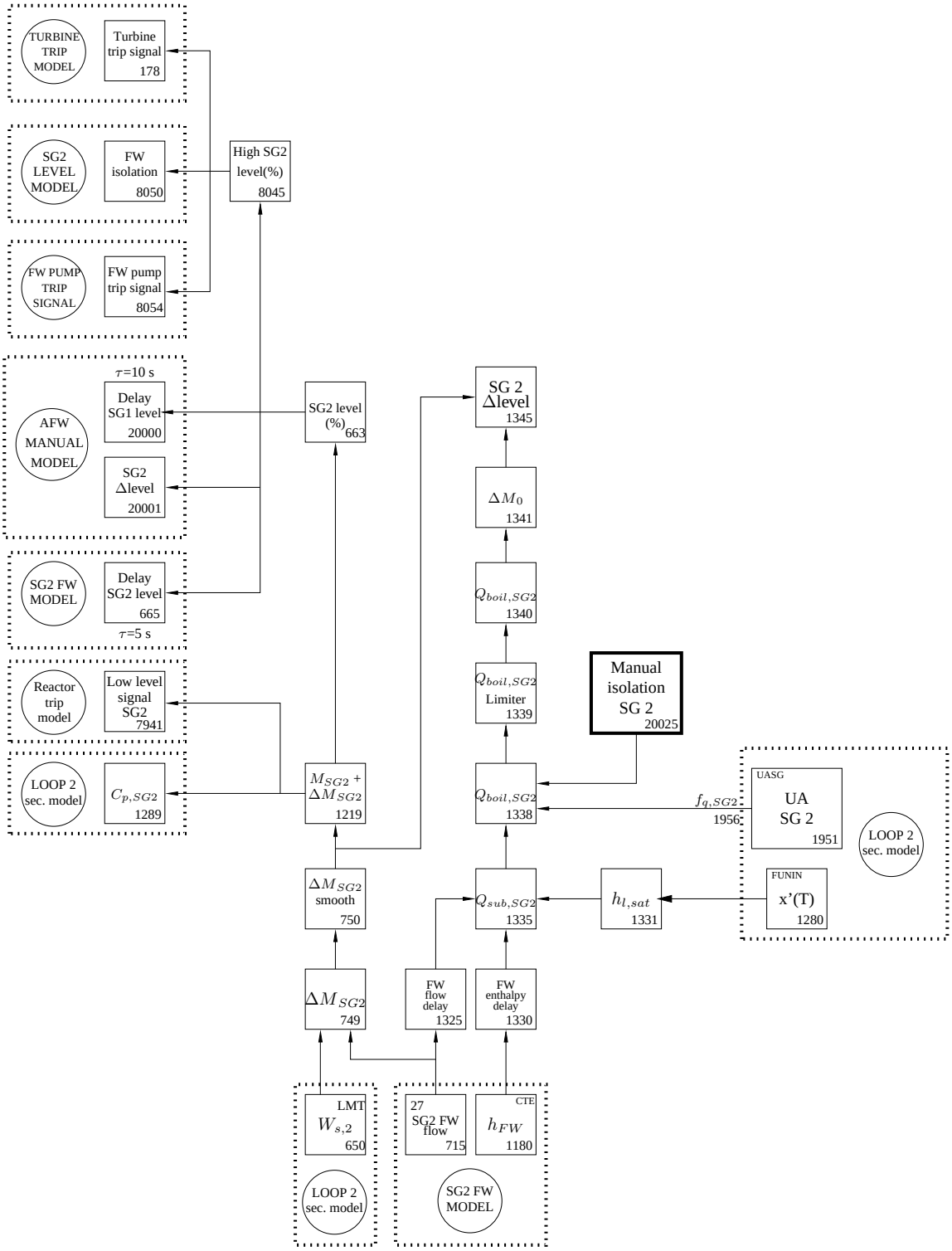


Figura 3.28: Esquema del cálculo del nivel del generador de vapor del lazo con presionador.

3.1.5.3 Control de nivel de los generadores de vapor

Para el modelo del control del sistema de agua de alimentación principal se decidió implementar un nuevo bloque proporcional-integral (PI) en TRETA, debido a que el existente no presenta el comportamiento esperado. Para corregir esta problemática se realizó la computerización de un nuevo algoritmo de cálculo para el PI en el módulo *funmix*, como la función de cálculo número 28, Figura 3.29. Se realizaron pruebas de validación del PI implementado en TRETA, incluyendo los casos de control limitado y no limitado, para verificar la saturación. La señal de entrada empleada fue la misma que para el caso del PID existente previamente en el código TRETA, lo que permitió comprobar las diferencias entre ambas implementaciones del PID. Basándose en la nueva implementación, se modeló el control del caudal del FWS, Figuras 3.25 y 3.26, resumiéndose en la Tabla 3.2 los valores de inicialización considerados, extraídos del modelo de la CNA, Queral et al. (2002b). Para verificar el modelo, se realizó un conjunto de pruebas contra resultados de simulaciones obtenidas mediante RELAP que dieron resultados satisfactorios.

	Nivel (bloques)	**Caudal** (bloques)
Valores SP/nominales	50.6 % (670 y 1065)	828.74 kg/s (695 y 1100)
Retrasos medidas	t_d = 5 s (665 y 1060)	t_d = 1 s (660 y 1055)
A diferencias	—	A = 0.2014 (675 y 1070)
PI	A = 0.63 (680 y 1075) τ = 400.0 s Lim_{upp} = 50.0 Lim_{low} = -50.0 INI = 59.9259 %	A = 0.54 (690 y 1085) τ = 16.1 s Lim_{upp} = 100.0 Lim_{low} = 0.0 INI = 0.0

Tabla 3.2: Parámetros del mode de control de agua de alimentación principal.

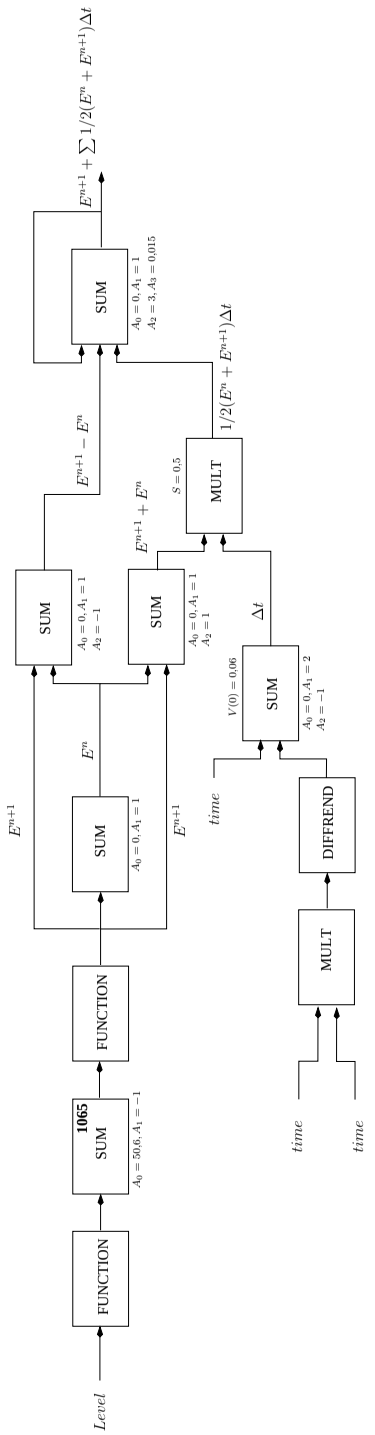


Figura 3.29: Diagrama del algoritmo PID implementado en TRETA.

3.1.6 Modelo del sistema de inyección de seguridad

El sistema inyecta por las tres ramas frías al volumen de mezclado de la bajante y del plenum inferior, bloque 2291. En el caudal de inyección se ha incluido un retardo de 3 segundos, retraso ligado con los tiempos de actuación del sistema, bloques 2286 y 2290. La distribución del caudal a los lazos se considera homogénea.

Los datos empleados para el modelo del SIS se han extraído del modelo de CNA de TRACE, Queral et al. (2002b), obteniéndose el caudal de inyección del SIS en función de la presión del RCS. El resultado final son los valores caudal-presión relacionados en el bloque 2280, Figura 3.30. Las condiciones del fluido que se han considerado son de 21.1 ^{o}C y presión atmosférica, siendo la entalpía correspondiente de 88.55156 kJ/kg, bloque 2289.

El caudal nominal de inyección se ha considerado el equivalente a las dos bombas de carga del sistema, aunque en la práctica es ligeramente inferior. Esta aproximación es una estimación conservadora del caudal que aporta el sistema.

La señal de actuación de inyección de seguridad se comenta en la Sección 3.1.8.

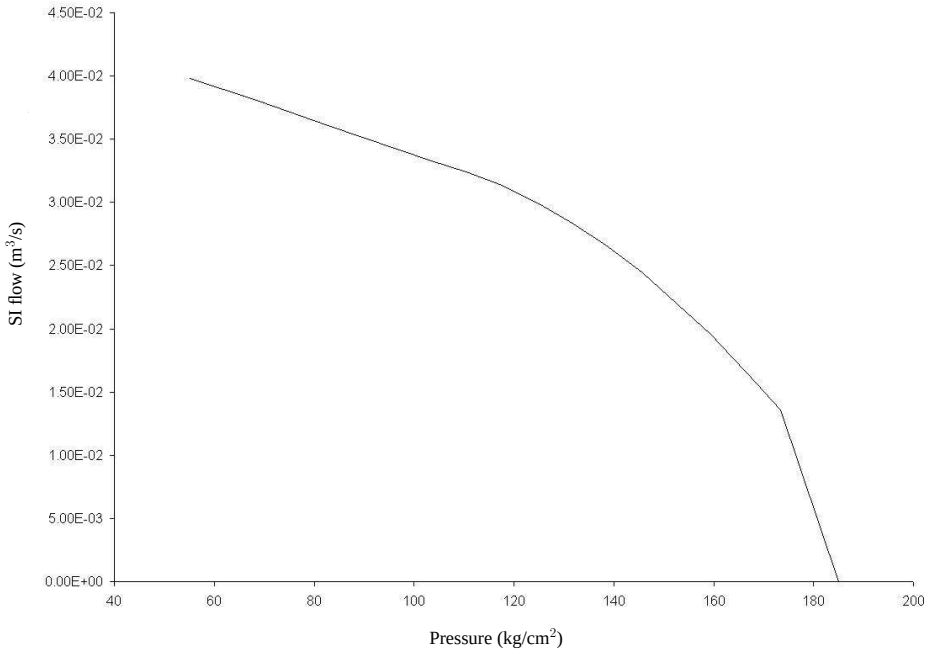


Figura 3.30: Dependencia del caudal del SIS en función de la presión del RCS.

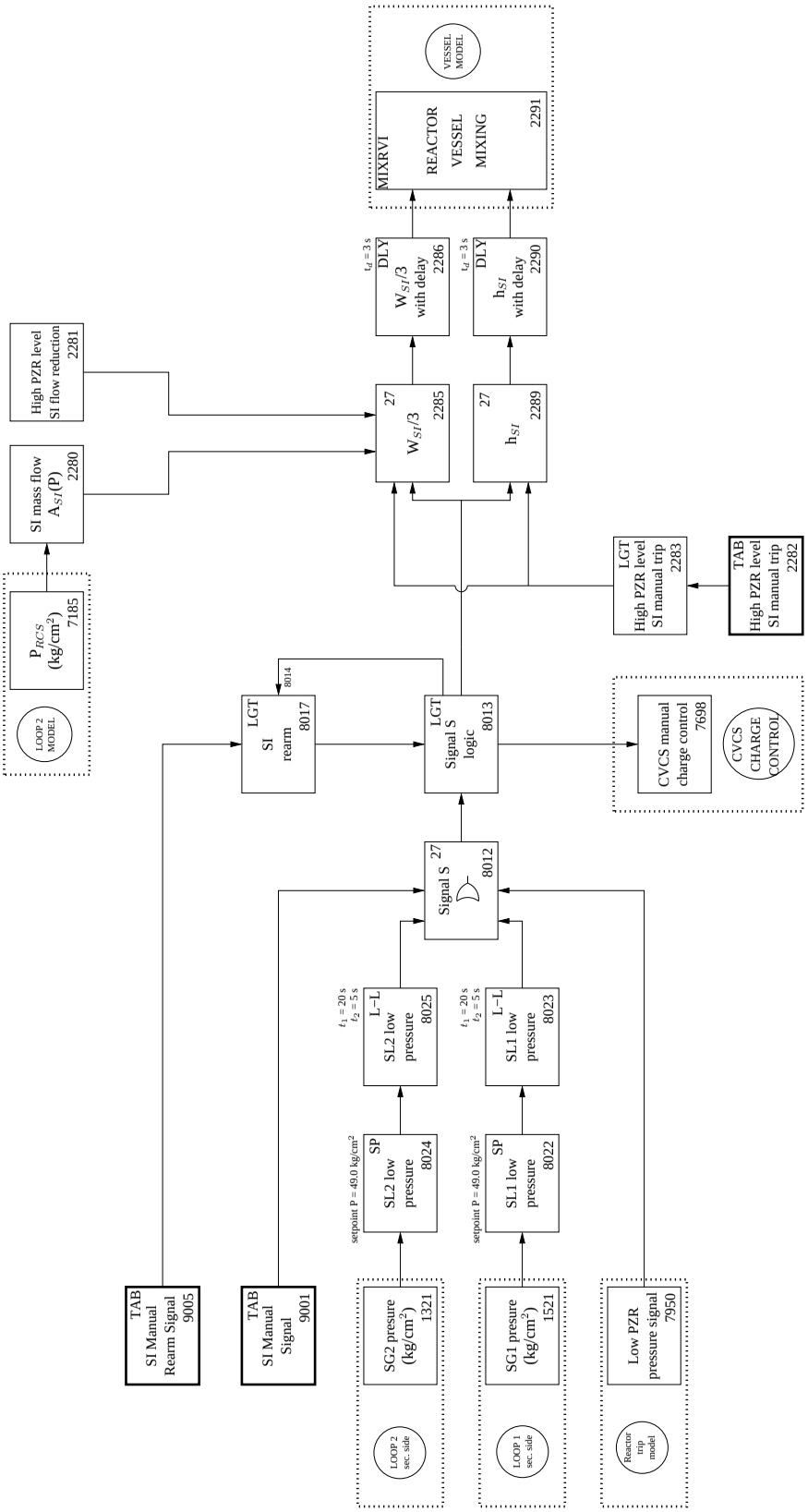


Figura 3.31: Modelo del sistema de inyección de seguridad.

3.1.7 Sistema de aislamiento de las SL y modelo de roturas en el secundario

El sistema de aislamiento de las líneas de vapor, Figura 3.32, actúa por la señal de aislamiento de las líneas de vapor, bloque 8065. En la actuación del sistema se ha incluido una retraso de cuatro segundos, relacionado con el tiempo característico de cierre de las MSIV.

El modelo de rotura permite simular roturas en una línea de vapor, rotura asimétrica, o en el colector de vapor, rotura simétrica, bloque 50. Además, se considera la posibilidad de que la rotura sea aislable en el caso de roturas localizadas en la línea de vapor, bloque 45. El caudal de salida se calcula considerando condiciones de flujo crítico, empleando el modelo homogéneo, bloque 56. Según la localización de la rotura, se determina la presión a considerar en el cálculo de las condiciones de flujo crítico, bloque 51. El área máxima estipulada para la rotura es la correspondiente a tres veces la del anillo restrictor de un SG, con un valor de 0.13 m^2, siendo por consiguiente de 0.39 m^2.

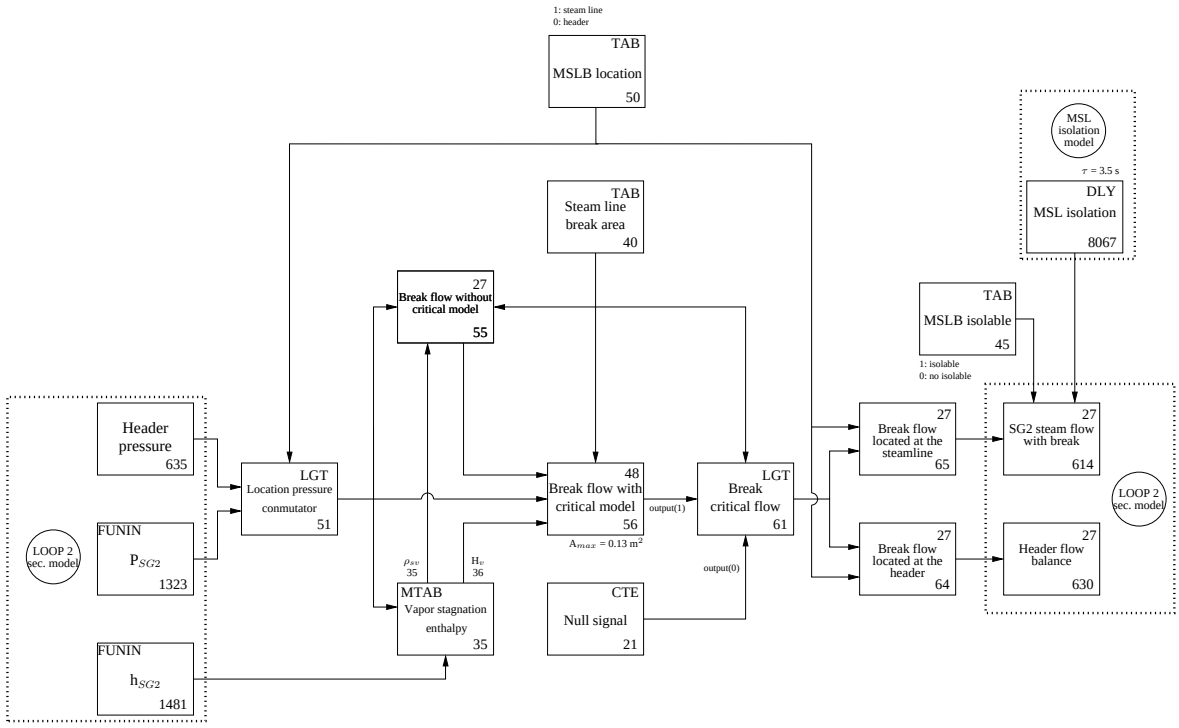


Figura 3.32: Modelos del sistema de aislamiento de las SL y de las roturas en el secundario.

3.1.8 Modelo del sistema de protección del reactor y de salvaguardias tecnológicas

Este modelo consta de:

- Señal de disparo del reactor y los *scram* asociados.
- Señal de disparo de la turbina.
- Señal de actuación del SIS.
- Señal de actuación del AFWS.
- Señal de aislamiento de las líneas de vapor.
- Señal de aislamiento del agua del FWS.
- Señal de disparo de las bombas de FWS.

La implementación de las señales se puede consultar en las Figuras 3.33 a 3.40. En la Tabla 3.3 se resumen los bloques de demanda manual de sistemas y señales de protección y salvaguardias.

Cabe resaltar que el estado actual del modelo del sistema de salvaguardias no es completo, debiéndose considerar:

- La posibilidad de realizar el modelado de las coincidencias en las señales.
- Corregir la secuencia de cálculo de la lógica, de forma que se consideren la dependencia de las señales.

Ambos puntos no son de especial relevancia para los objetivos de simulación de este trabajo y su implementación ha sido pospuesta para considerarla en desarrollos posteriores.

Señal	**Bloque**
Disparo del reactor	310
Disparo de turbina	69
Inyección de seguridad	9001
Aislamiento del FWS	9010
Aislamiento de las SL	9020
Actuación del AFWS	9030

Tabla 3.3: Bloques de demanda manual de sistemas y señales de protección y salvaguardias.

Señal automática	**Bloque**
Disparo de la turbina	178
Señal C7	512
Bajo caudal en el lazo 2	7923
Bajo caudal en el lazo 1	7926
Alto flujo neutrónico	7933
Alta presión en el presionador	7936
Alto nivel en el presionador	7938
Baja presión en el presionador	7940
Bajo nivel en el SG 2	7942
Bajo nivel en el SG 1	7944
Muy baja presión en el presionador	7950
OTΔT y OPΔT del lazo 2	7968
OTΔT y OPΔT del lazo 1	7988
Alta variación del flujo neutrónico	7992
Inyección de seguridad (señal S)	8013/8014
Disparo automático del reactor	8021
Demanda de agua de alimentación auxiliar (señal W)	8035
Alto nivel en el SG 1	8040
Alto nivel en el SG 2	8045
Aislamiento del agua de alimentación normal	8051
Disparo de las bombas de agua de alimentación normal	8054
Aislamiento de las líneas de vapor	8065/8068

Tabla 3.4: Señales automáticas implementadas en el modelo de planta PWR-W.

Actuación	Señal	Punto de tarado[1].
Disparo del reactor	Alto flujo neutrónico en el RF (1/2)	$10^5 cuentas/s$
	Alto flujo neutrónico en el RI (1/2)	25 % Potencia nom.
	Alto flujo neutrónico en el RP (2/4)	$\geq 25\,\%$ Potencia nom.
		$\geq 109\,\%$ Potencia nom.
	Alta variación flujo neutrónico (2/4)	$\pm 5\,\%$ en 2 s.
	Baja presión en el PZR	$138{,}0\,kp/cm^2 + P7$
	Alta presión en el PZR	$169\,kp/cm^2$
	Alto nivel en el PZR	92 %
	Bajo nivel en un SG	$\leq 17{,}6\,\%$(5.6 % SAR)
	$OP\Delta T$ Lazo 1/3 (2/3)	
	$OT\Delta T$ Lazo 2 (2/3)	
	SI	
	Disparo de turbina	
	Bajo caudal en el primario (1/3)	90 % + P8
	Bajo caudal en el primario (2/3)	90 % + P7
	Actuación manual del operador	
Disparo de turbina	Señal de disparo del reactor	
	Disparo TDP del FWS	
	Alto nivel en un SG	$\geq 68{,}1\,\%$
	Muy baja presión en el PZR	$130\,kp/cm^2$
	Actuación manual del operador	
	SI. Señal S	

Tabla 3.5: Señales de actuación del sistema de protección del reactor y del disparo de turbina.

Actuación	Señal	Punto de tarado[2].
SI	Muy baja presión en el PZR	$131,12\,kp/cm^2$
	Baja presión en una línea de vapor	$48{,}1\,kp/cm^2$
	Alta presión en el recinto de contención	$1{,}45\,kp/cm^2$
	Actuación manual del operador	
	Rearmado manual	
Aislamiento de las MSL	Baja presión en una línea de vapor	$48{,}1\,kp/cm^2$
	Alta tasa de despresurización de línea de vapor. *Sólo activo por debajo de P-11* (1/3)	-7.030 bar/s
	Alta presión en el recinto de contención	$1{,}45\,kp/cm^2$
	Actuación manual del operador	
Iniciación del AFWS	Disparo turbobombas FW (2 MDP)	
	Muy bajo nivel en un SG (2 MDP + TDP)	$\leq 17{,}6\,\%$ (5.6 % SAR) (1/3)
	SI. Señal S (2 MDP)	
	Actuación manual del operador	
Aislamiento FW	Alto nivel en un SG (P14)	$\geq 68{,}1\,\%$
	Baja temperatura media del primario + P4 (Señal S1)	289 °C
	Actuación manual del operador	
	Muy baja presión en el PZR	$131,12\,kp/cm^2$
	SI. Señal S	
Disparo de las turbobombas del FW	Señal de aislamiento de las MSL	
	Alto nivel en un SG	68,1 %
	Muy baja presión en el PZR	$131,12\,kp/cm^2$
	Disparo de la turbina	
Aislamiento de la carga del CVCS	Actuación manual	
	Inyección de seguridad, Señal S	
	Muy baja presión en el PZR	$131,12\,kp/cm^2$
Aislamiento de la descarga del CVCS	Actuación manual	
	Bajo nivel en el PZR	15 %
	Inyección de seguridad, Señal S	
Apertura de las SRV	Actuación manual	
	Alta presión en un SG	$85,76\,kp/cm^2$

Tabla 3.6: Señales de actuación de las salvaguardias tecnológicas y otros sistemas o componentes.

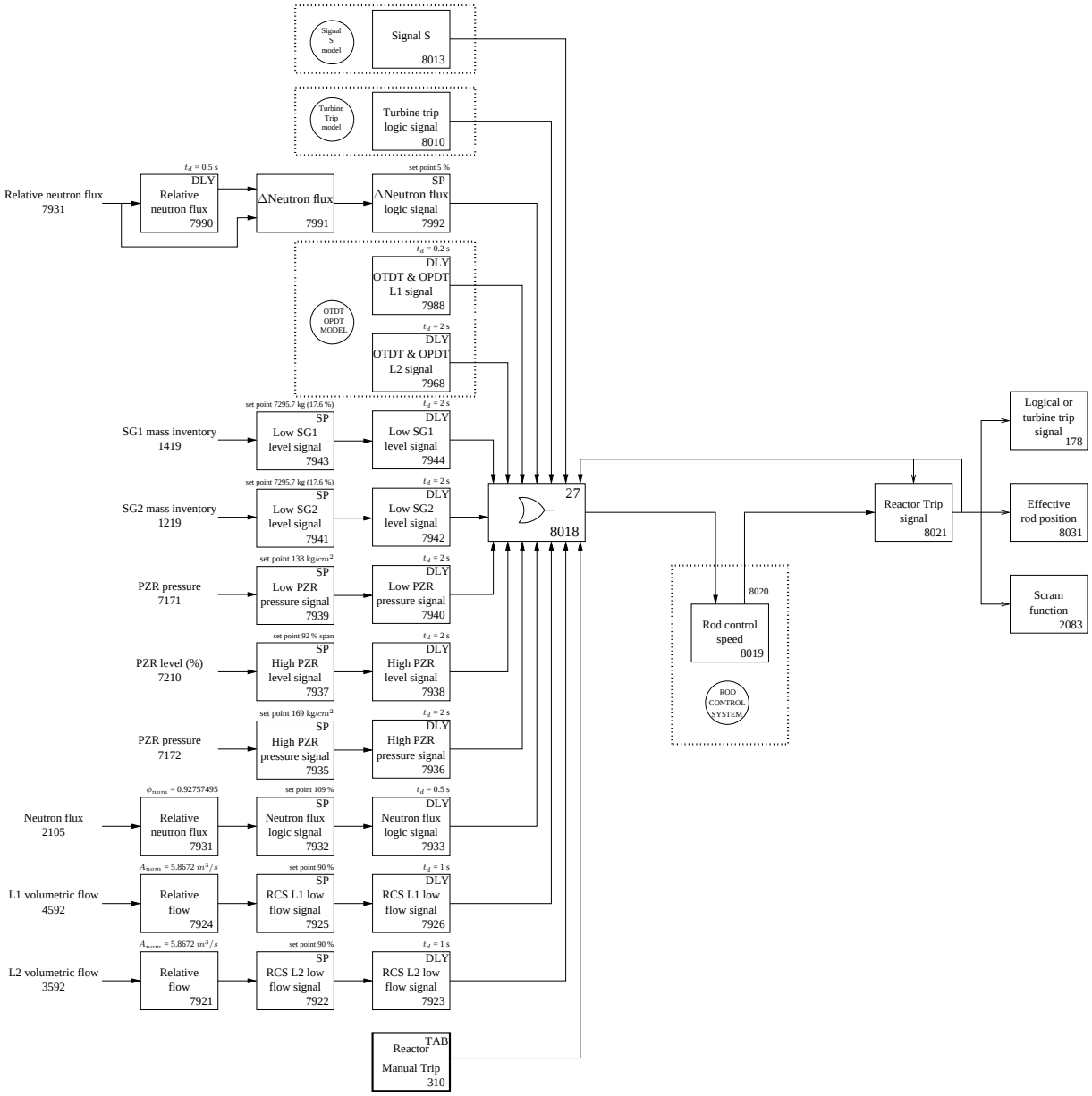


Figura 3.33: Señales de disparo del reactor.

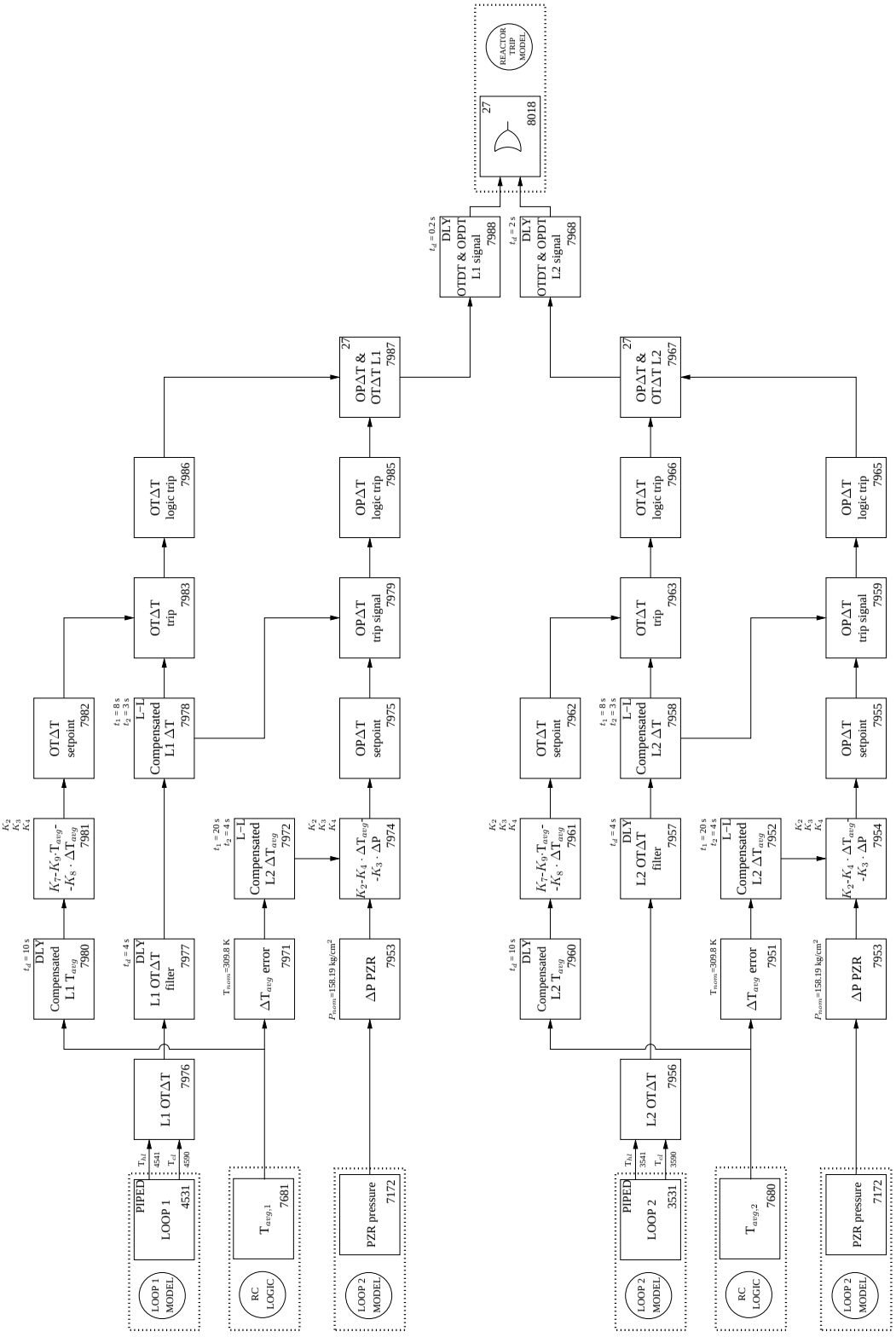


Figura 3.34: Señales OPΔT y OTΔT.

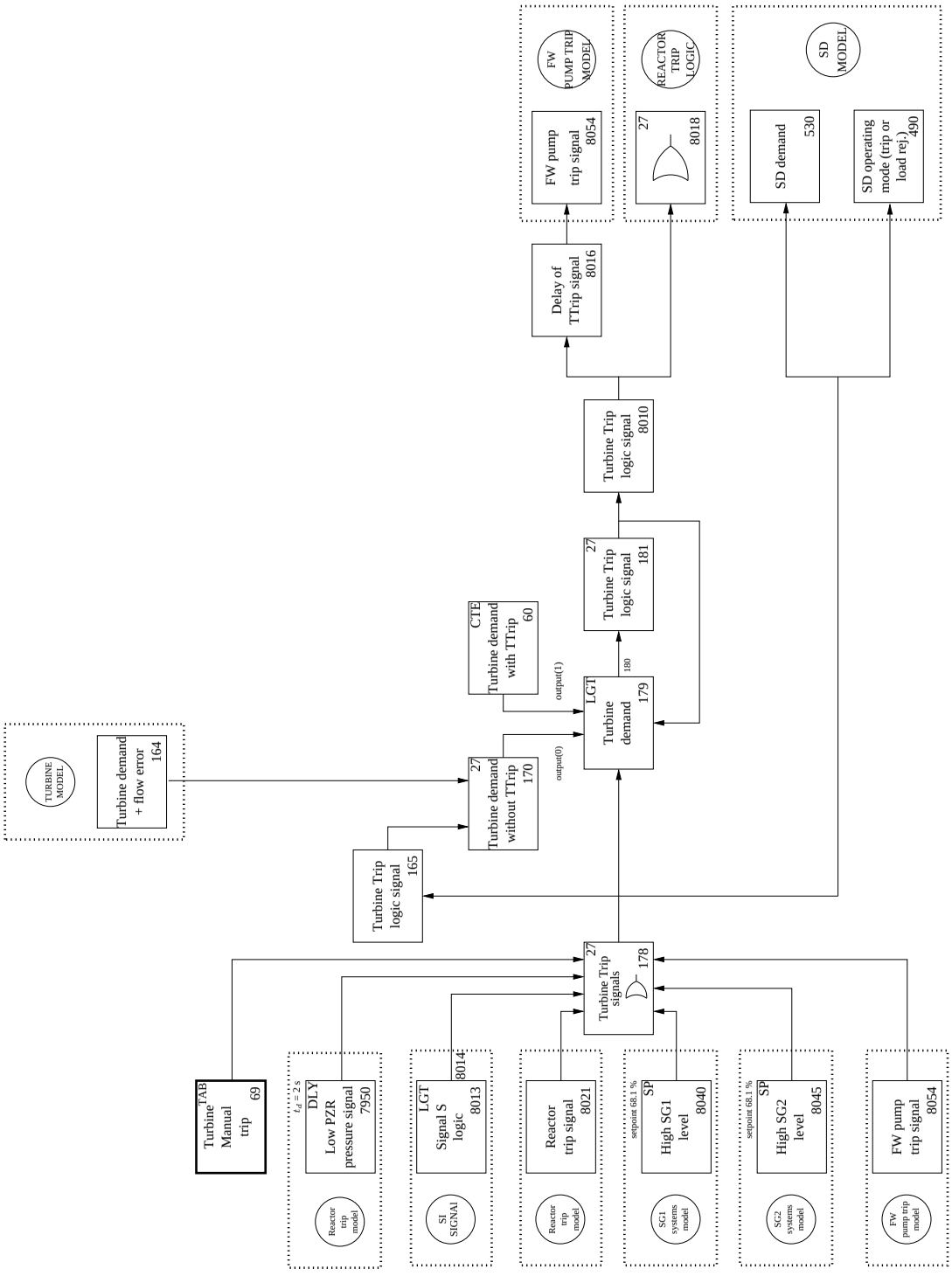


Figura 3.35: Señal de disparo de turbina.

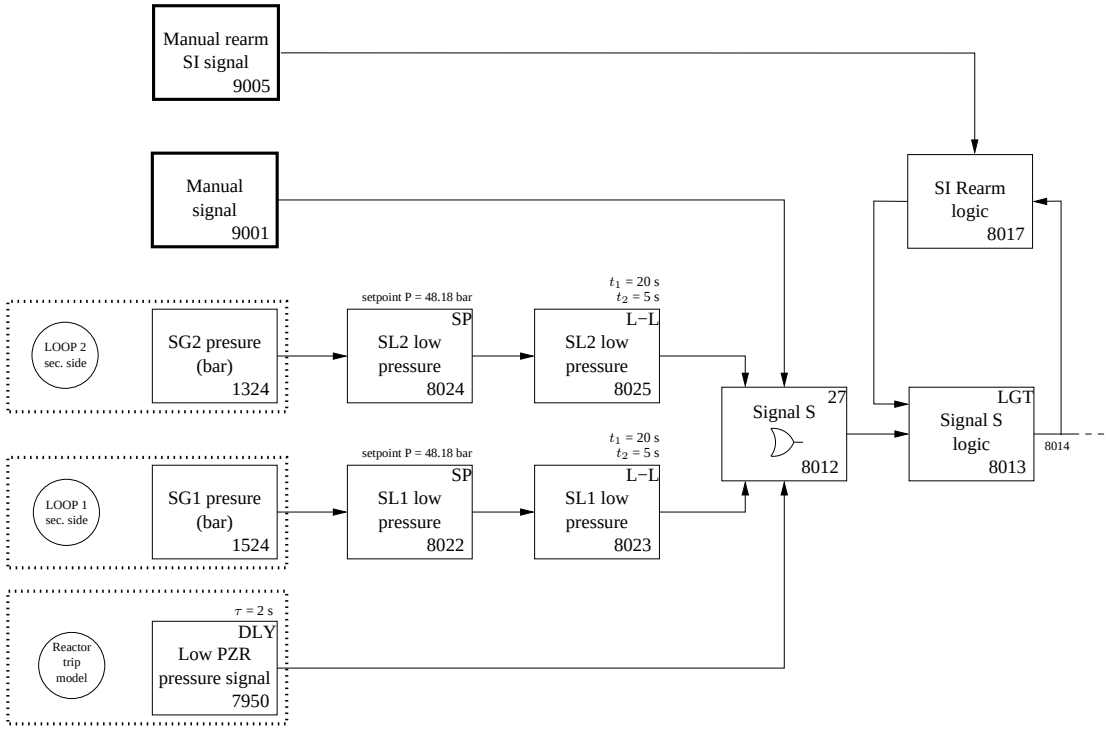


Figura 3.36: Señal S.

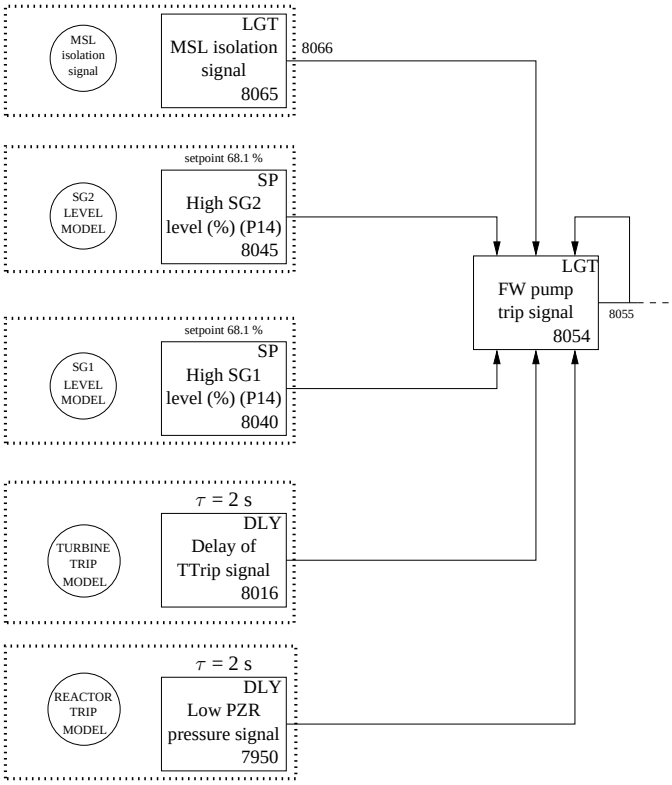


Figura 3.37: Señal de disparo de las bombas de agua de alimentación.

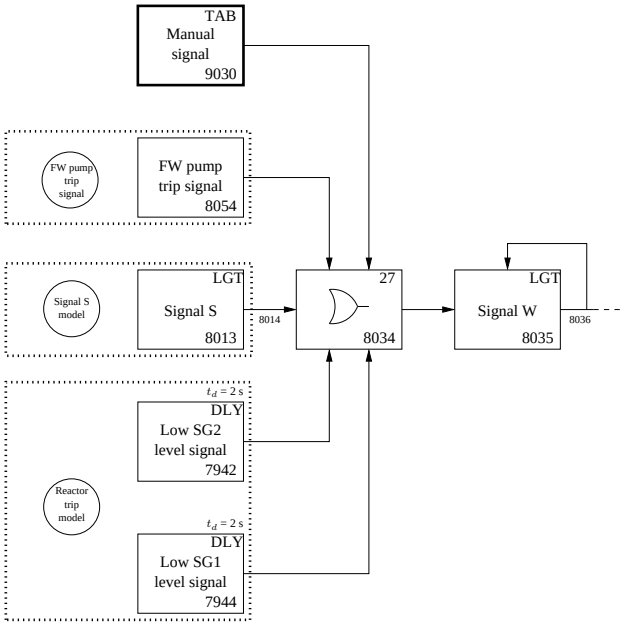


Figura 3.38: Señal W.

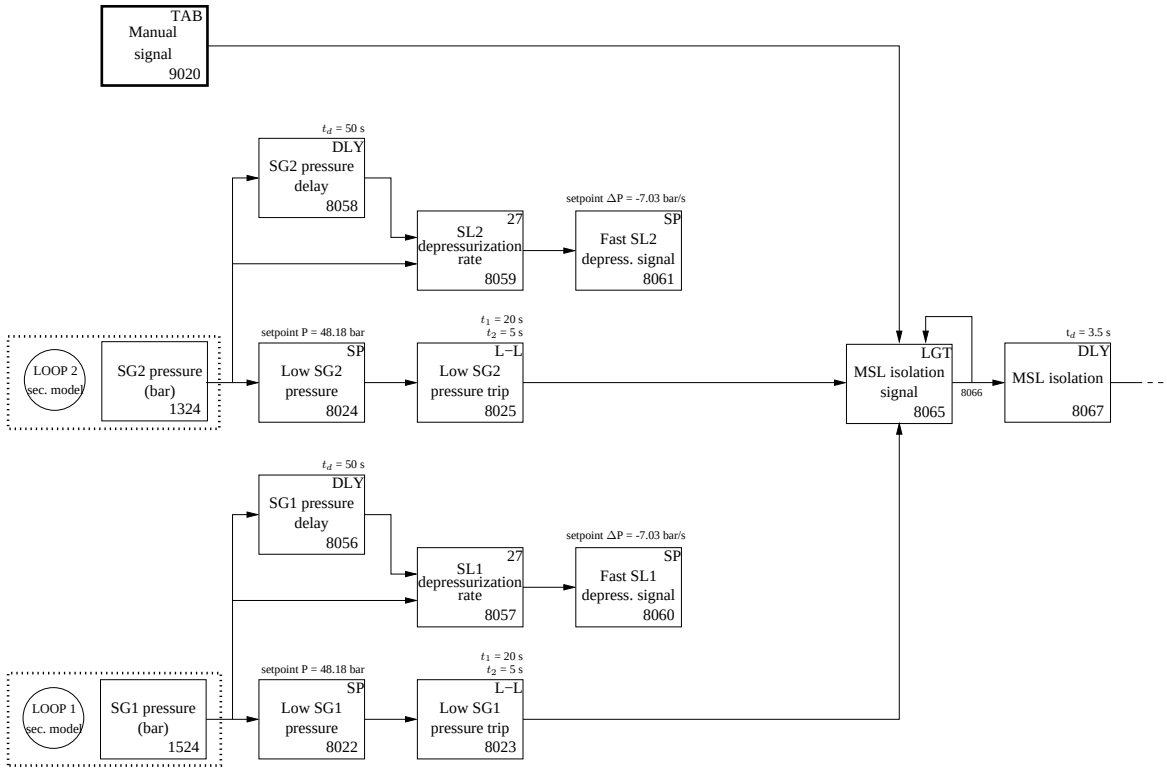


Figura 3.39: Señal de aislamiento de las líneas de vapor.

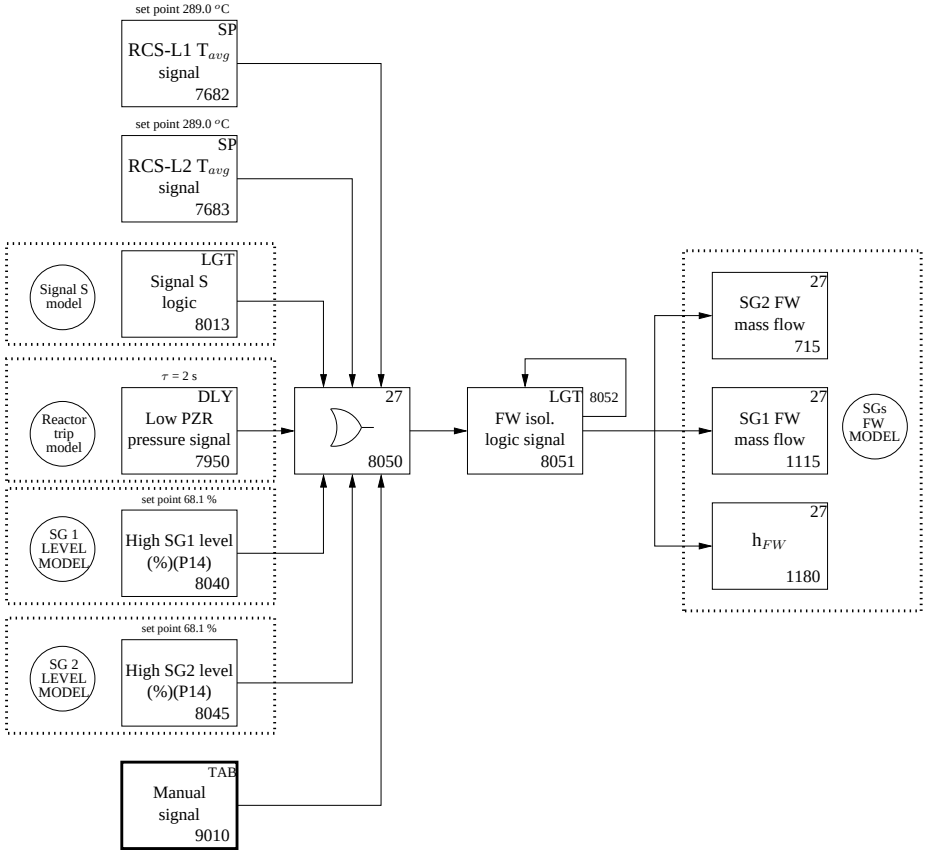


Figura 3.40: Señal de aislamiento del NFWS.

3.2 Estructura de cálculo del modelo genérico de un PWR-W de tres lazos

Para poder realizar un estudio sobre las realimentaciones del modelo desarrollado, Tabla 3.7 y Figura 3.41, se procedió a su comparación con el modelo previo suministrado por el CSN, que fue realizado en la UPM, Figura 3.42, Poveda (1999) y Lacuna (1999).

Las conclusiones obtenidas fueron que el modelo desarrollado, a parte de presentar modelos adicionales y mejoras en algunos de los existentes, posee mejores capacidades de simulación al abarcar rangos de operación en secuencias accidentales más amplios. En lo que respecta a las realimentaciones, se introdujeron modificaciones que le proporcionan mayor estabilidad, garantizando la convergencia en fases de cálculo que anteriormente no convergían.

El listado completo de los bloques del modelo desarrollado se encuentra en Expósito y Queral (2006b).

Módulo	Realimentación	Descripción
540	533	Position of the Steam dump valve
632	610	Steam density in the header
634	633	Header pressure
635	610	Header pressure for feedback
1300	1280	SG 1 Temperature
1320	610	SG 1 Pressure
1500	1480	SG 2 Temperature
1520	615	SG 2 Pressure
1521	610	SG 2 Pressure
2057	1279	Qsg2
2270	2088	Core heat power
3715	3661	Angular speed of RCP
3721	3531	Transparent block
4715	4661	Angular speed of RCP
4721	4531	Transparent block
5751	2088	Average coolant temperature
5761	1951	Cold leg outlet flow
7171	7005	Pressurizer pressure
7505	2291	Pressure in primary circuit
8033	2085	Effective rod control position

Tabla 3.7: Relación de las realimentaciones del modelo de planta PWR-W para el código TRETA. Versión CSN/DSE.

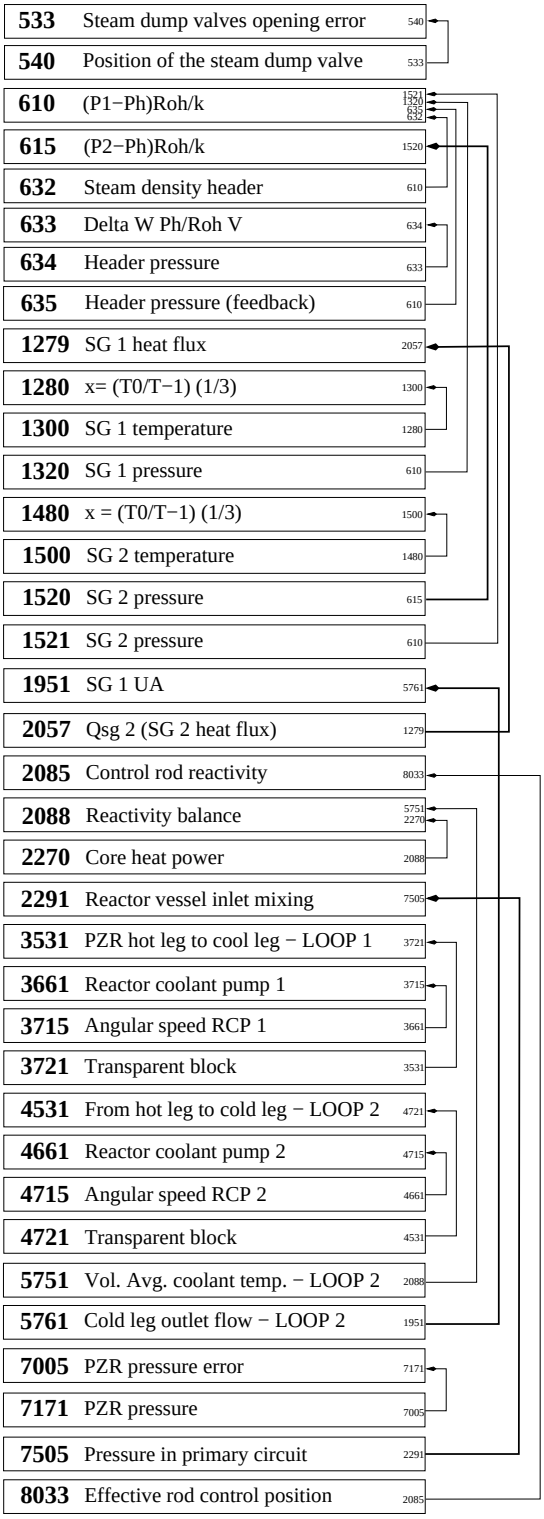


Figura 3.41: Esquema de realimentaciones del modelo de planta PWR-W. Versión CSN/DSE.

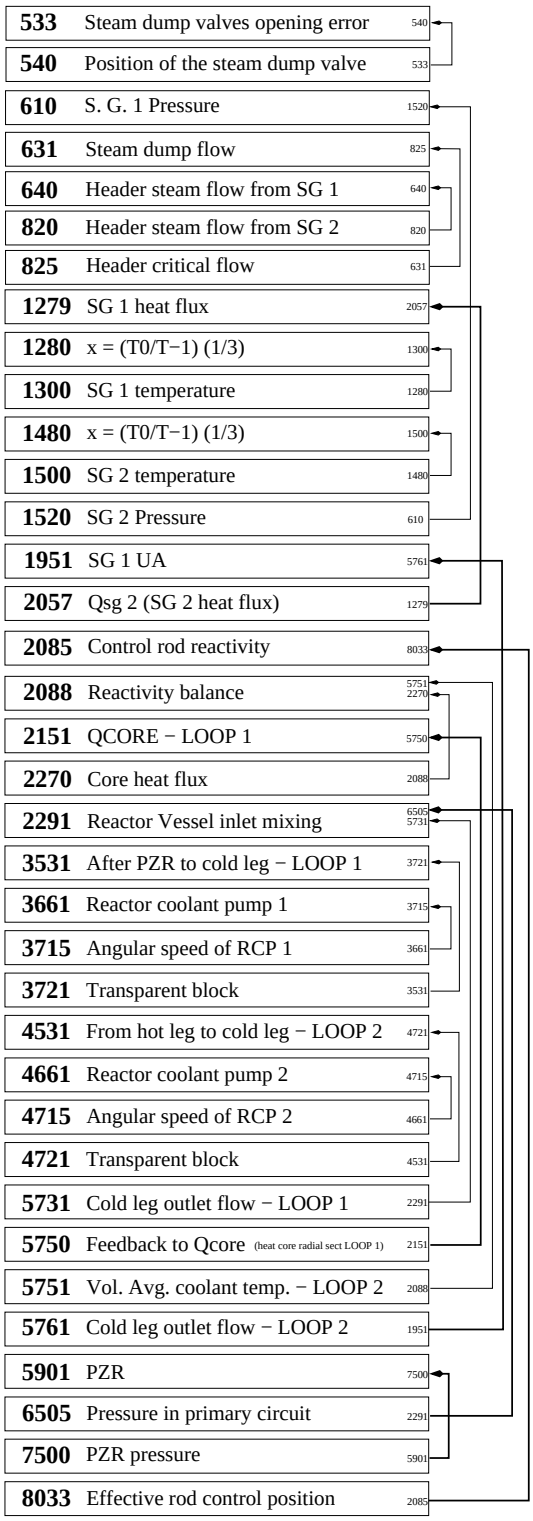


Figura 3.42: Esquema de realimentaciones del modelo de planta PWR-W. Versión ETSII-UPM.

Sistema/control		TT	MSLB	3RCP	ECCS	LOFW	LR-50
Control pres.	RV	NO	NO	NO	SI	SI	SI
	Ducha	NO	NO	NO	SI	SI	SI
	Calentadores prop.	SI	SI	SI	SI	SI	SI
	Calentadores apoyo	SI	SI	NO	NO	NO	SI
SV - PZR		NO	NO	NO	SI	NO	NO
Control de nivel	CVCS	SI	NO	SI	NO	SI	SI
	Ais. descarga	NO	SI	NO	NO	NO	NO
	Activ. calent.	NO	SI	NO	NO	NO	NO
	Desact. calent.	NO	SI	NO	NO	NO	NO
Control de barras		NO	NO	NO	NO	NO	NO
ECCS	HPIS	NO	SI	NO	—	NO	NO
RCP		NO	NO	SI	NO	NO	NO
Control de turbina		NO	NO	NO	NO	NO	SI
Alivio de vapor	modo T	SI	NO	SI	SI	SI	SI
AFW		SI	SI	SI	SI	SI	SI
RV secundario		SI	SI	NO	NO	NO	NO
SV secundario		NO	NO	NO	NO	NO	NO
MSIV		NO	SI	NO	NO	NO	NO
Disparo de turbina		—	SI	SI	SI	SI	SI

Tabla 3.8: Transitorios considerados para la verificación del modelo de planta PWR-W.

3.3 Transitorios de verificación del modelo

Los transitorios considerados para la verificación del modelo fueron:

- Disparo de las tres bombas del primario (3RCP).
- Disparo de turbina (TT).
- Rechazo de carga del 50 % (LR50).
- Señal espuria de inyección de seguridad (SI).
- Pérdida de agua de alimentación normal (LNFW).
- Rotura aislable en el colector de las líneas de vapor (MSLB).

En la Tabla 3.8, se incluye el conjunto de sistemas que se valida en cada transitorio, considerando su posible actuación. Como se puede comprobar, mediante este conjunto base de transitorios se cubre la actuación de los sistemas implementados en el modelo, permitiendo su ajuste para la correcta simulación de posteriores secuencias. Como conclusión general, el comportamiento del modelo es correcto, presentando un rango de operación en transitorios lo suficientemente amplio como para posibilitar la simulación de secuencias accidentales y, por lo tanto, la operación en emergencias. El alcance del modelo en este rango de operación se puso a prueba en las aplicaciones del mismo con el simulador integral, Capítulo 6.

3.3.1 Resultados de la simulación del disparo de las tres RCP

El disparo o perdida de las tres bombas del refrigerante del reactor se incluyen dentro de los transitorios de disminución de caudal de refrigerante del FSAR, como incidente de condición 2 o 3 con una frecuencia moderada a infrecuente. En los análisis de seguridad se estudia este transitorio suponiendo, además, que las válvulas de alivio del primario y secundario no actúan, actuando solamente las de seguridad. Esta consideración no se ha considerado en la simulación.

En este tipo de transitorios, el aumento inicial de la temperatura del moderador provoca una realimentación negativa que hace disminuir la potencia. Si a pesar de esta disminución, no se puede refrigerar adecuadamente el combustible se puede producir una disminución del DNBR que lleve al daño en las vainas del combustible, para evitar este posible daño se produce una señal de disparo del reactor.

A continuación se describen los sucesos observados en la simulación, Tabla 3.9:

- 300 s: se produce el disparo de las tres bombas de circulación del refrigerante del primario, Figura 3.3, lo que provoca una reducción del caudal que circula por el primario, Figura 3.6, y por lo tanto un deterioro significativo de la capacidad de evacuación del calor del núcleo, lo que lleva a un sobrecalentamiento del núcleo y en especial de las vainas del combustible. El aumento de la temperatura del moderador provoca una realimentación negativa que hace disminuir la potencia, pero esta disminución no es suficiente para evitar el calentamiento del núcleo y el aumento de temperatura del refrigerante, Figura 3.5.

- 301,80 s: tiene lugar el disparo del reactor por señal de bajo caudal en las líneas del primario, Figura 3.2, señal diseñada para evitar que se dañen las vainas del combustible al disminuir el DNBR, es decir, la capacidad de transmisión de calor, lo que llevaría a una fragilización de las vainas. El disparo del reactor produce la rápida disminución de la temperatura del núcleo, Figura 3.5, y también la disminución de la presión del primario, Figura 3.4, y del nivel del presionador, Figura 3.10.

- 302,20 s: el disparo de reactor conlleva el disparo de la turbina, Figura 3.12, lo que provoca un aumento de la presión en el secundario, Figura 3.14, y el alivio al condensador, Figura 3.16.

- 304,20 s: disparo de las bombas de agua de alimentación por disparo de la turbina, Figura 3.11. Al no haber agua de alimentación a los generadores de vapor se produce un rápido descenso del nivel de estos, Figura 3.13.

- 304,60 s: actuación del agua de alimentación auxiliar por disparo de las bombas de agua de alimentación, Figura 3.11, con lo que se reduce la pérdida de inventario de agua y a largo plazo se recupera el nivel de los generadores de vapor, Figura 3.13.

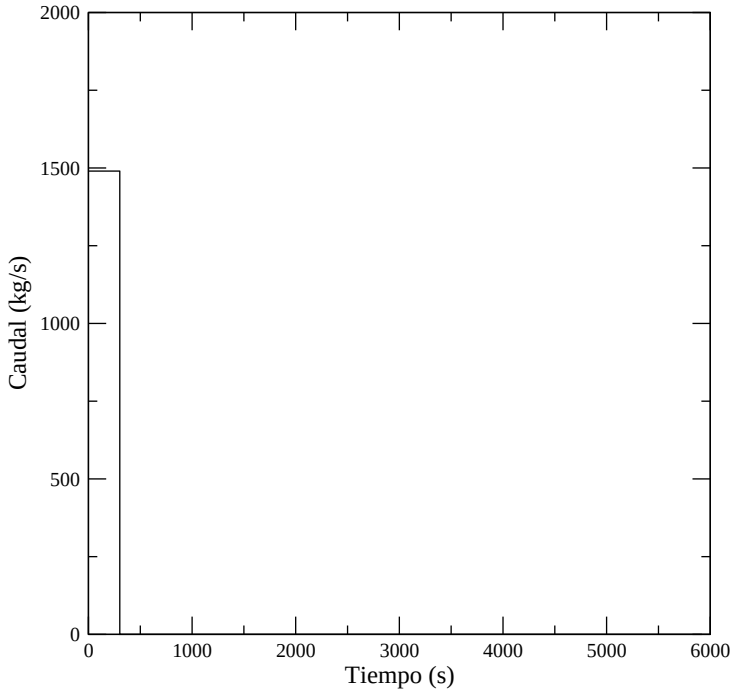
- 310,80 s: apertura de las válvulas de alivio y seguridad de los generadores de vapor por alta presión en el secundario, Figura 3.15, ya que se alcanza el tarado de presión de

dichas válvulas al no tener el alivio de vapor al condensador suficiente capacidad de alivio, Figura 3.14. La apertura de las válvulas de alivio de los generadores de vapor reduce la presión del secundario.

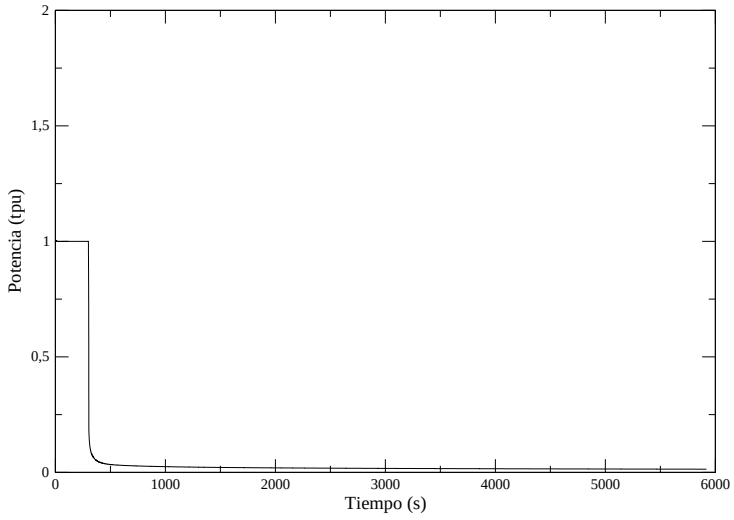
- 1769,40 - 2494,20 s: sucesivas aperturas de las válvulas de alivio del presionador por alta presión en el presionador, Figura 3.9. El ciclado tiene como origen la actuación de los calentadores a plena potencia para recuperar la presión del primario, Figura 3.8. Esto es debido a que el control PI ha realizado la integración del error negativo durante unos 1000 segundos. Dicha actuación hasta que se compensa el efecto integral del error provoca en nuestro modelo que la presión alcance el tarado de las válvulas de alivio, Figura 3.4.
- Final: en la finalización de la simulación se tienen los siguientes resultados:
  - La presión en el circuito primario se estabiliza en $15{,}5 \cdot 10^6$ Pascales.
  - La presión en el circuito secundario se estabiliza en $7{,}0 \cdot 10^6$ Pascales.
  - La temperatura media del primario se estabiliza en 293 ^{o}C.

Actuaciones automáticas	**Tiempo (s)**
Disparo de las tres RCP	300
Disparo del reactor por la señal de bajo caudal en las líneas del RCS	301,80
Disparo de la turbina por disparo del reactor Apertura del alivio al condensador por alta presión en los generadores de vapor	302,20
Disparo de las bombas de agua de alimentación por disparo de la turbina	304,20
Actuación del agua de alimentación auxiliar por disparo de las bombas de agua de alimentación	304,60
Apertura de las válvulas de seguridad y alivio de los generadores de vapor por alta presión en los generadores de vapor	310,80
Apertura de las válvulas de seguridad y alivio del presionador por alta presión en el presionador	1769,40 1837,80 1915,60 1999,60 2085,20 2181,40 2265,40 2344,80 2420,80 2494,20

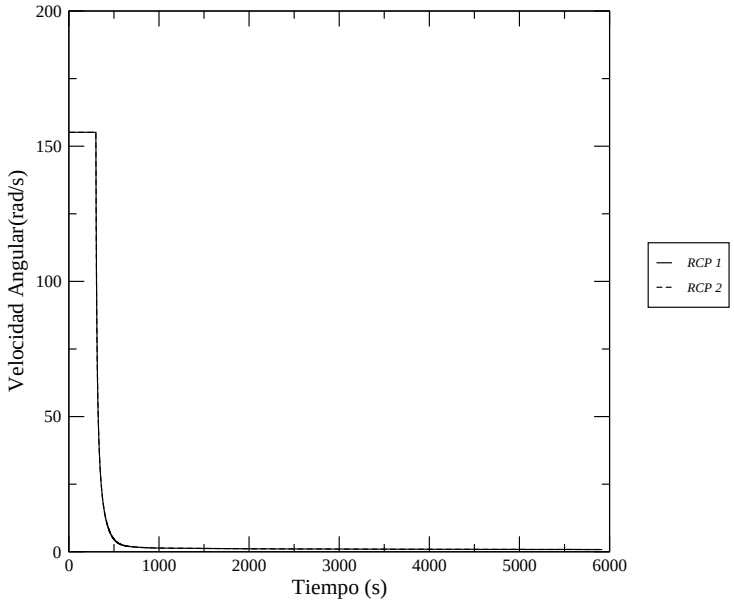
Tabla 3.9: Actuaciones automáticas que actúan en el transitorio de disparo de las tres RCP.



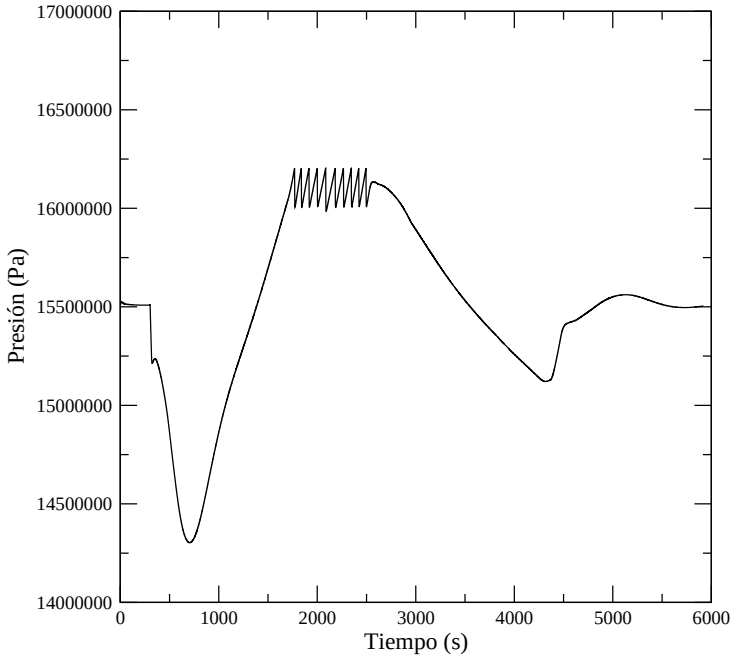
Gráfica 3.1: Disparo de las tres RCP. Caudal de vapor en la turbina.



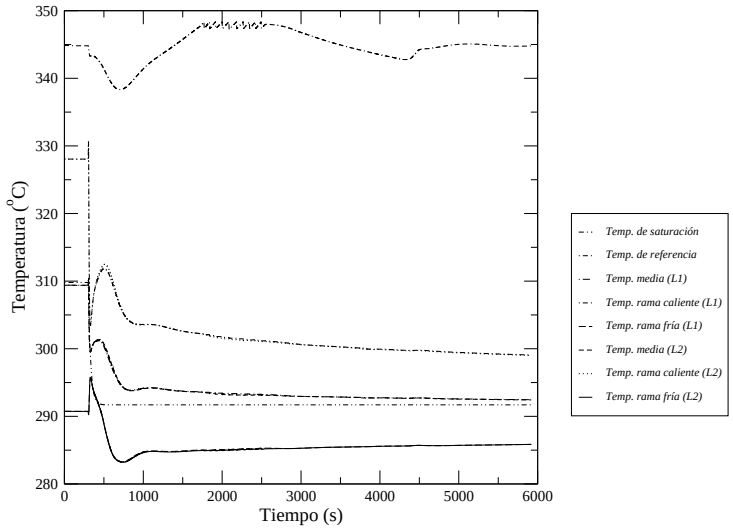
Gráfica 3.2: Disparo de las tres RCP. Potencia del reactor.



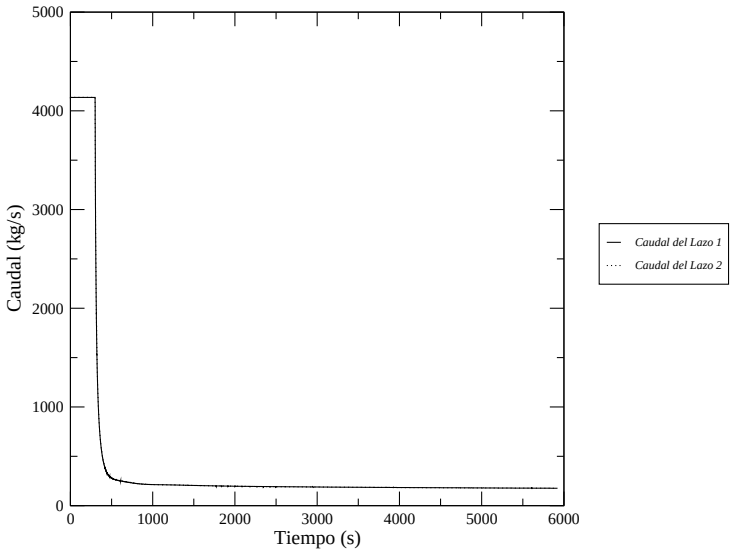
Gráfica 3.3: Disparo de las tres RCP. Velocidad de las RCP.



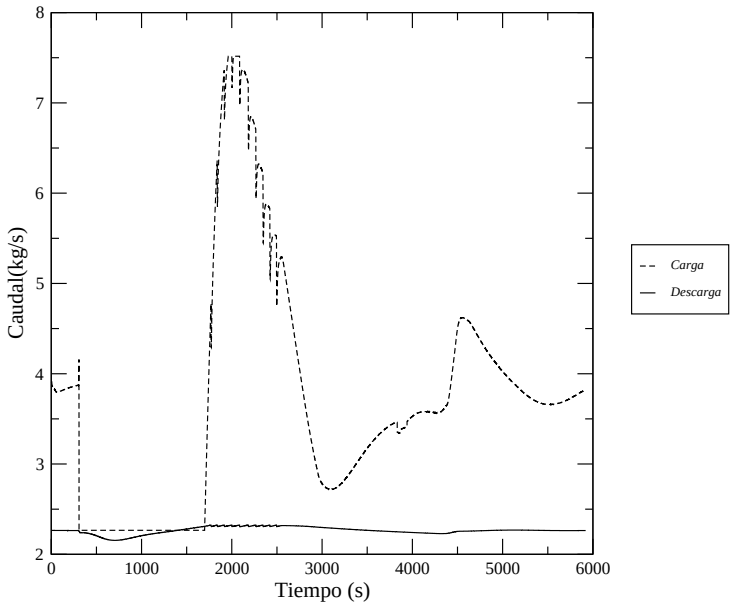
Gráfica 3.4: Disparo de las tres RCP. Presión del RCS.



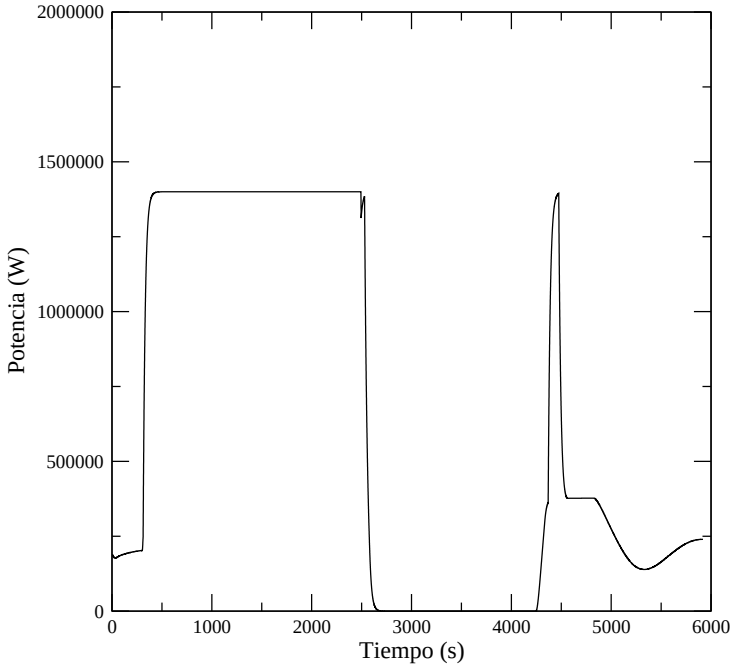
Gráfica 3.5: Disparo de las tres RCP. Temperaturas del RCS.



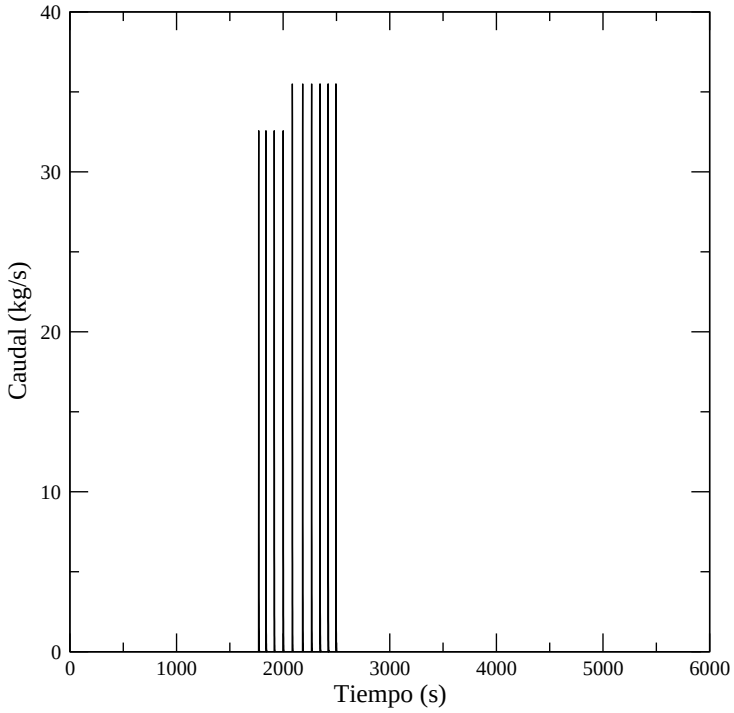
Gráfica 3.6: Disparo de las tres RCP. Caudales de los lazos del primario.



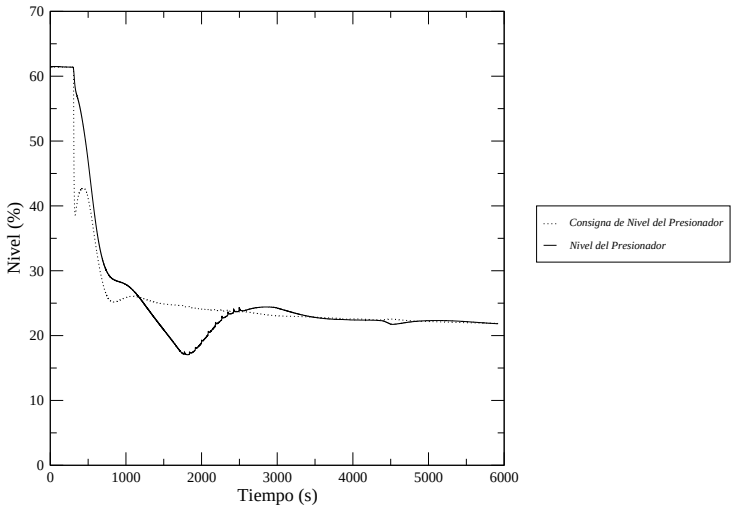
Gráfica 3.7: Disparo de las tres RCP. Caudales de la carga y la descarga del CVCS.



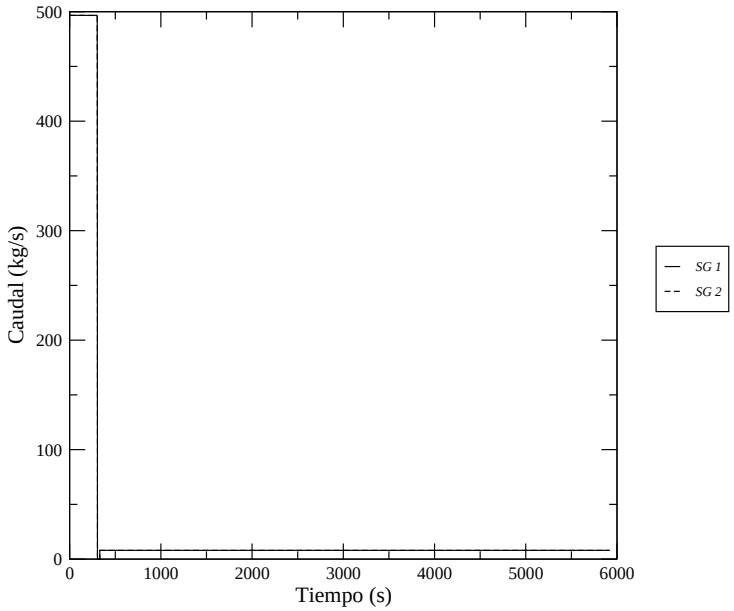
Gráfica 3.8: Disparo de las tres RCP. Potencia de los calentadores.



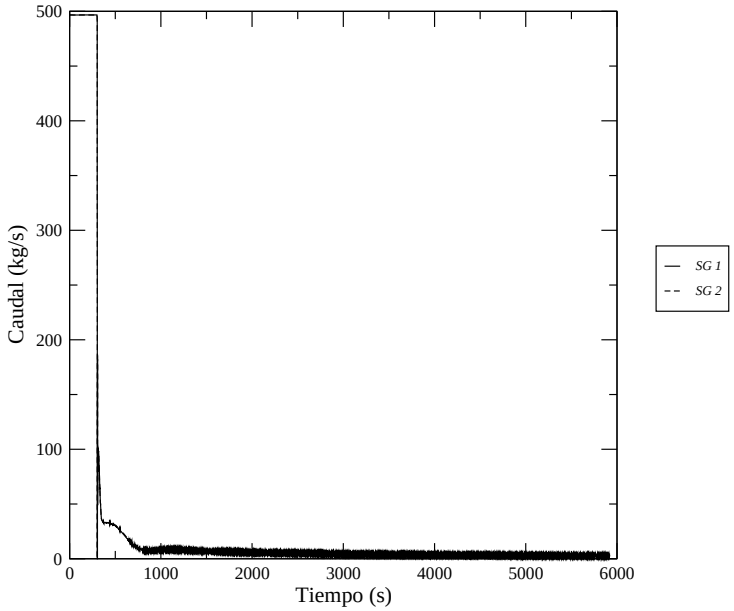
Gráfica 3.9: Disparo de las tres RCP. Caudal de las válvulas de alivio y seguridad del PZR.



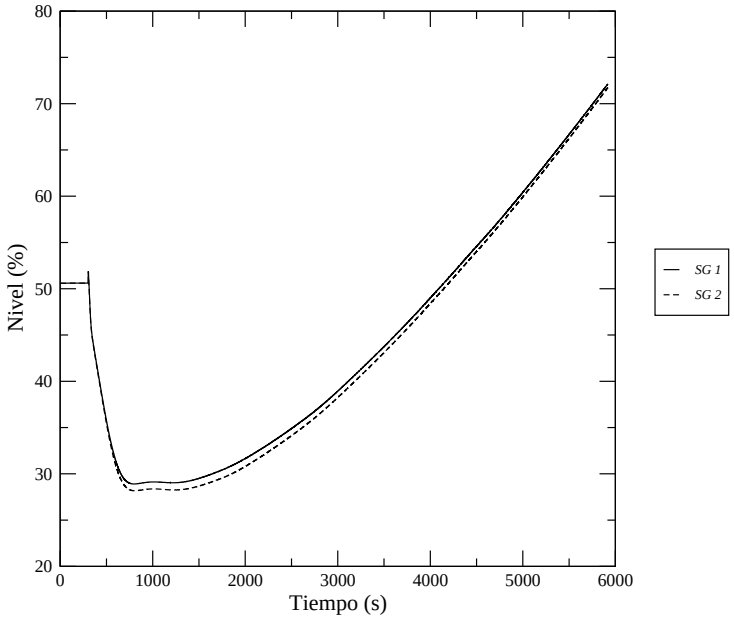
Gráfica 3.10: Disparo de las tres RCP. Nivel del PZR y consigna del nivel del PZR.



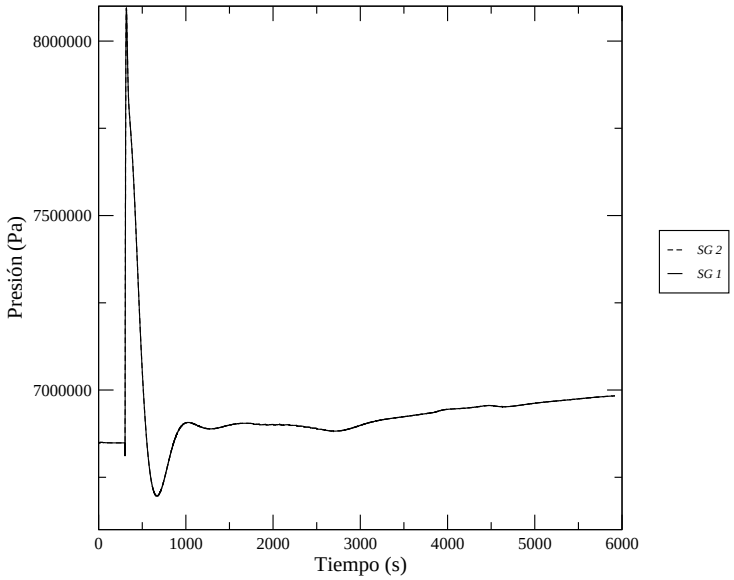
Gráfica 3.11: Disparo de las tres RCP. Caudales del agua de alimentación de los generadores de vapor.



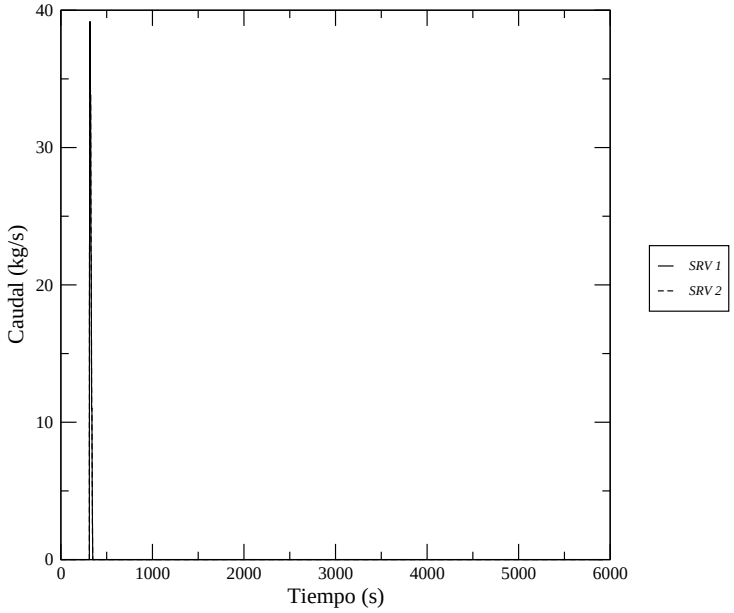
Gráfica 3.12: Disparo de las tres RCP. Caudal de vapor del generador de vapor.



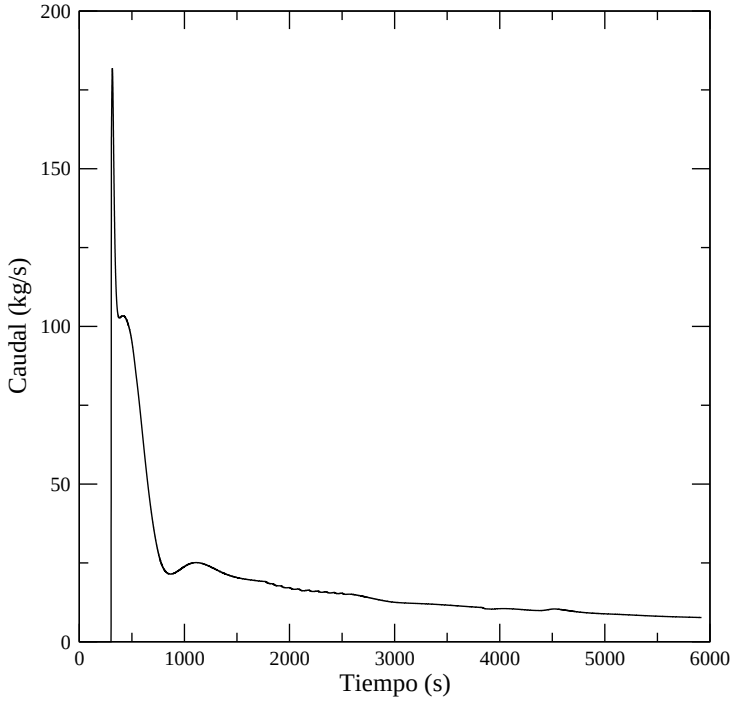
Gráfica 3.13: Disparo de las tres RCP. Niveles de los generadores de vapor.



Gráfica 3.14: Disparo de las tres RCP. Presión en los generadores de vapor.



Gráfica 3.15: Disparo de las tres RCP. Caudal de las válvulas de alivio y seguridad de los generadores de vapor.



Gráfica 3.16: Disparo de las tres RCP. Caudal de alivio al condensador.

3.3.2 Resultados de la simulación del disparo de turbina

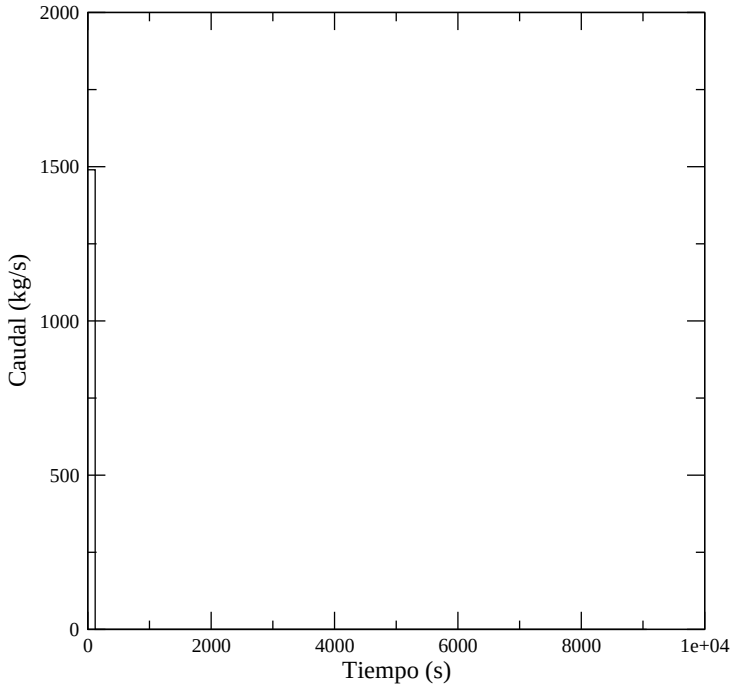
El transitorio de disparo de turbina se caracteriza por el disparo de la turbina que provoca el disparo del reactor, el resto de los sistemas de la planta funcionan correctamente.

A continuación se describen los sucesos observados en la simulación, Tabla 3.10:

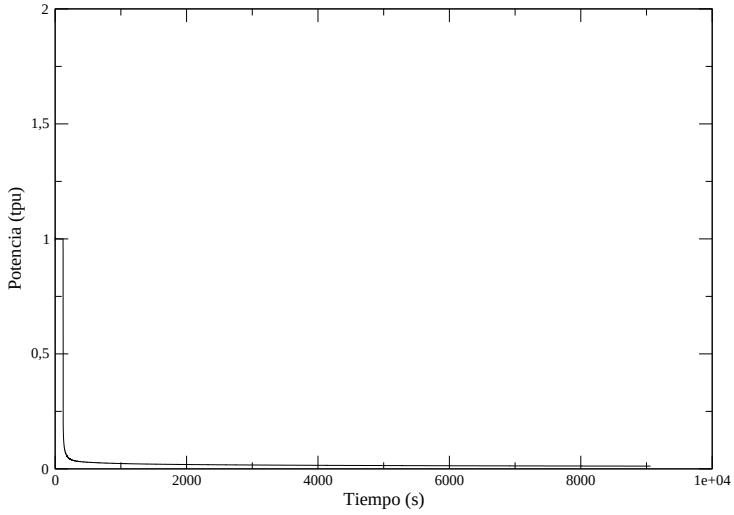
- 120 s: se produce el disparo de la turbina, Figura 3.17, y dispara el reactor, Figura 3.18, produciéndose la apertura del alivio al condensador, Figura 3.31. Todo ello provoca la caída de temperatura en el primario, Figura 3.20, una caída pronunciada de la presión, Figura 3.19, y la actuación de los calentadores a plena capacidad, Figura 3.24, para recuperar la presión en el primario. La contracción del refrigerante del primario produce una disminución progresiva del nivel del presionador, figura 3.25.
- 122,20 s: disparo de las bombas de agua de alimentación por disparo de la turbina, Figura 3.26, evitando la excesiva refrigeración del primario. El disparo de las bombas de agua de alimentación producirá un deterioro de la capacidad de transferencia de calor del primario al secundario al reducirse rápidamente el nivel de los generadores de vapor, Figura 3.28, y también conlleva el aumento de presión en los generadores de vapor, Figura 3.29.
- 122,40 s: actuación del agua de alimentación auxiliar por disparo de las bombas de agua de alimentación, Figura 3.26, provocando la recuperación a medio plazo de los niveles en los generadores de vapor, Figura 3.28.
- 126,60 s: apertura de las válvulas de alivio de los generadores de vapor, Figura 3.30, por alcanzarse la presión del tarado de dichas válvulas, lo que provoca la caída de la presión en el secundario, Figura 3.29.
- 833,00 s: apertura de la ducha del presionador por alta presión en el primario, Figura 3.23.
- 3592,00 s: aislamiento de la descarga del CVCS por bajo nivel en el presionador, menos del 15 %, Figura 3.22, esto lleva a la recuperación del nivel del presionador, Figura 3.25.
- Final: en la finalización de la simulación se tienen los siguientes resultados:
  - La presión en el circuito primario se estabiliza en $15{,}5 \cdot 10^6$ Pascales.
  - La presión en el circuito secundario se estabiliza en $7{,}65 \cdot 10^6$ Pascales.
  - La temperatura media del primario se estabiliza en 293 ^{o}C.

Actuaciones automáticas	**Tiempo (s)**
Disparo de turbina Disparo del reactor por disparo de turbina Apertura del alivio al condensador por disparo de la turbina	120
Disparo de las bombas de agua de alimentación por disparo de la turbina	122,20
Actuación del agua de alimentación auxiliar por disparo de las bombas de agua de alimentación	122,40
Apertura de las válvulas de seguridad y alivio de los generadores de vapor por alta presión en los generadores de vapor	126,60
Apertura de la ducha del presionador por alta presión en el presionador	833,00
Aislamiento de la descarga del CVCS por bajo nivel en el presionador (<15 %)	3592,00

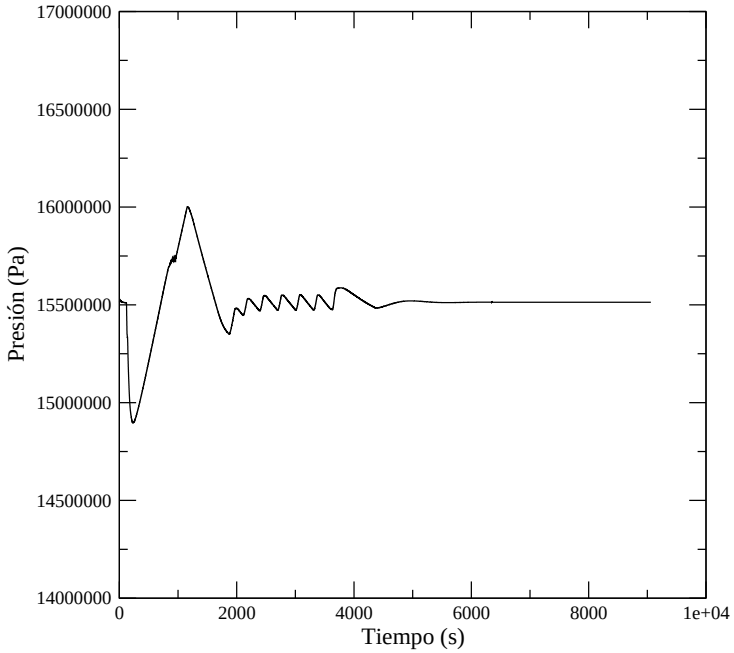
Tabla 3.10: Actuaciones automáticas que actúan en el transitorio de disparo de turbina.



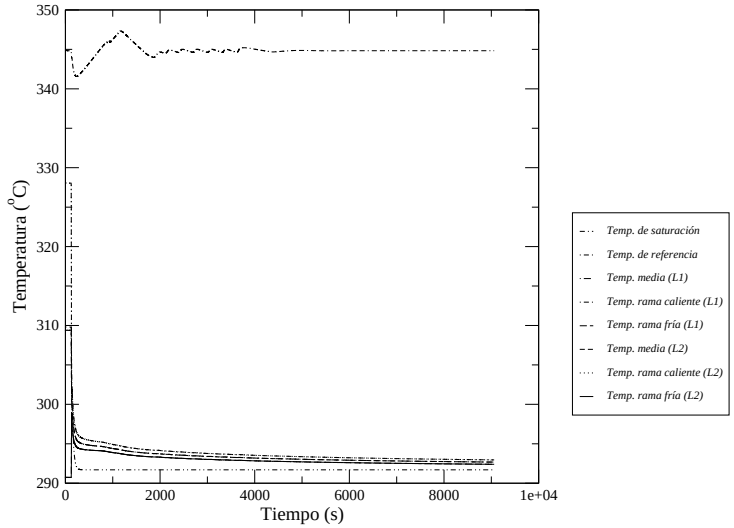
Gráfica 3.17: Disparo de turbina. Caudal de vapor en la turbina.



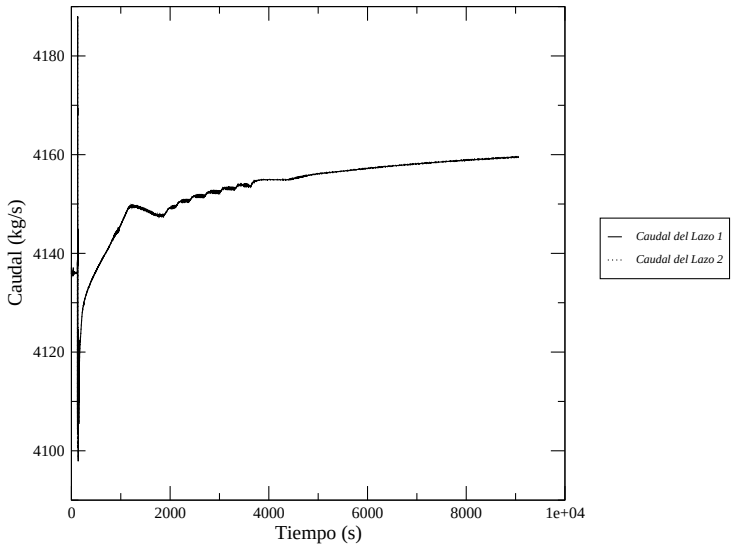
Gráfica 3.18: Disparo de turbina. Potencia del reactor.



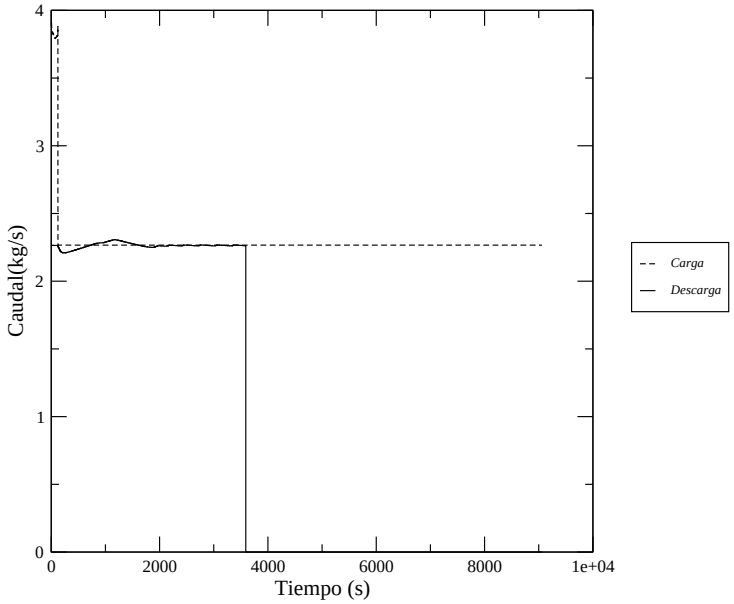
Gráfica 3.19: Disparo de turbina. Presión del RCS.



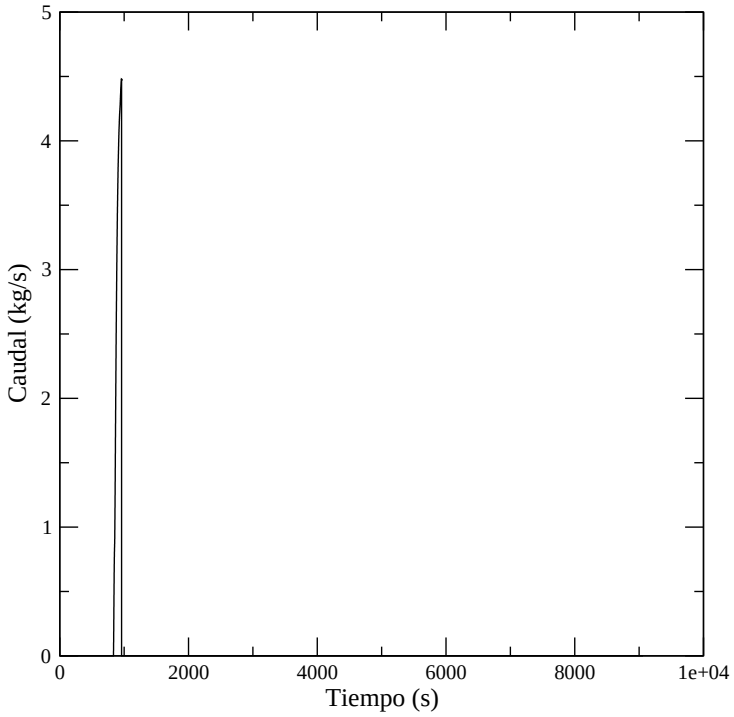
Gráfica 3.20: Disparo de turbina. Temperaturas del RCS.



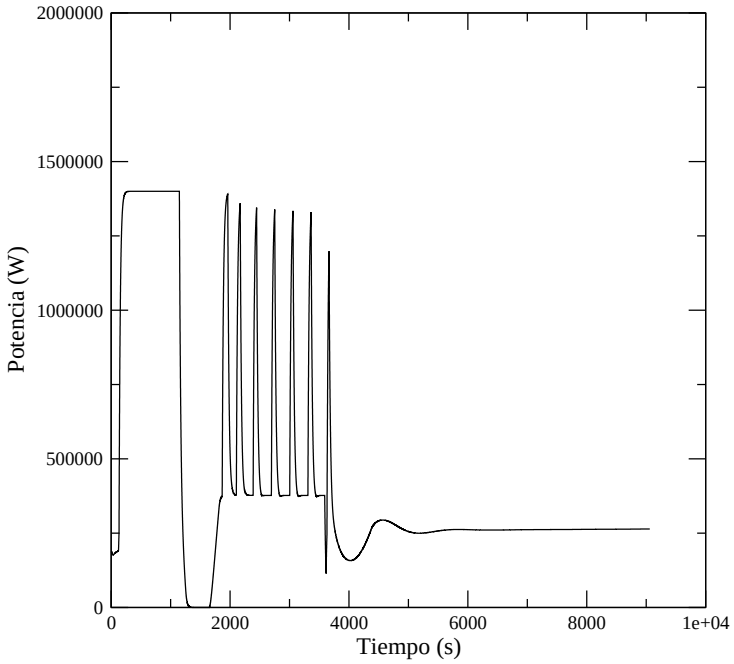
Gráfica 3.21: Disparo de turbina. Caudales de los lazos del primario.



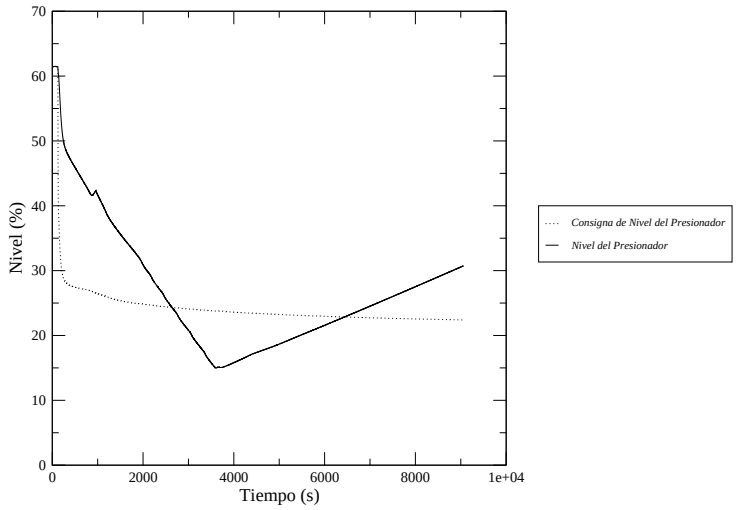
Gráfica 3.22: Disparo de turbina. Caudales de la carga y la descarga del CVCS.



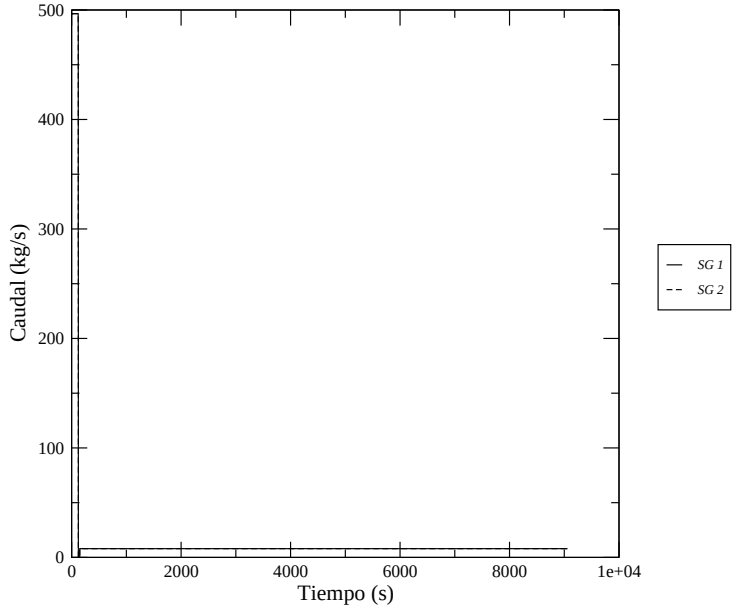
Gráfica 3.23: Disparo de turbina. Caudal de la ducha del PZR.



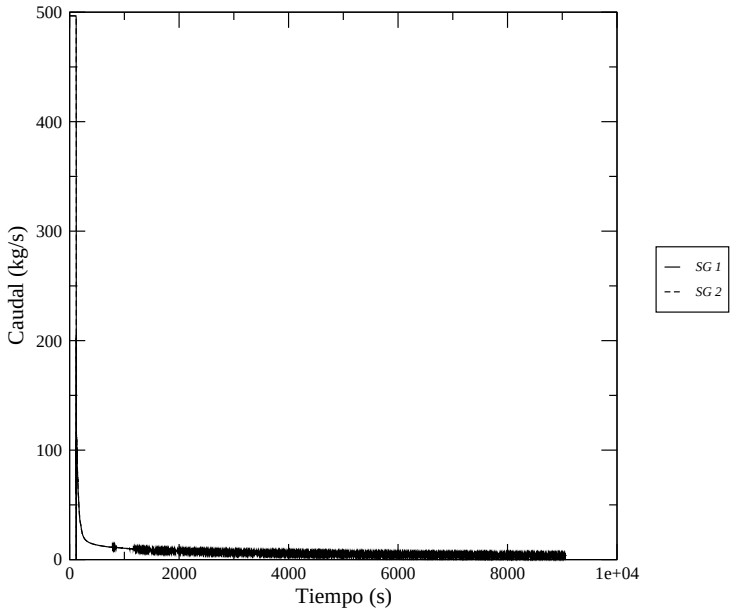
Gráfica 3.24: Disparo de turbina. Potencia de los calentadores.



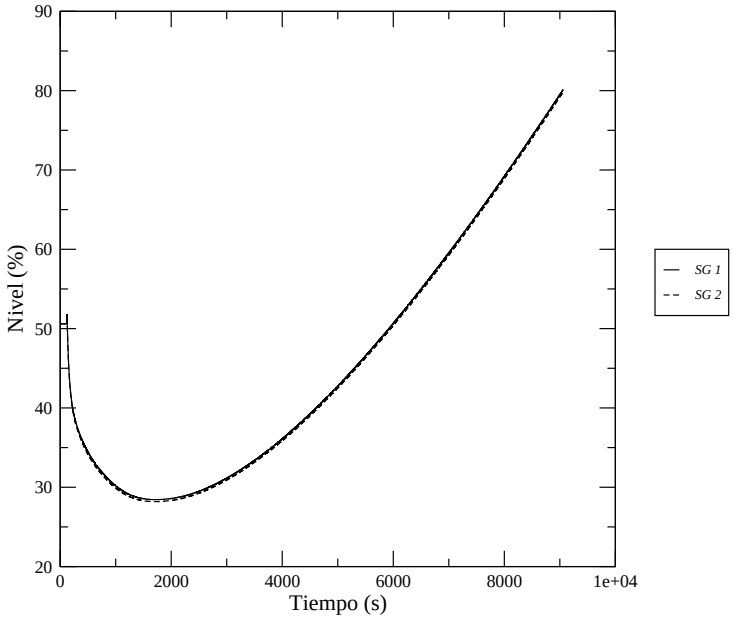
Gráfica 3.25: Disparo de turbina. Nivel del PZR y consigna del nivel del PZR.



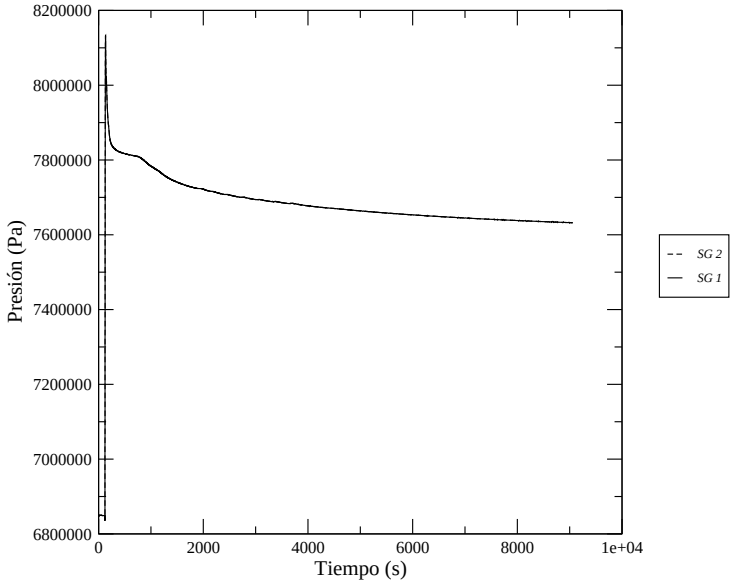
Gráfica 3.26: Disparo de turbina. Caudales del agua de alimentación de los generadores de vapor.



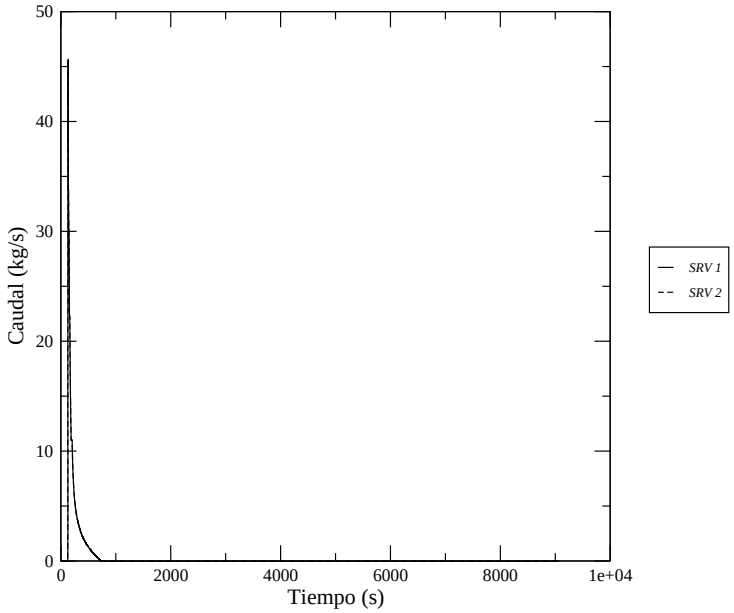
Gráfica 3.27: Disparo de turbina. Caudales de vapor de los generadores de vapor.



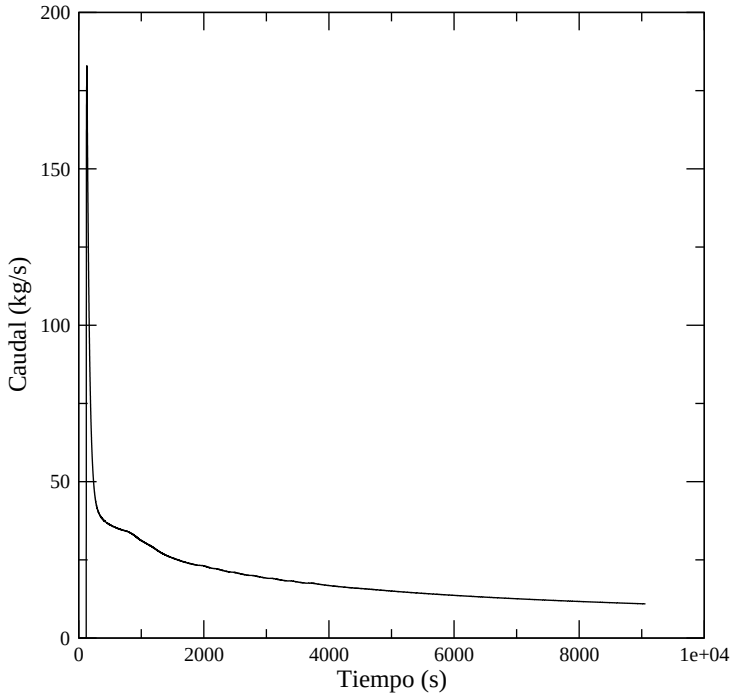
Gráfica 3.28: Disparo de turbina. Niveles de los generadores de vapor.



Gráfica 3.29: Disparo de turbina. Presión en los generadores de vapor.



Gráfica 3.30: Disparo de turbina. Caudal de las válvulas de alivio y seguridad de los generadores de vapor.



Gráfica 3.31: Disparo de turbina. Caudal de alivio al condensador.

3.3.3 Resultados de la simulación del rechazo de carga del 50 %

Este transitorio consiste en la realización de un rechazo de carga del 50 %. Tras asimilar la turbina el rechazo, la planta no debe disparar, debiendo ser capaz de absorber este rechazo mediante la actuación de las barras de control, el alivio al condensador y las válvulas de alivio de los generadores de vapor.

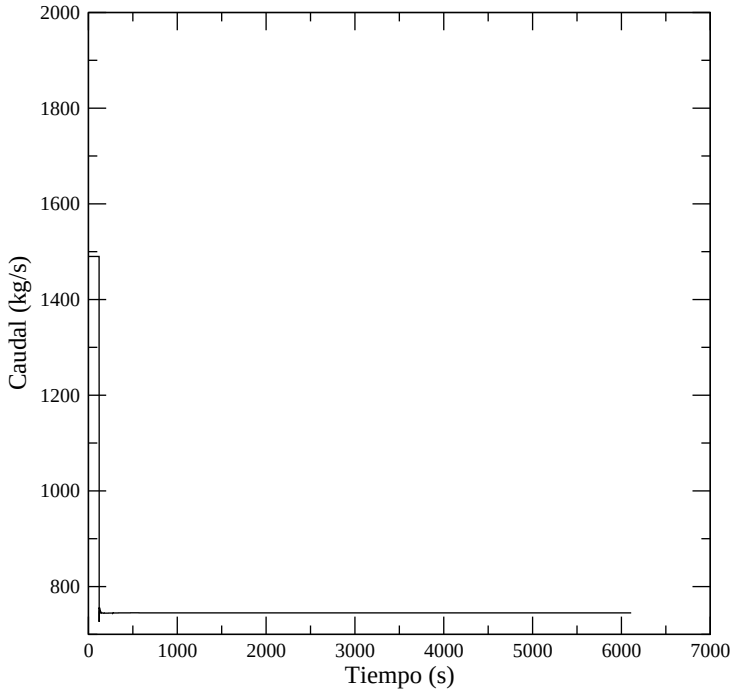
En nuestra simulación la inserción de las barras de control se produce a más velocidad de la recomendada con lo que provoca que la potencia baje mucho más rápido, produciendo unas temperaturas del primario durante el proceso de descenso de la potencia menores, lo que provoca que no descienda el nivel de los generadores de vapor y que no llegue la presión del secundario al tarado de las válvulas de alivio de los generadores de vapor.

A continuación se describen los sucesos observados en la simulación, Tabla 3.11:

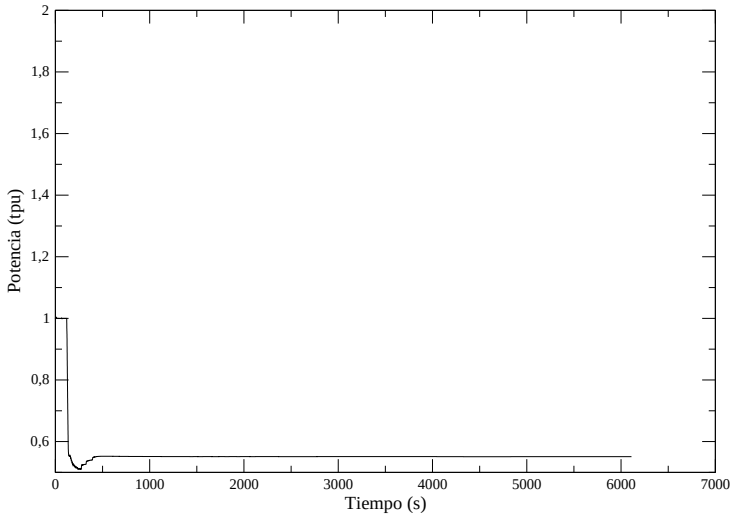
- 120 s: se produce el rechazo de carga del 50 %, Figura 3.32, y, como se observa en la Figura 3.33, se produce una reducción de la potencia del reactor demasiado rápida en comparación con la velocidad de inserción de barras propia del control de barras en modo de rechazo de carga. Este comportamiento se traduce en que las temperaturas que se alcanzan en las ramas calientes del primario sean menores que las esperadas, Figura 3.36, llevando a una menor transmisión de calor al secundario. Finalmente, esta reducción de potencia excesivamente rápida provoca que el aumento de presión en el secundario, Figura 3.43, sea a su vez menor del esperado, no siendo necesaria la actuación de las válvulas de alivio de los generadores de vapor para evacuar el exceso de vapor producido.
- 125,60 s: se activa la ducha del presionador por alta presión en el primario, Figuras 3.38 y 3.35.
- 135,00 s: demanda del alivio al condensador, Figura 3.45, por alta presión en los generadores de vapor, Figura 3.43, debido al rechazo de carga del 50 %. El alivio de vapor al condensador es suficiente para reducir la presión en el secundario. El rechazo de carga también produce la reducción del caudal de agua de alimentación de los generadores de vapor hasta la mitad del caudal nominal, Figura 3.41.
- 1335,40 - 2117,60 s: sucesivas aperturas de las válvulas de alivio del presionador por alta presión en el presionador, Figura 3.39, debido a la actuación de los calentadores a plena potencia para recuperar la presión del primario, Figura 3.34. De forma similar a los transitorios comentados anteriormente, estos calentadores están controlados por un PI, que al haber estado integrando negativamente durante unos 1000 segundos tiene que compensar este efecto integral negativo integrando positivamente, lo que provoca en nuestro modelo que la presión alcance el tarado de las válvulas de alivio, Figura 3.35.
- Final: en la finalización de la simulación se tienen los siguientes resultados:
  - La presión en el circuito primario tiende a estabiliza en $15{,}5 \cdot 10^6$ Pascales.
  - La presión en el circuito secundario se estabiliza en $7{,}65 \cdot 10^6$ Pascales.
  - La temperatura media del primario se estabiliza en 301,3 ^{o}C.

Actuaciones automáticas	**Tiempo (s)**
Rechazo de carga del 50 %	120
Apertura de la ducha del presionador por alta presión en el primario	125,60
Apertura del alivio al condensador por error de temperatura en el primario	135,00
Apertura de las válvulas de seguridad y alivio del presionador por alta presión en el primario	1335,40 1457,40 1560,20 1729,20 1870,00 1955,80 2117,60

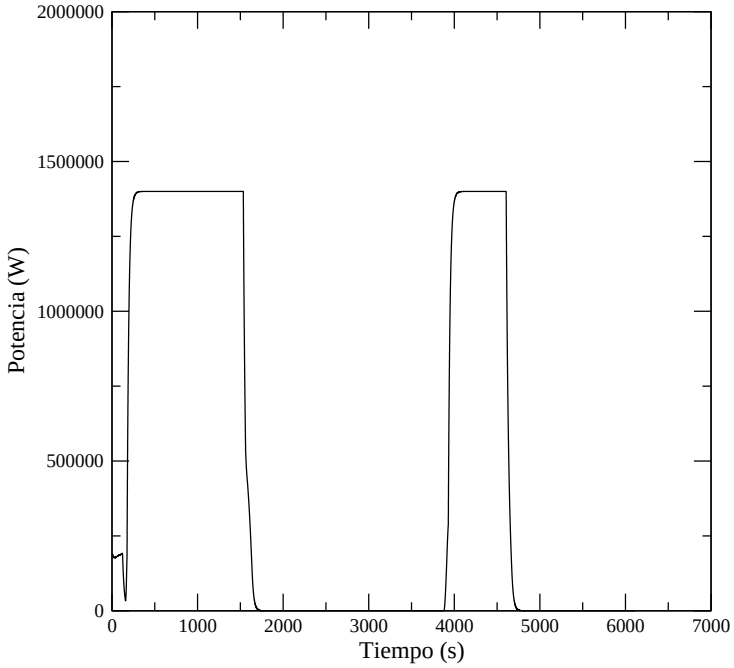
Tabla 3.11: Actuaciones automáticas que actúan en el transitorio de rechazo de carga del 50 %.



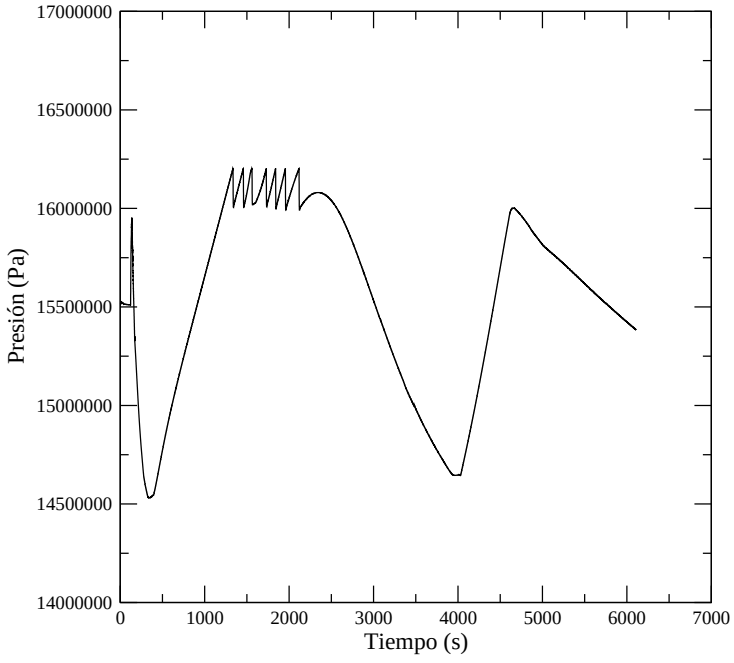
Gráfica 3.32: Rechazo de carga del 50 %. Caudal de vapor en la turbina.



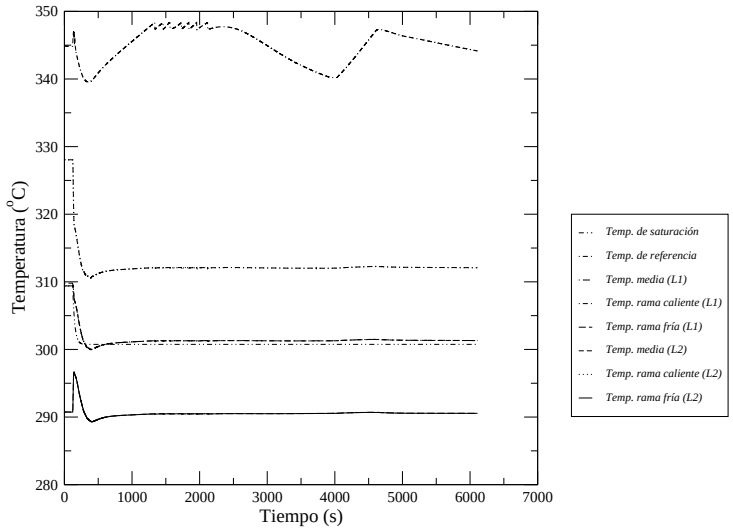
Gráfica 3.33: Rechazo de carga del 50 %. Potencia del reactor.



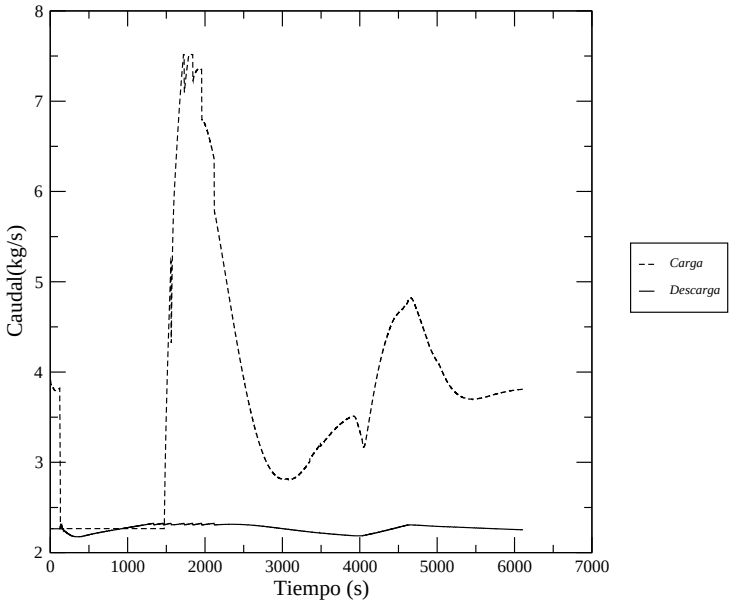
Gráfica 3.34: Rechazo de carga del 50 %. Potencia de los calentadores.



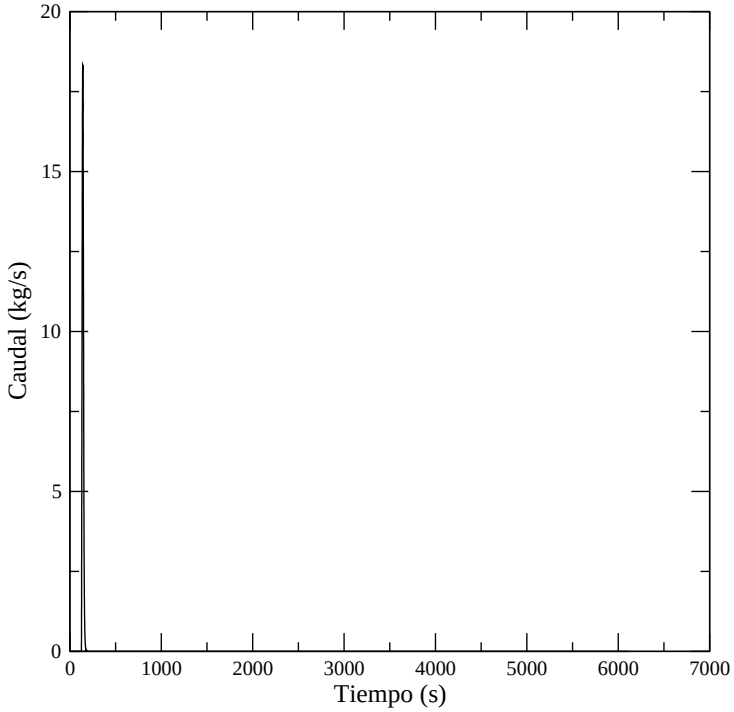
Gráfica 3.35: Rechazo de carga del 50 %. Presión del RCS.



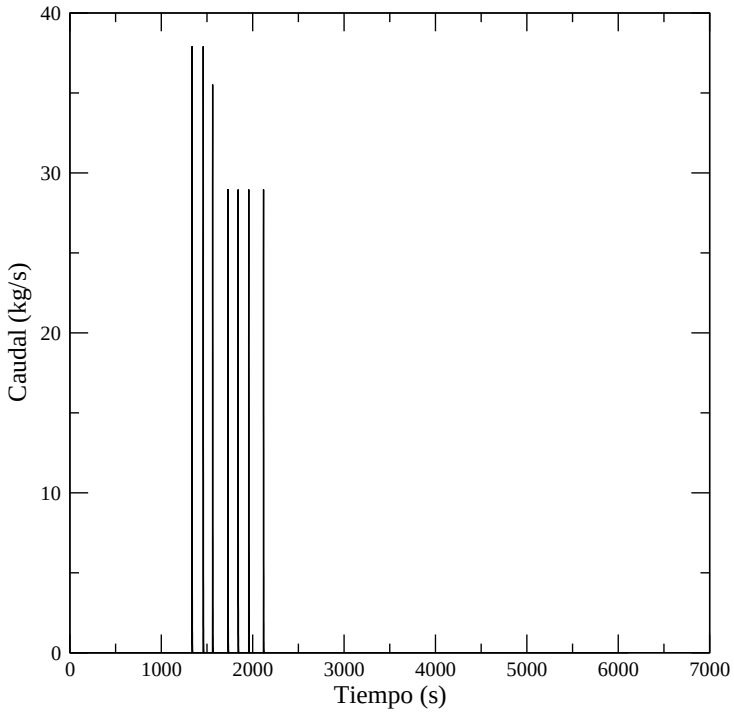
Gráfica 3.36: Rechazo de carga del 50 %. Temperaturas del RCS.



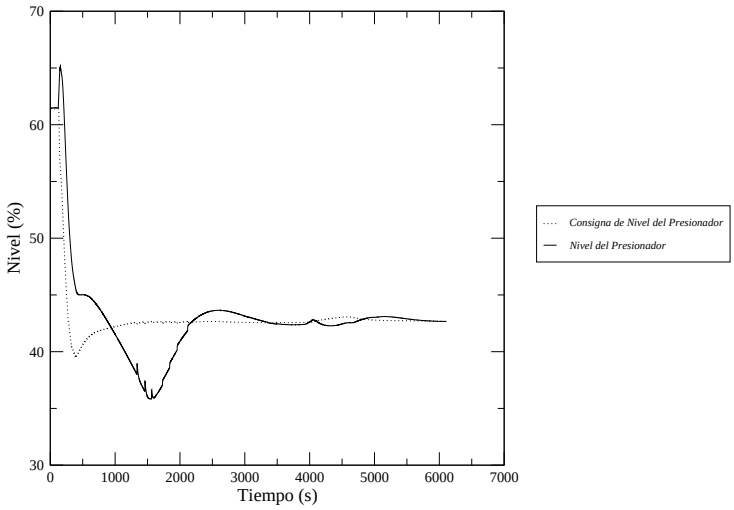
Gráfica 3.37: Rechazo de carga del 50 %. Caudales de la carga y la descarga del CVCS.



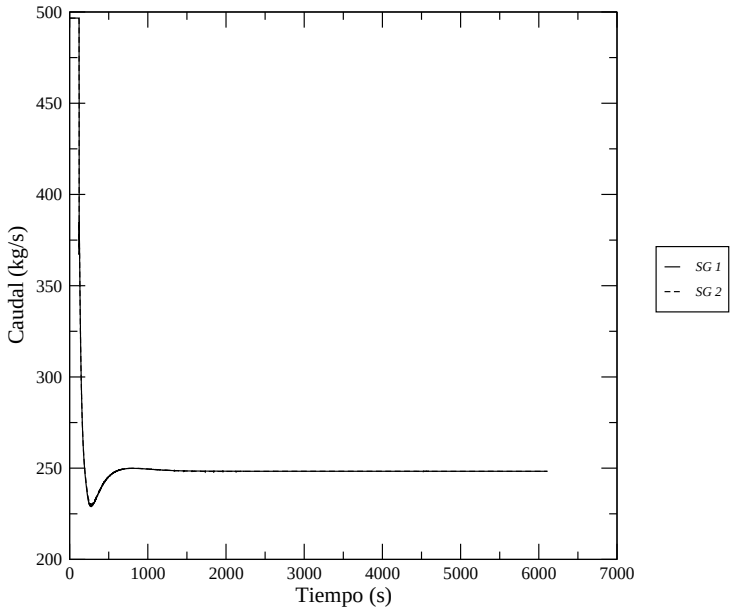
Gráfica 3.38: Rechazo de carga del 50 %. Caudal de la ducha del PZR.



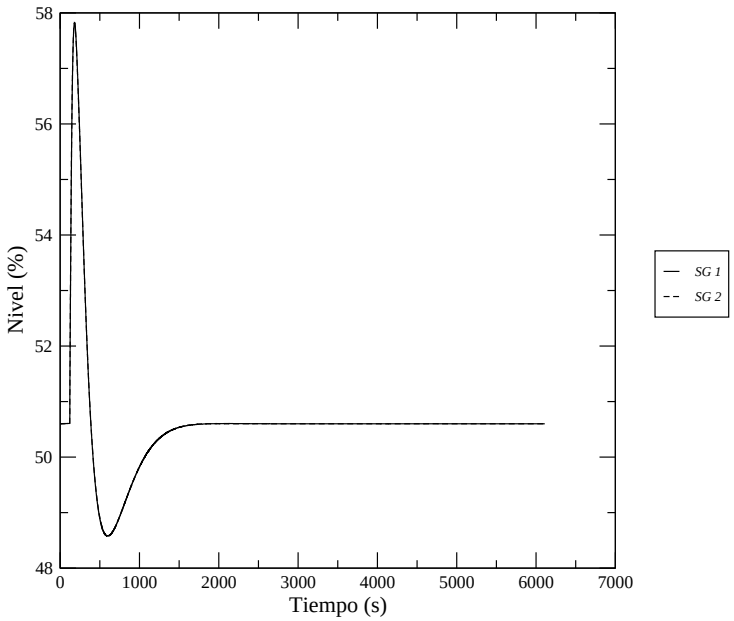
Gráfica 3.39: Rechazo de carga del 50 %. Caudal de las válvulas de alivio y seguridad del PZR.



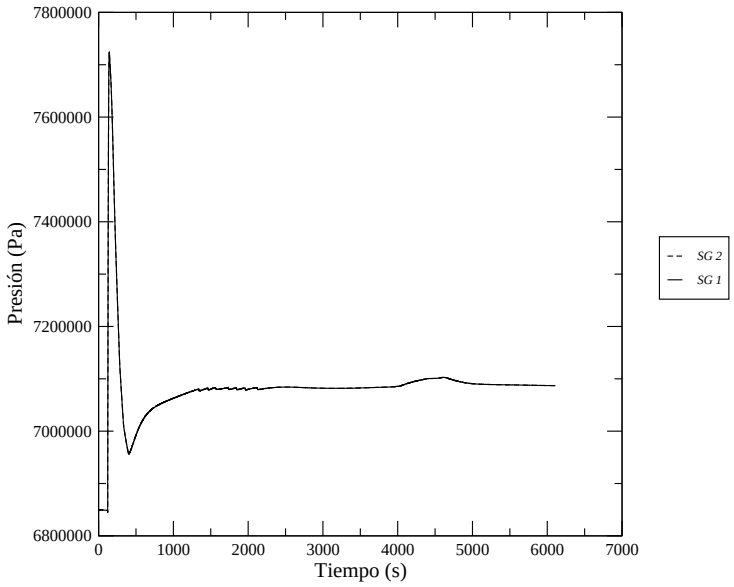
Gráfica 3.40: Rechazo de carga del 50 %. Nivel del PZR y consigna del nivel del PZR.



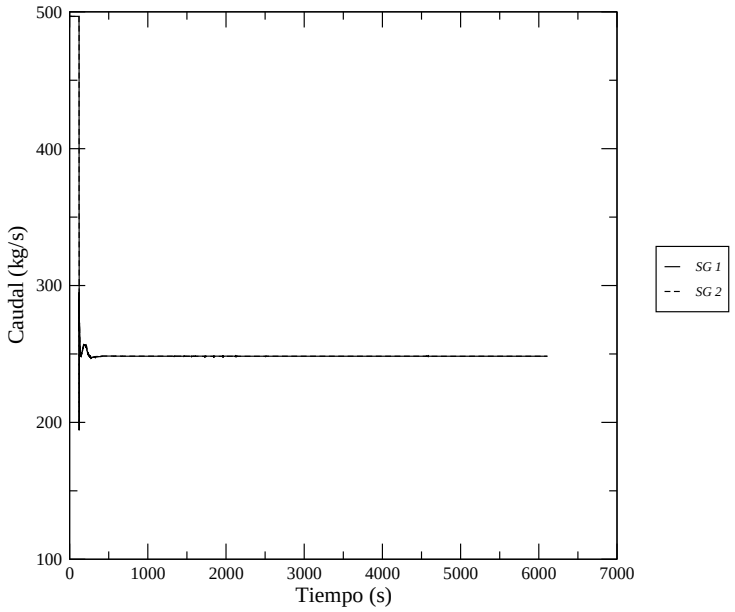
Gráfica 3.41: Rechazo de carga del 50 %. Caudales del agua de alimentación de los generadores de vapor.



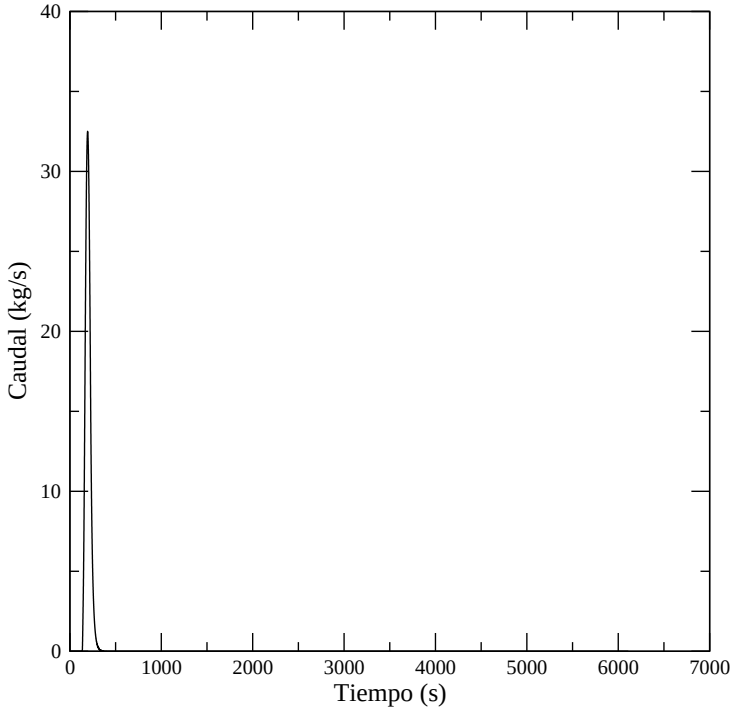
Gráfica 3.42: Rechazo de carga del 50 %. Niveles de los generadores de vapor.



Gráfica 3.43: Rechazo de carga del 50 %. Presión en los generadores de vapor.



Gráfica 3.44: Rechazo de carga del 50 %. Caudales de vapor de los generadores de vapor.



Gráfica 3.45: Rechazo de carga del 50 %. Caudal de alivio al condensador.

3.3.4 Resultados de la simulación de la inyección espuria de seguridad

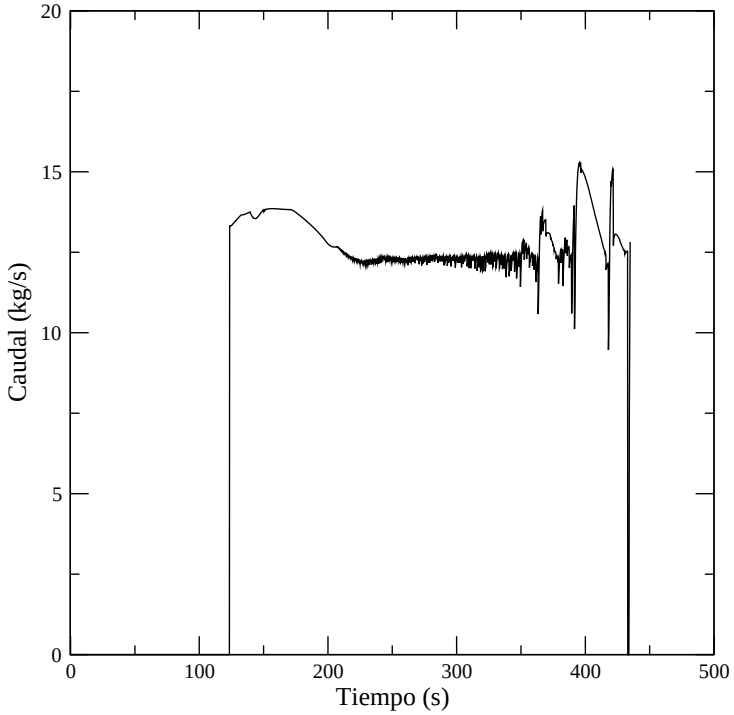
Este transitorio consiste en la inyección espuria de seguridad hasta el llenado del presionador, sin ninguna actuación manual.

A continuación se describen los sucesos observados en la simulación, Tabla 3.12:

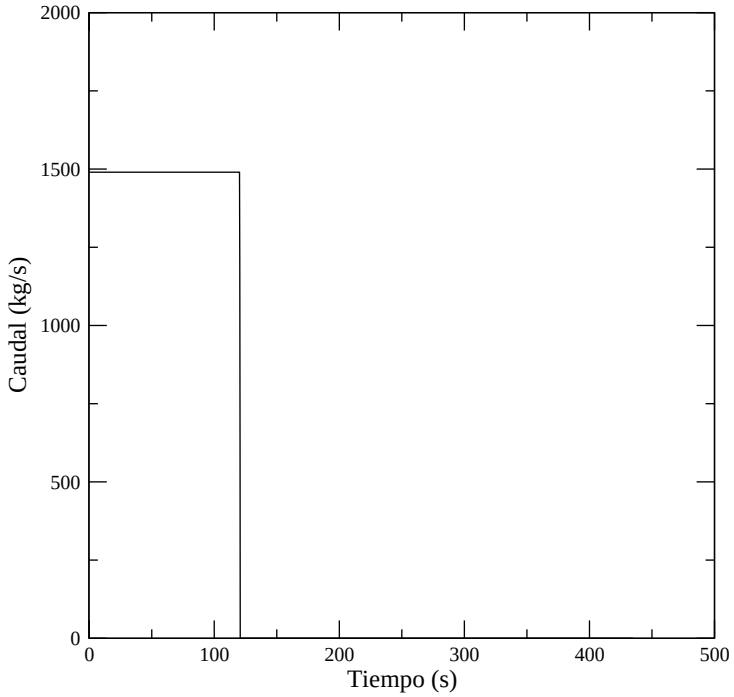
- 120 s: se produce la inyección espuria de seguridad, Figura 3.46, que produce a medio plazo el llenado del presionador, Figura 3.54.
- 120,20s : se produce debido a la inyección espuria de seguridad el disparo del reactor, Figura 3.48, el aislamiento del agua de alimentación normal, la actuación del agua de alimentación auxiliar, Figura 3.55, y el aislamiento de la carga y descarga del CVCS, Figura 3.51. El paso del agua de alimentación normal al auxiliar produce inicialmente una reducción rápida del nivel de los generadores de vapor y a largo plazo la recuperación de este nivel, Figura 3.56.
- 120,40 s: se produce el disparo de la turbina, Figura 3.47, por disparo del reactor y la apertura del alivio al condensador, Figura 3.60.
- 126,40 s: Apertura de las válvulas de alivio de los generadores de vapor, Figura 3.58, por alta presión en el secundario, Figura 3.57, debido a la reducción del aporte de agua de alimentación, Figura 3.55.
- 194,60 s: Apertura de la ducha por alta presión en el primario, Figura 3.52.
- 346,40 - 429,80 s: sucesivas aperturas de las válvulas de seguridad y alivio del presionador por alta presión en el presionador, Figura 3.53. De forma similar a los transitorios comentados anteriormente, estos calentadores están controlados por un PI, que al haber estado integrando negativamente durante unos 1000 segundos tiene que compensar este efecto integral negativo integrando positivamente, lo que provoca en nuestro modelo que la presión alcance el tarado de las válvulas de alivio, Figura 3.49.
- Final: En la finalización de la simulación se tienen los siguientes resultados:
  - La presión en el circuito primario tiende a estabilizarse en $15{,}5 \cdot 10^6$ Pascales.
  - La presión en el circuito secundario tiende a estabilizarse en $7{,}65 \cdot 10^6$ Pascales.
  - La temperatura media del primario se estabiliza en 297,2 ^{o}C.

Actuaciones automáticas	**Tiempo (s)**
Inyección espuria de seguridad (señal S)	120
Aislamiento del agua de alimentación normal por señal S Actuación del agua de alimentación auxiliar por señal S Disparo del reactor por señal S Aislamiento de la carga y descarga del CVCS por señal S	120,20
Disparo de turbina por disparo del reactor Apertura del alivio al condensador por alta presión en los generadores de vapor	120,40
Disparo de las bombas de agua de alimentación por disparo de la turbina	122,60
Apertura de las válvulas de seguridad y alivio de los generadores de vapor por alta presión en los generadores de vapor	126,40
Apertura de la ducha del presionador	194,60
Apertura de las válvulas de seguridad y alivio del presionador por alta presión en el presionador	346,40 360,20 376,00 414,80 429,80

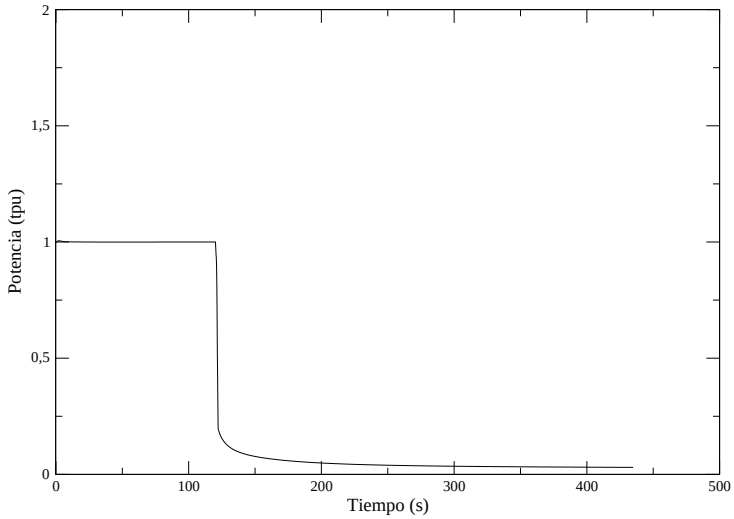
Tabla 3.12: Actuaciones automáticas que actúan en el transitorio de inyección espuria de seguridad.



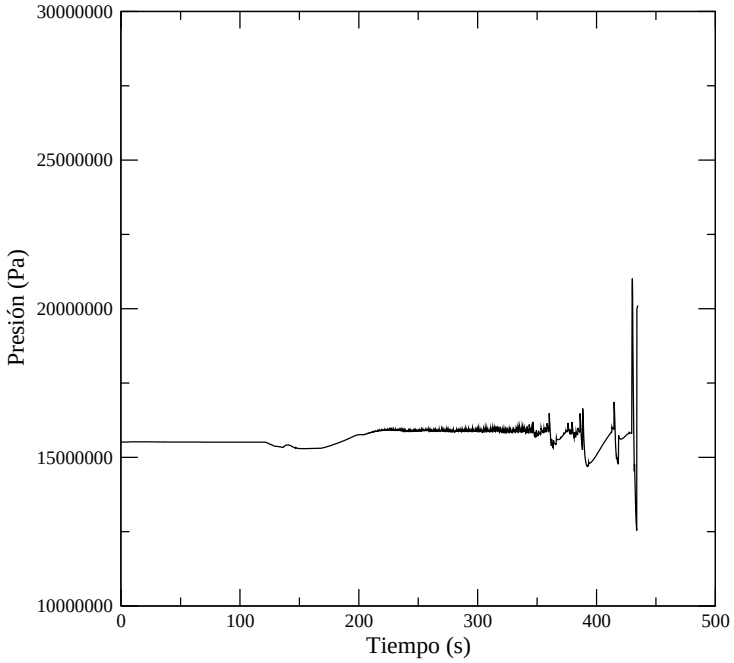
Gráfica 3.46: Inyección espuria de seguridad. Caudal de la inyección de seguridad.



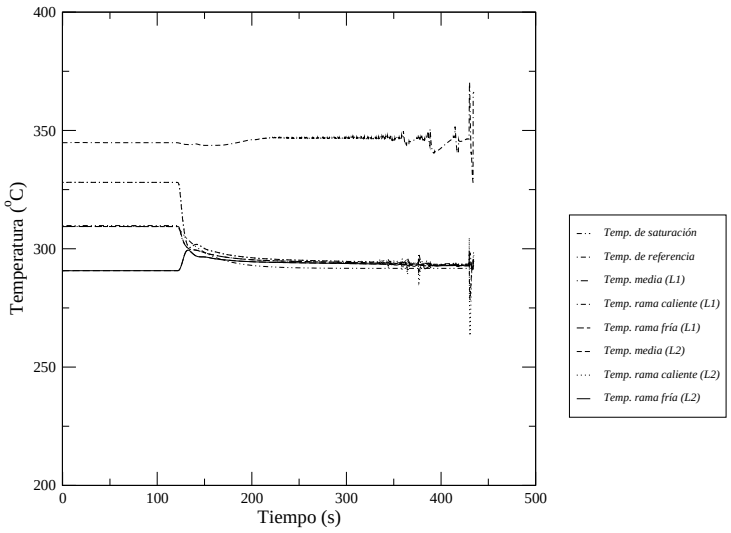
Gráfica 3.47: Inyección espuria de seguridad. Caudal de vapor en la turbina.



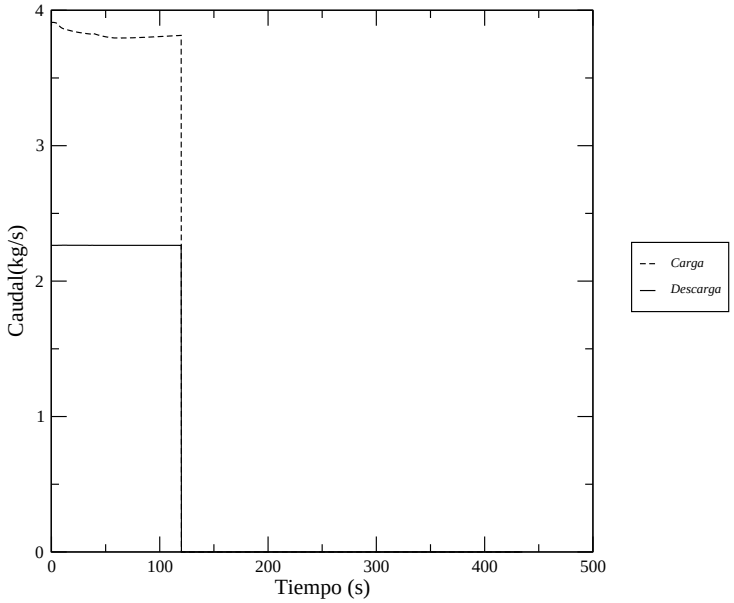
Gráfica 3.48: Inyección espuria de seguridad. Potencia del reactor.



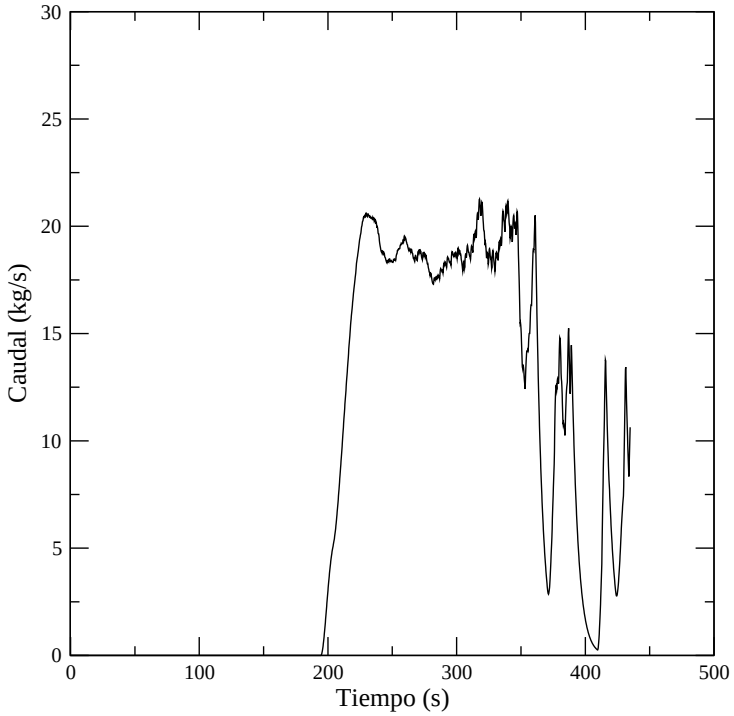
Gráfica 3.49: Inyección espuria de seguridad. Presión del RCS.



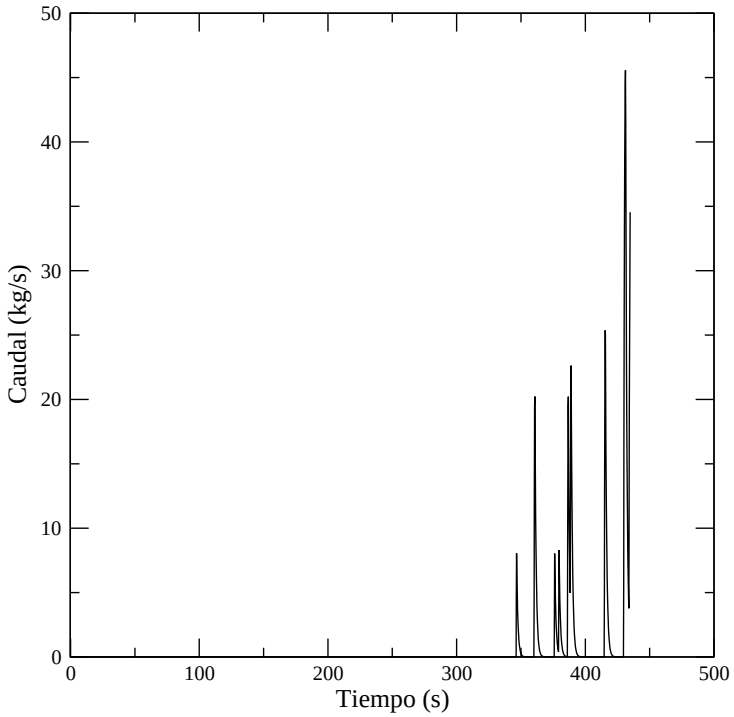
Gráfica 3.50: Inyección espuria de seguridad. Temperaturas del RCS.



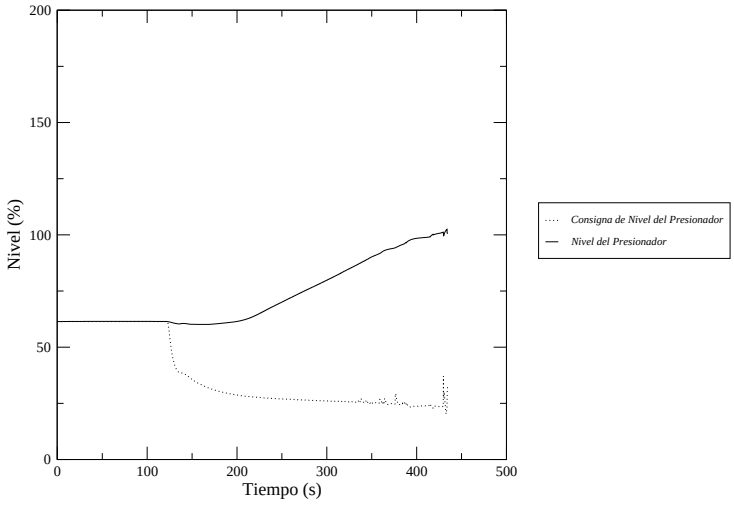
Gráfica 3.51: Inyección espuria de seguridad. Caudales de la carga y la descarga del CVCS.



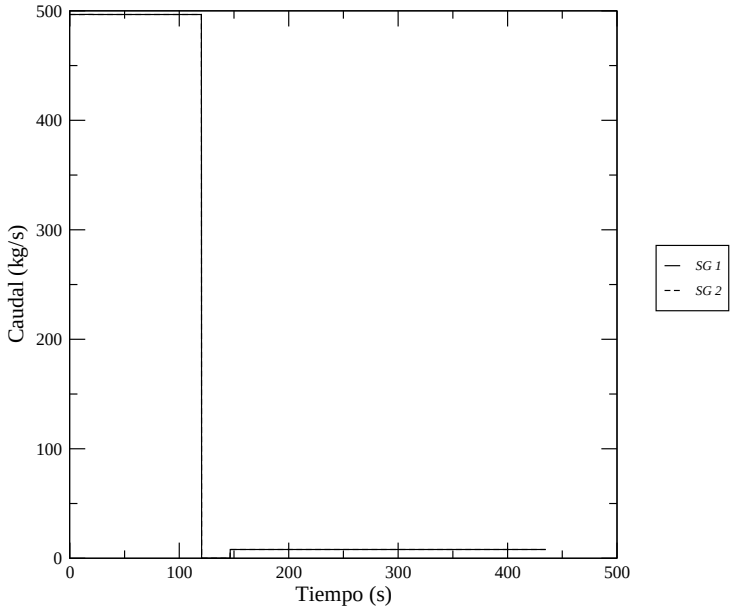
Gráfica 3.52: Inyección espuria de seguridad. Caudal de la ducha del PZR.



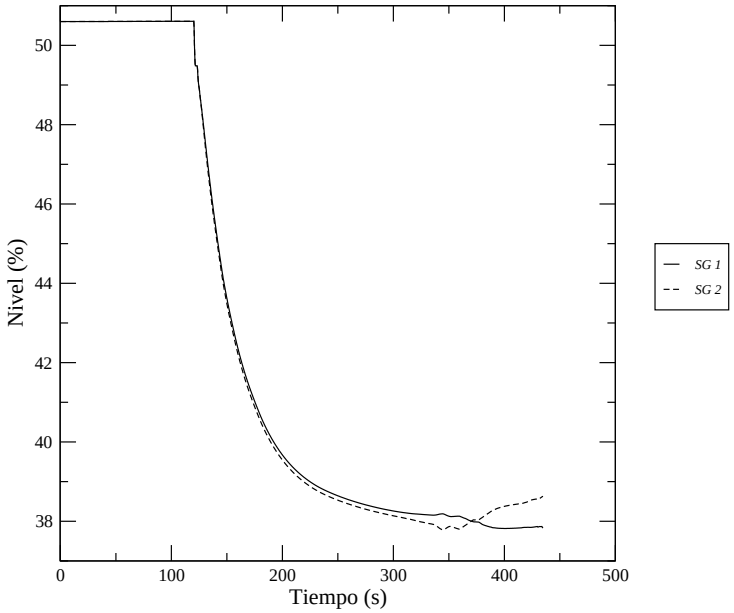
Gráfica 3.53: Inyección espuria de seguridad. Caudal de las válvulas de alivio y seguridad del PZR.



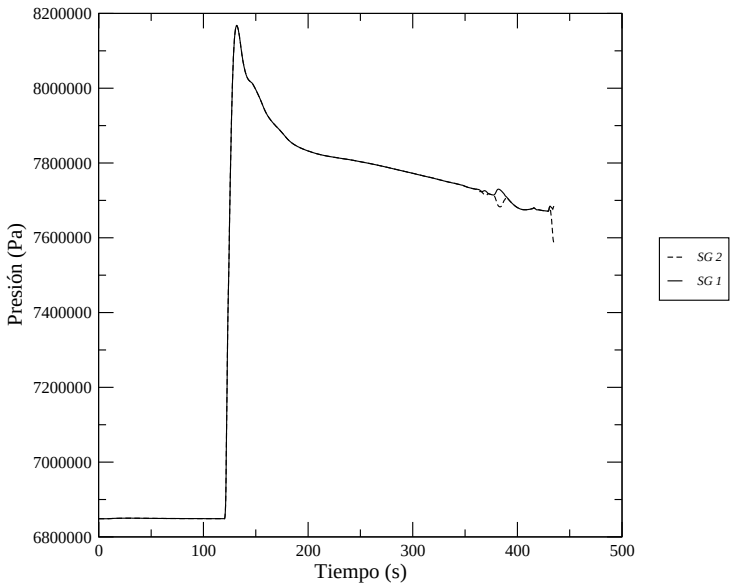
Gráfica 3.54: Inyección espuria de seguridad. Nivel del PZR y consigna del nivel del PZR.



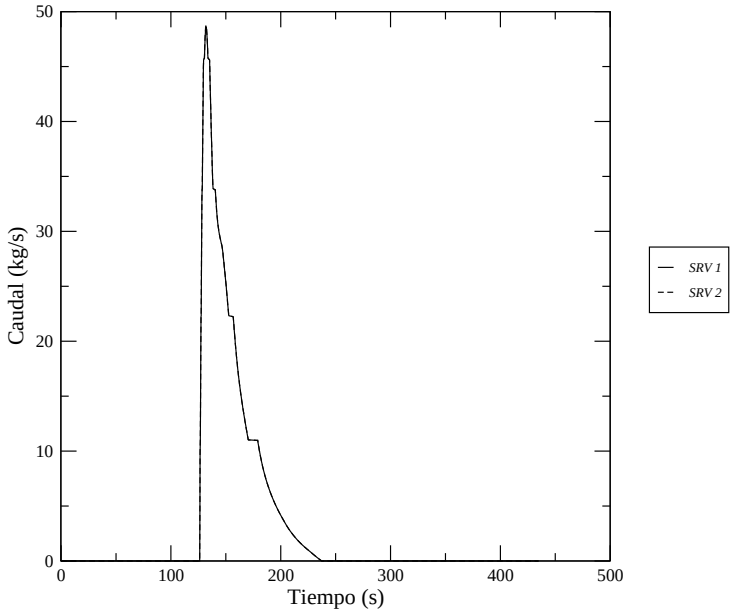
Gráfica 3.55: Inyección espuria de seguridad. Caudales del agua de alimentación de los generadores de vapor.



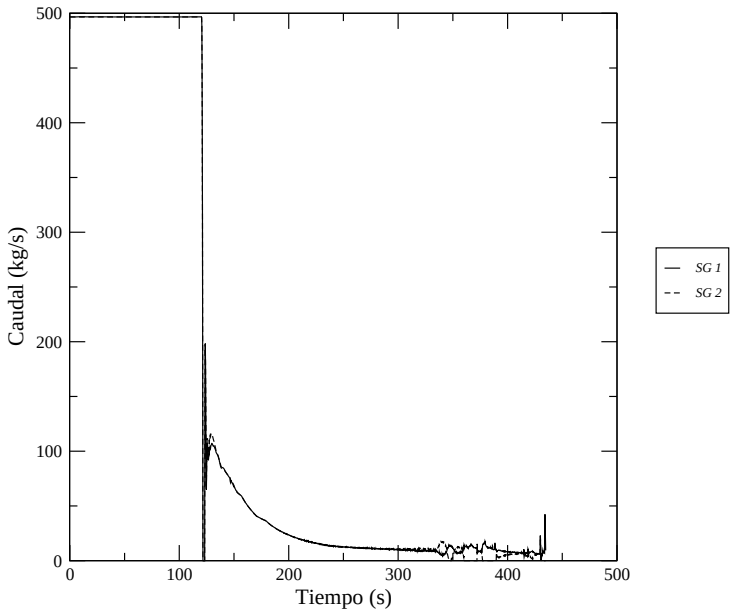
Gráfica 3.56: Inyección espuria de seguridad. Niveles de los generadores de vapor.



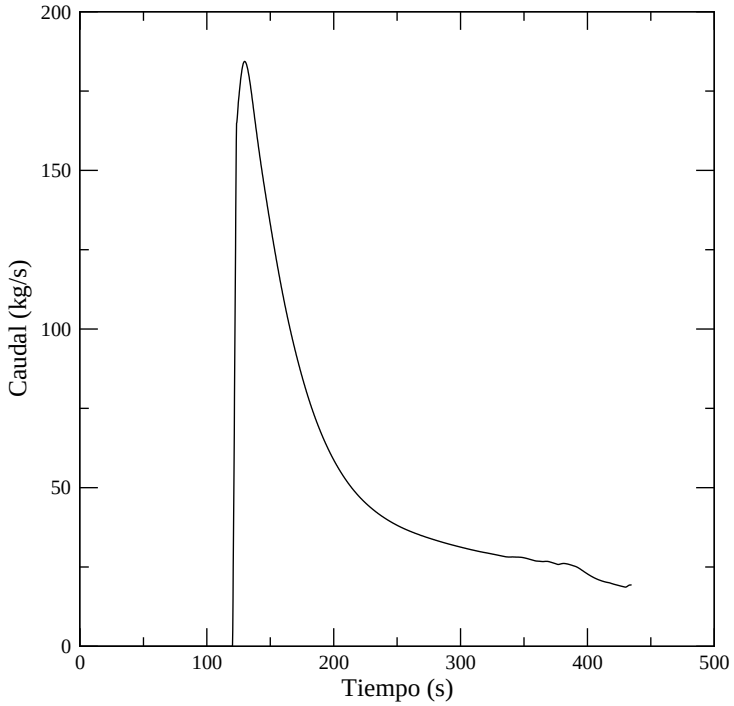
Gráfica 3.57: Inyección espuria de seguridad. Presión en los generadores de vapor.



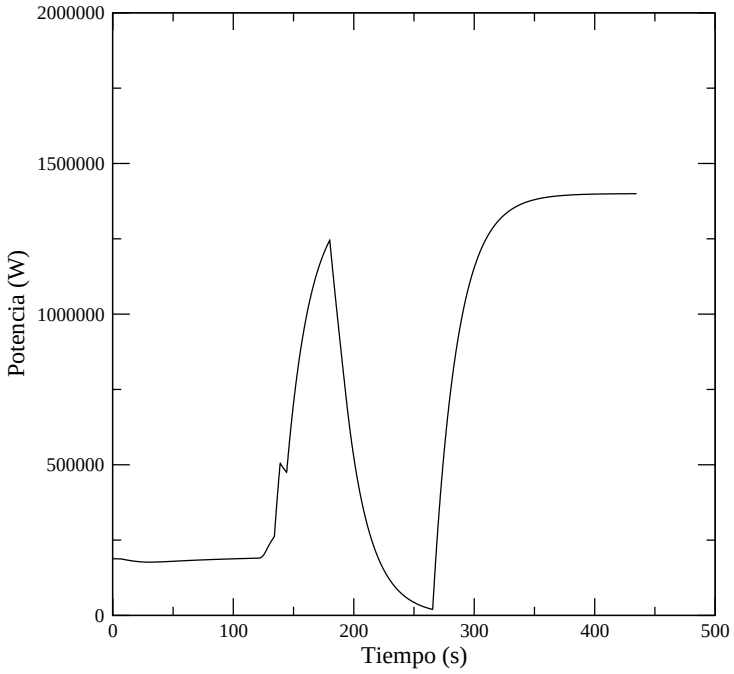
Gráfica 3.58: Inyección espuria de seguridad. Caudal de las válvulas de alivio y seguridad de los generadores de vapor.



Gráfica 3.59: Inyección espuria de seguridad. Caudales de vapor de los generadores de vapor.



Gráfica 3.60: Inyección espuria de seguridad. Caudal de alivio al condensador.



Gráfica 3.61: Inyección espuria de seguridad. Potencia de los calentadores.

3.3.5 Resultados de la simulación de la pérdida del agua de alimentación normal

El transitorio de pérdida de agua de alimentación se caracteriza por la pérdida del aporte principal del agua de alimentación del secundario, manteniéndose en operativo el sistema de aporte de agua de alimentación auxiliar.

A continuación se describen los sucesos observados en la simulación, Tabla 3.13:

- 120 s: se produce el disparo de las bombas de agua de alimentación principal, Figura 3.71. Al no entrar agua en los generadores de vapor se produce un rápido descenso del nivel de estos, Figura 3.72, y un aumento de la presión en el secundario, Figura 3.75. Este comportamiento provoca la degradación de la transferencia de calor entre el primario y el secundario incrementando la temperatura del primario, produciendo la disminución de la densidad del refrigerante del núcleo, un aumento del nivel en el presionador, Figura 3.70, el consiguiente aumento en la presión del primario y una disminución del caudal circulante por el primario, Figura 3.66.

- 128,20 s: apertura de la ducha del presionador, debido al aumento de la presión del primario, Figura 3.68.

- 145,40 s: apertura de las válvulas de alivio del presionador, Figura 3.69, debido a que la ducha no ha conseguido reducir la presión en el primario y se alcanza el tarado de las válvulas de alivio del presionador, Figura 3.64. Con esta apertura y con la regulación de los caudales de carga y descarga del CVCS, Figura 3.67, se consigue reducir la presión en el primario y se provoca una disminución lenta y progresiva del nivel del presionador, Figura 3.70.

- 149,60 s: disparo del reactor por bajo nivel en los generadores de vapor, Figura 3.72, debido a que alguno de los generadores de vapor tiene menos del 17.6 % del nivel de rango estrecho. El disparo del reactor lleva a la caída de la potencia, Figura 3.63, causando la disminución de la temperatura del primario. Esta disminución de la temperatura provoca el aumento de la densidad del refrigerante, y como consecuencia el descenso del nivel y de la presión del presionador, Figura 3.70.

- 149,80 s: actuación del agua de alimentación auxiliar por bajo nivel en los generadores de vapor, Figura 3.71, con lo que se reduce la perdida de inventario de agua y a largo plazo se recupera el nivel de los generadores de vapor, Figura 3.72.

- 150,00 s: Disparo de la turbina por disparo del reactor, Figura 3.62, y como consecuencia se abre el alivio al condensador, Figura 3.78.

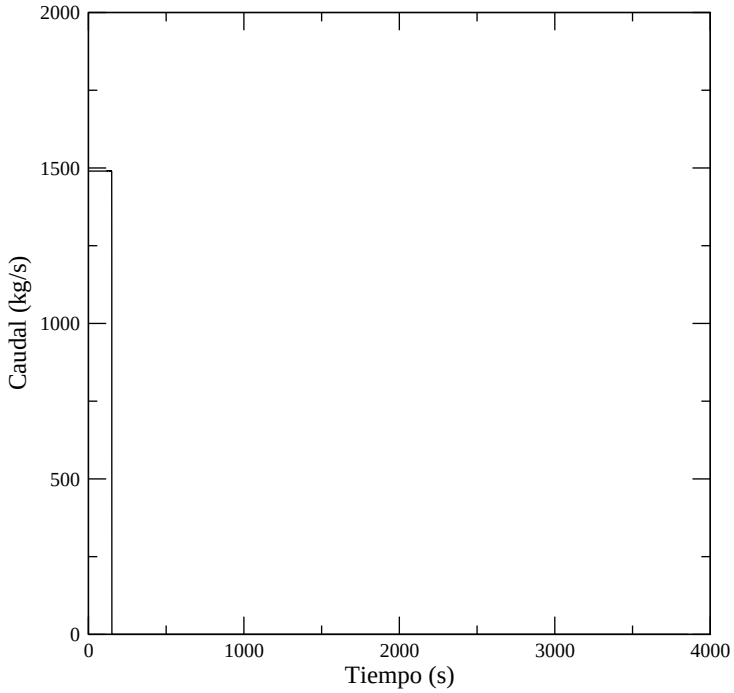
- 154,80 s: apertura de las válvulas de alivio de los generadores de vapor por alta presión en los generadores de vapor, Figura 3.76. El alivio al condensador no tiene suficiente capacidad para reducir la presión en el secundario en el poco tiempo que lleva actuando (4.80 s), y debido al progresivo aumento de la presión en el secundario por la falta de

aporte de agua de alimentación se alcanza el tarado de apertura de las válvulas de alivio. Como resultado de su apertura y el alivio al condensador, se reduce la presión en el secundario, Figura 3.75.

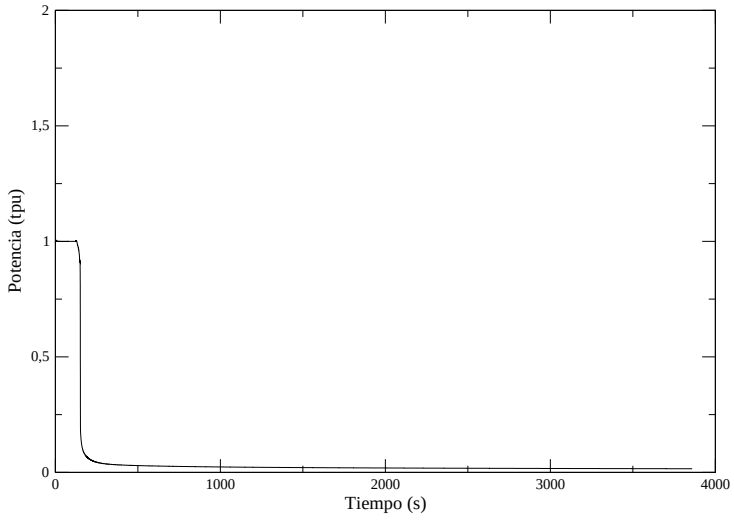
- 1643,20 s: apertura de las válvulas de alivio del presionador, Figura 3.69, por alta presión en el primario, debido a que los calentadores proporcionales y de apoyo están actuando para recuperar la presión del primario, Figura 3.79. La actuación continuada de los calentadores provoca una sobrepresurización del primario, Figura 3.64, ya que estos calentadores están controlados por un PI, que al haber estado integrando un error negativo significativo durante unos 1000 segundos, implica la demanda de los calentadores hasta que la integración del error positivo compensa el efecto integral negativo.
- 3818,40 s: aislamiento de la descarga del CVCS por bajo nivel en el presionador, Figura 3.67, con lo que el nivel del presionador se recupera, Figura 3.70.
- Final: en la finalización de la simulación se tienen los siguientes resultados:
  - La presión en el circuito primario es de $13{,}5 \cdot 10^6$ Pascales y tiende a estabilizarse.
  - La presión en el circuito secundario se estabiliza en $7{,}7 \cdot 10^6$ Pascales.
  - La temperatura media del primario se estabiliza en 293 ^{o}C.

Actuaciones automáticas	**Tiempo (s)**
Perdida del agua de alimentación normal	120
Apertura de la ducha del presionador por alta presión en el presionador	128,20
Apertura de las válvulas de seguridad y alivio del presionador por alta presión en el presionador	145,40
Disparo del reactor por bajo nivel en los generadores de vapor (<17.6 %)	149,60
Actuación del agua de alimentación auxiliar por bajo nivel en los generadores de vapor (<17.6 %)	149,80
Disparo de turbina por disparo del reactor Apertura del alivio al condensador por alta presión en los generadores de vapor	150,00
Apertura de las válvulas de seguridad y alivio de los generadores de vapor por alta presión en los generadores de vapor	154,80
Apertura de las válvulas de seguridad y alivio del presionador por alta presión en el presionador	1643,20
Aislamiento de la descarga del CVCS por bajo nivel en el presionador (<15 %)	3818,40

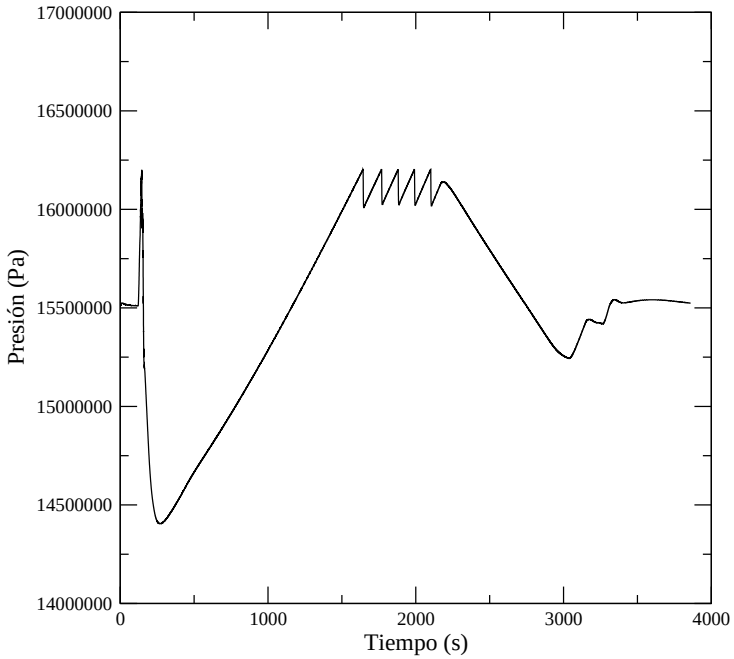
Tabla 3.13: Actuaciones automáticas que actúan en el transitorio de perdida de agua de alimentación normal.



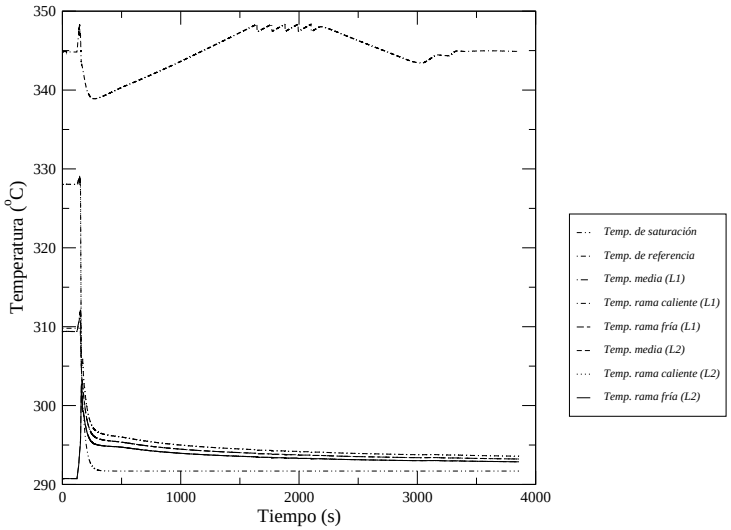
Gráfica 3.62: Pérdida del agua de alimentación normal. Caudal de vapor en la turbina.



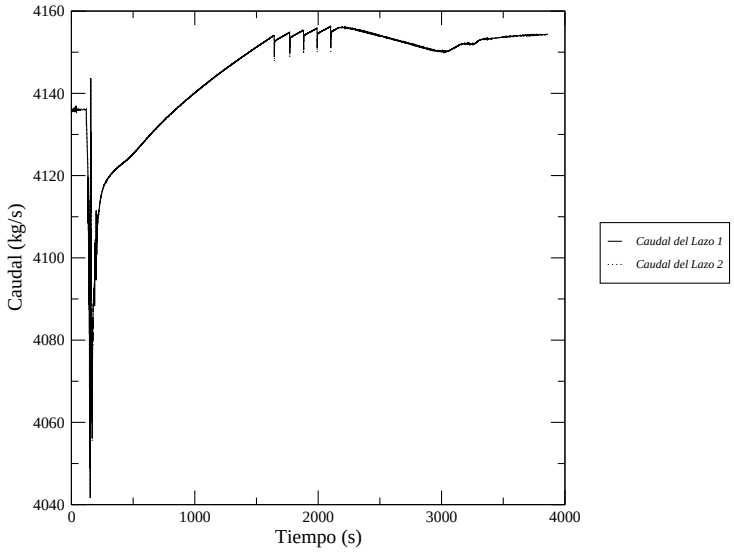
Gráfica 3.63: Pérdida del agua de alimentación normal. Potencia del reactor.



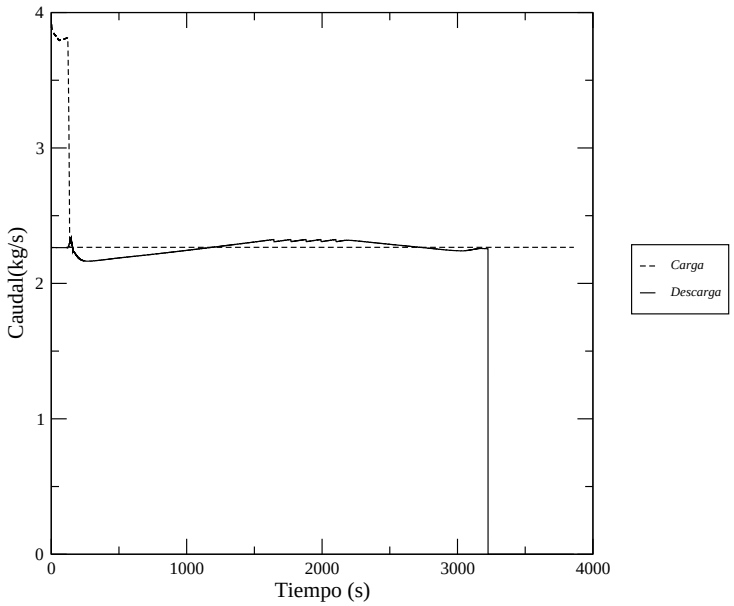
Gráfica 3.64: Pérdida del agua de alimentación normal. Presión del RCS.



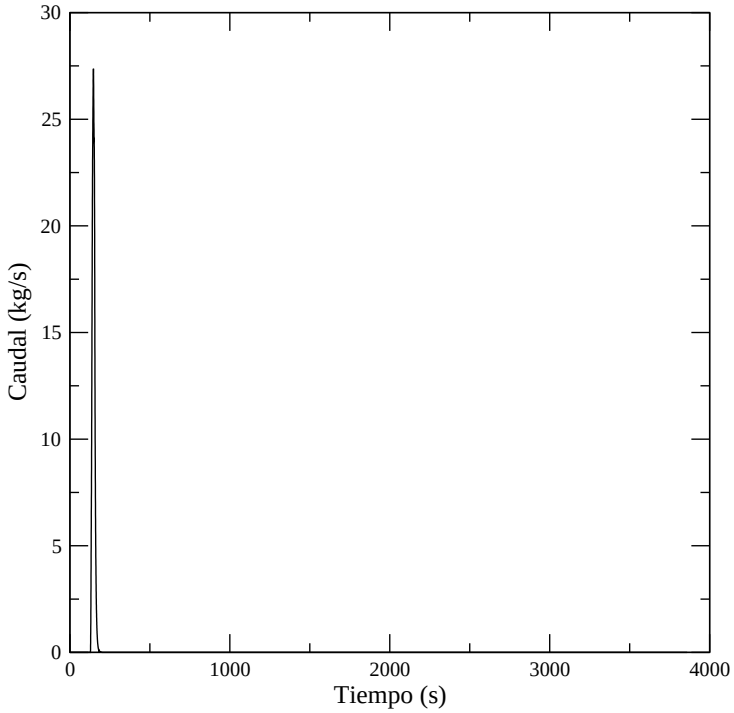
Gráfica 3.65: Pérdida del agua de alimentación normal. Temperaturas del RCS.



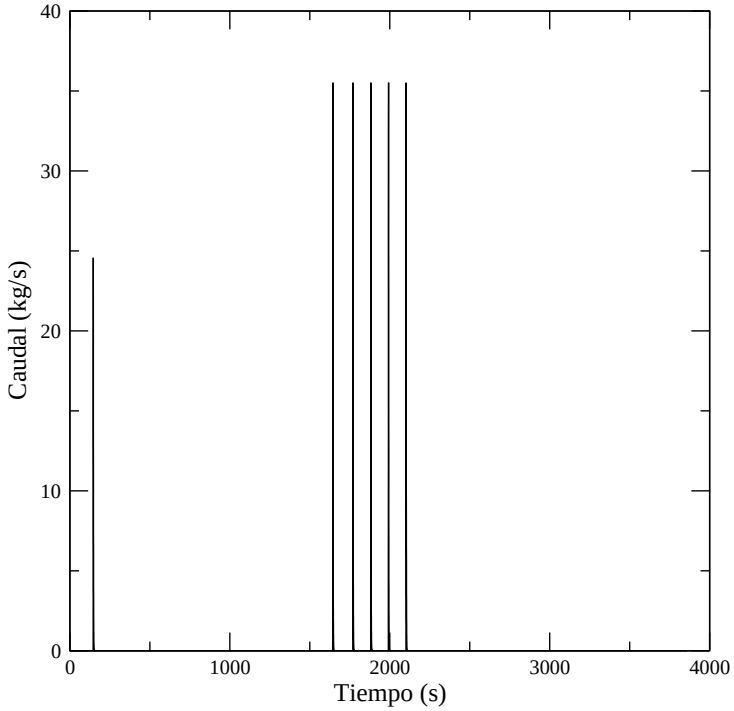
Gráfica 3.66: Pérdida del agua de alimentación normal. Caudales de los lazos del primario.



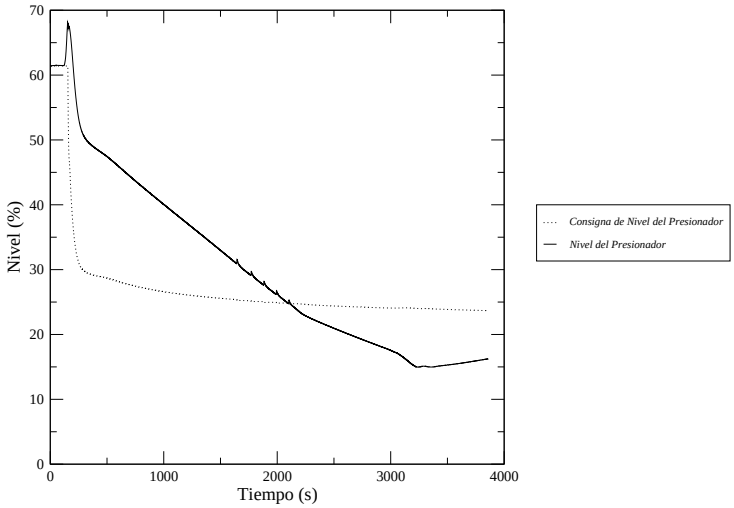
Gráfica 3.67: Pérdida del agua de alimentación normal. Caudales de la carga y la descarga del CVCS.



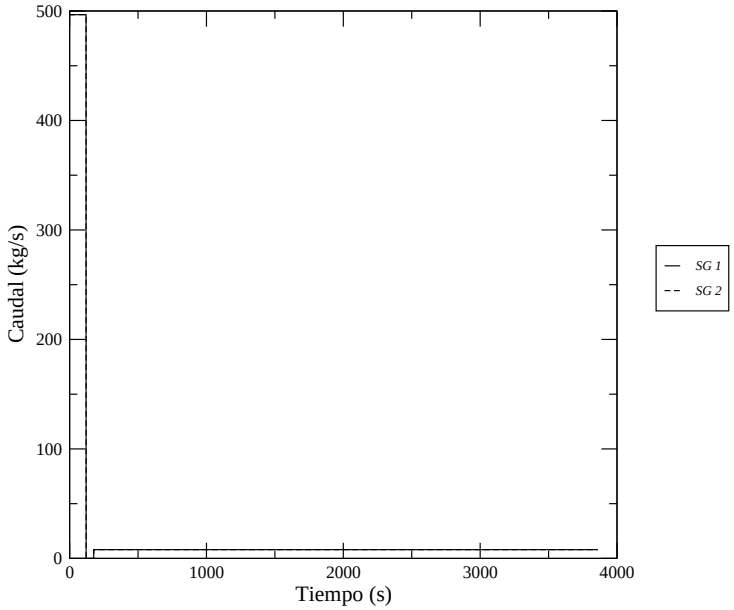
Gráfica 3.68: Pérdida del agua de alimentación normal. Caudal de la ducha del PZR.



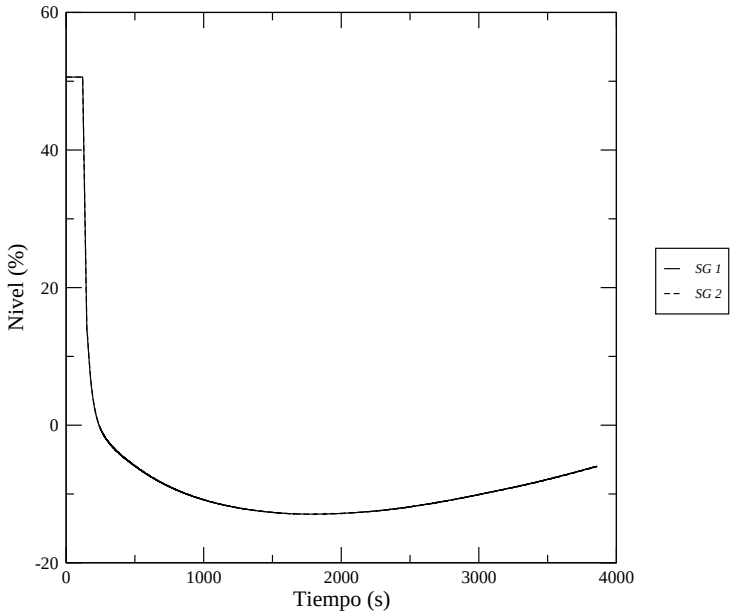
Gráfica 3.69: Pérdida del agua de alimentación normal. Caudal de las válvulas de alivio y seguridad del PZR.



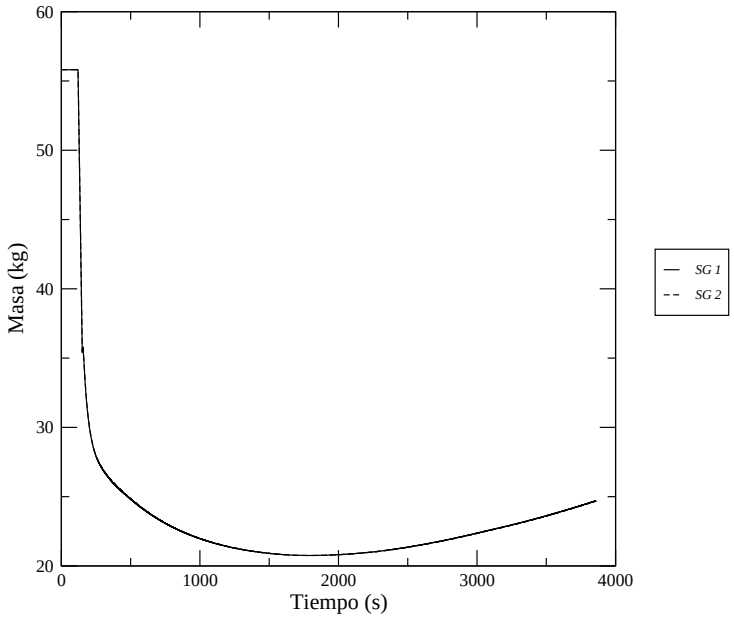
Gráfica 3.70: Pérdida del agua de alimentación normal. Nivel del PZR y consigna del nivel del PZR.



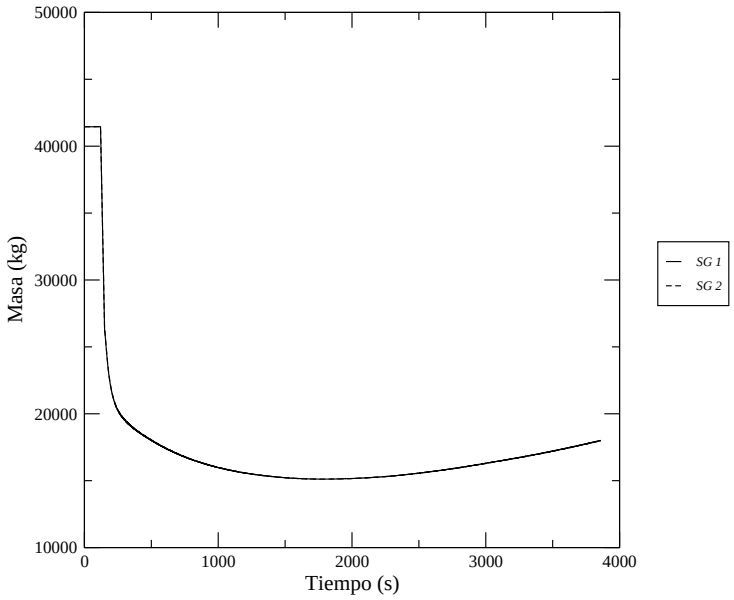
Gráfica 3.71: Pérdida del agua de alimentación normal. Caudales del agua de alimentación de los generadores de vapor.



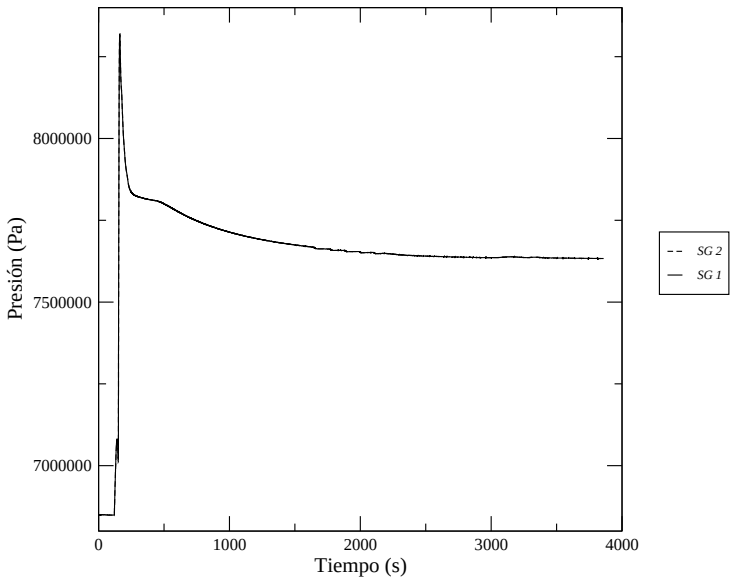
Gráfica 3.72: Pérdida del agua de alimentación normal. Niveles de rango estrecho de los generadores de vapor.



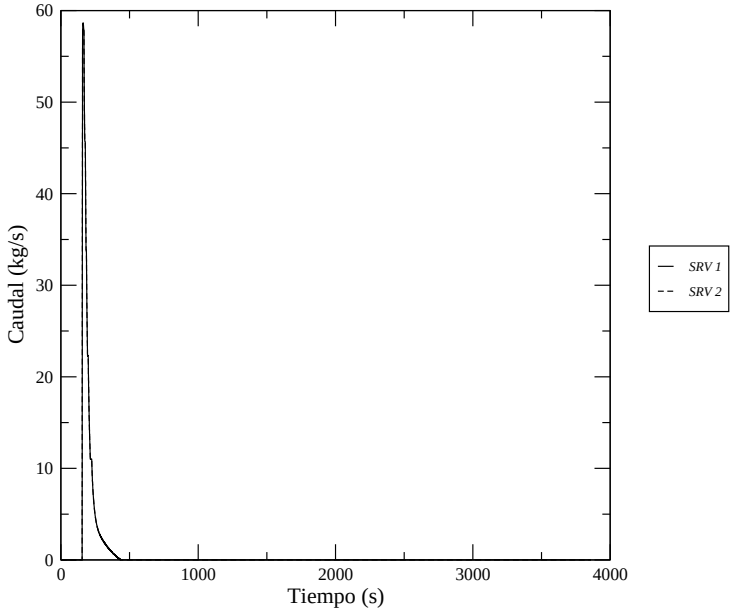
Gráfica 3.73: Pérdida del agua de alimentación normal. Niveles de rango ancho de los generadores de vapor.



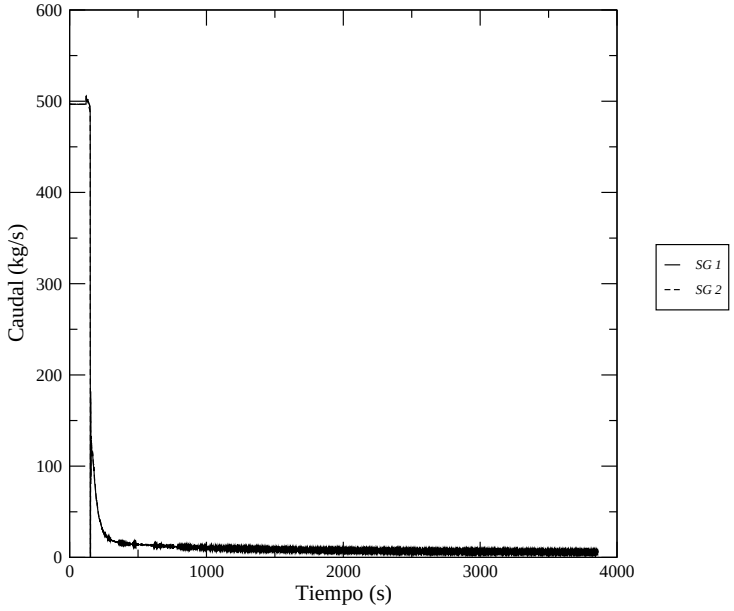
Gráfica 3.74: Pérdida del agua de alimentación normal. Inventario de los generadores de vapor.



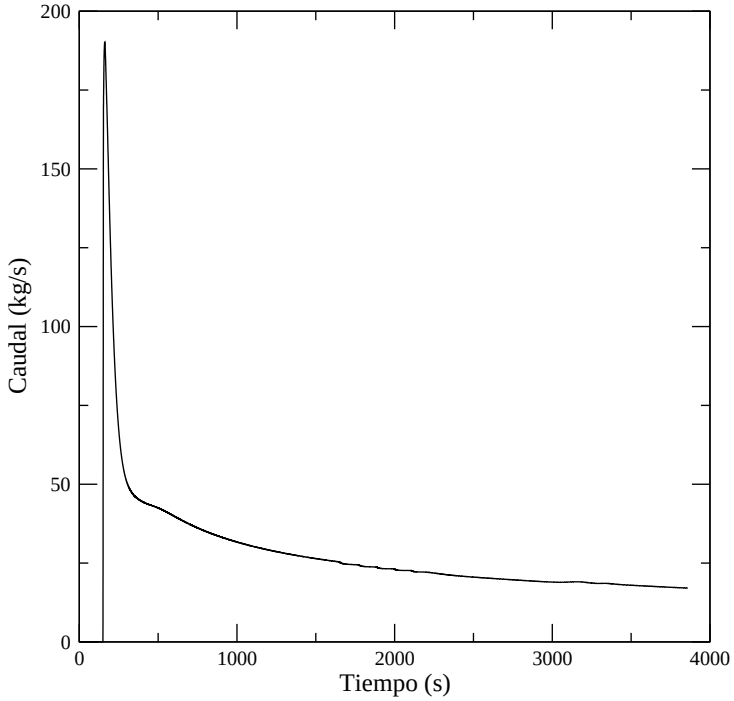
Gráfica 3.75: Pérdida del agua de alimentación normal. Presión en los generadores de vapor.



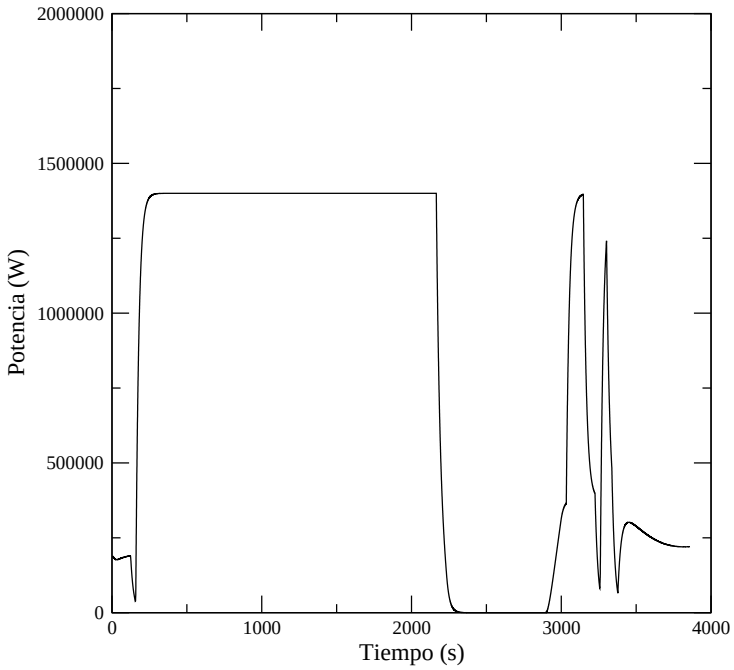
Gráfica 3.76: Pérdida del agua de alimentación normal. Caudal de las válvulas de alivio y seguridad de los generadores de vapor.



Gráfica 3.77: Pérdida del agua de alimentación normal. Caudales de vapor de los generadores de vapor.



Gráfica 3.78: Pérdida del agua de alimentación normal. Caudal de alivio al condensador.



Gráfica 3.79: Pérdida del agua de alimentación normal. Potencia de los calentadores.

3.3.6 Resultados de la simulación de la rotura aislable en el colector

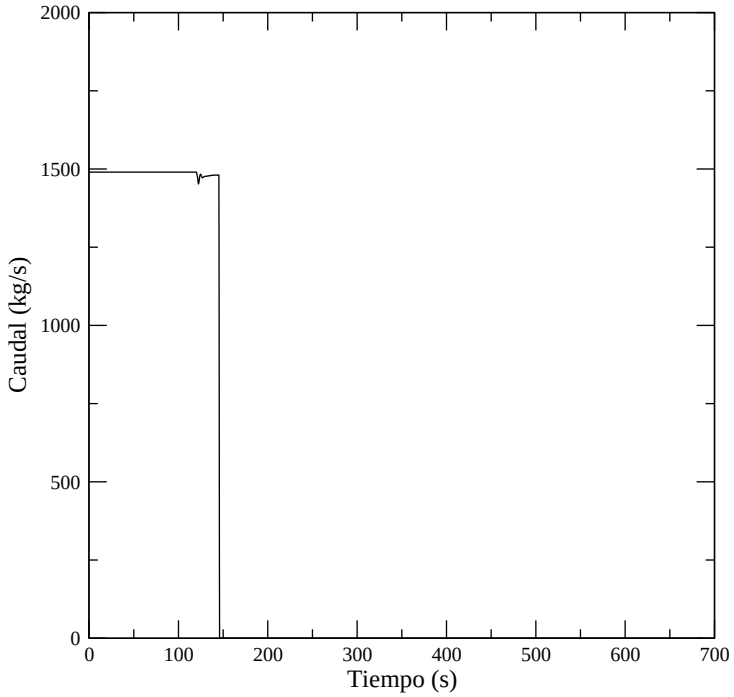
En el transitorio de rotura aislable en el colector se simula una rotura de tamaño medio en el colector siendo aislada, sin ninguna acción del operador.

A continuación se describen los sucesos observados en la simulación, Tabla 3.14:

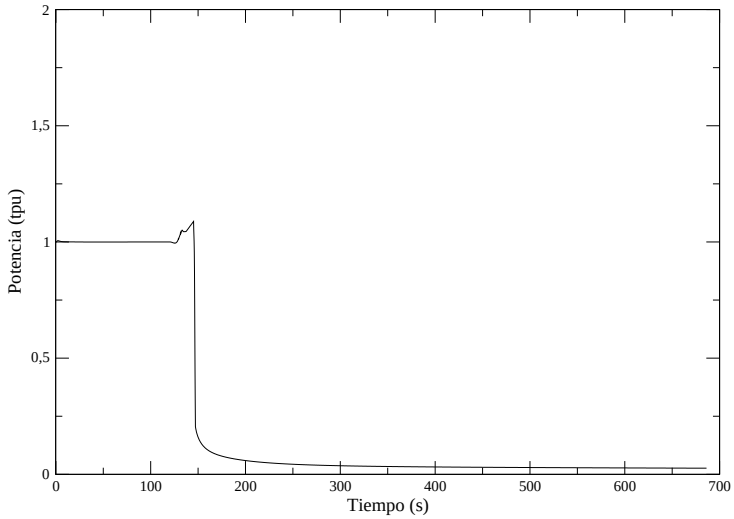
- 120 s: rotura aislable en el colector, con lo que cae la presión en el secundario, Figura 3.92, esto produce un rápido enfriamiento del secundario, con lo que aumenta la transferencia de calor del primario al secundario y un rápido enfriamiento del primario, Figura 3.84. Este enfriamiento provoca una realimentación positiva que genera el rápido aumento de potencia, Figura 3.81, además debido a la despresurización del secundario debido a la rotura el caudal de vapor de los generadores de vapor aumenta, Figura 3.94.
- 145,20 s: disparo del reactor por alto flujo neutrónico, Figura 3.81.
- 145,40 s: disparo de la turbina por disparo del reactor, Figura 3.80, y apertura del alivio al condensador por disparo de la turbina, Figura 3.95.
- 147,60 s: disparo de las bombas de agua de alimentación por disparo de la turbina, Figura 3.90, y actuación del agua de alimentación auxiliar por disparo de las bombas de agua de alimentación, esta reducción del aporte de agua de alimentación produce a corto plazo una fuerte bajada del nivel de rango estrecho en los generadores de vapor, Figura 3.91, y una subida de la presión en los generadores de vapor mientras no entra el agua de alimentación auxiliar en los generadores de vapor, Figura 3.92.
- 257,20 s: aislamiento de las líneas de vapor, Figuras 3.94, por baja presión en los generadores de vapor, esto provoca el aumento de la presión y niveles de los generadores de vapor, Figuras 3.92 y 3.91.
- 257,40 s: actuación de la inyección de seguridad, Figuras 3.96, por muy baja presión en el presionador, Figuras 3.83, debido al fuerte enfriamiento del primario, Figuras 3.84,esto lleva al aumento del nivel del presionador hasta el llenado del presionador, Figuras 3.89, también se aísla la carga y descarga del CVCS debido a la inyección de seguridad.
- 355,60 s: apertura de la ducha del presionador, Figuras 3.87, por demanda del control de presión.
- 625,60 a 683,80 s: ciclado de las válvulas de alivio del presionador, Figuras 3.88, por alta presión en el presionador.
- Final: en la finalización de la simulación se tienen los siguientes resultados:
  - La presión en el circuito primario se estabiliza en $16{,}9 \cdot 10^6$ Pascales.
  - La presión en el circuito secundario se recupera progresivamente hasta alcanzar los $5{,}5 \cdot 10^6$ Pascales.
  - La temperatura media del primario se recupera progresivamente hasta alcanzar 273 ^{o}C.

Actuaciones automáticas	**Tiempo (s)**
Rotura aislable en el colector	120
Disparo del reactor por alto flujo neutrónico	145,20
Disparo de turbina por disparo del reactor Apertura del alivio al condensador por disparo de la turbina	145,40
Disparo de las bombas de agua de alimentación por disparo de la turbina Actuación del agua de alimentación auxiliar por Disparo de las bombas de agua de alimentación	147,60
Aislamiento de las líneas de vapor por baja presión en los generadores de vapor	257,20
Inyección de seguridad por muy baja presión en el presionador Aislamiento de la carga y descarga del CVCS por la inyección de seguridad	257,40
Apertura de la ducha del presionador	355,60
Apertura de las válvulas de seguridad y alivio del presionador por alta presión en el presionador	625,80 637,80 653,80 683,80

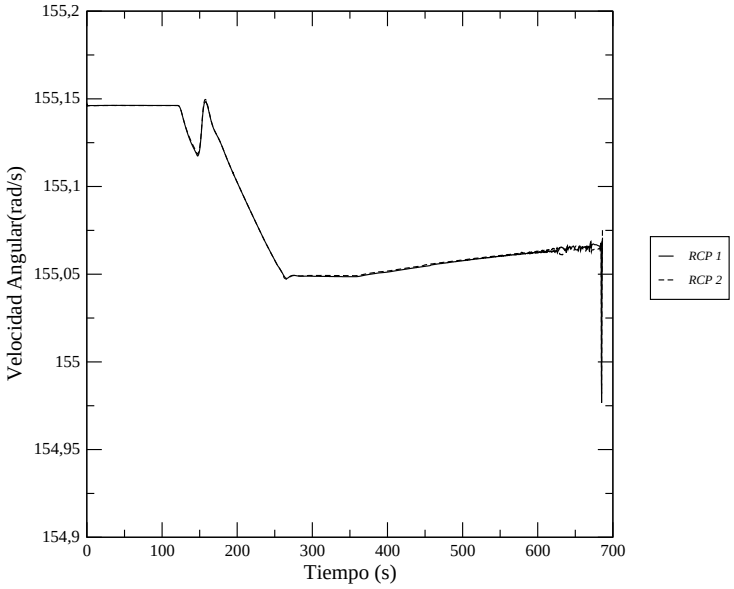
Tabla 3.14: Actuaciones automáticas que actúan en el transitorio de Rotura aislable en el colector con actuaciones automáticas.



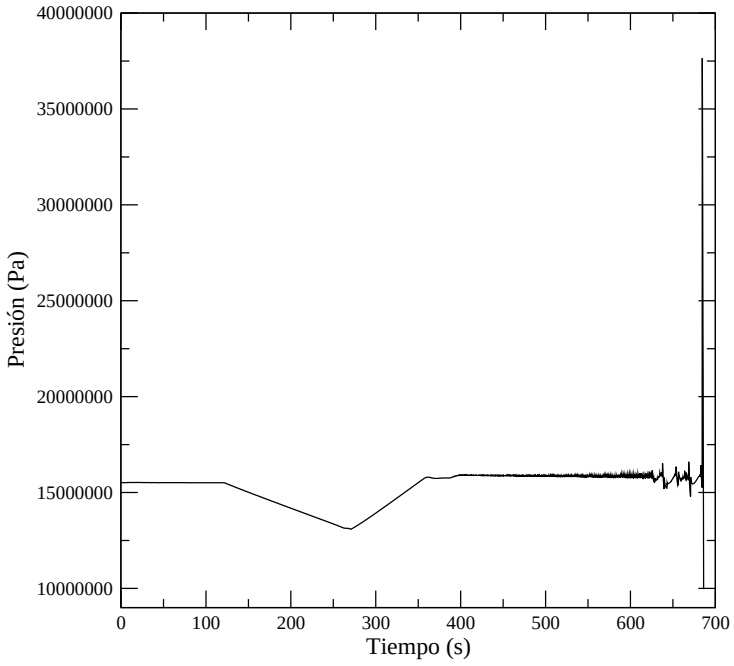
Gráfica 3.80: Rotura aislable en el colector. Caudal de vapor en la turbina.



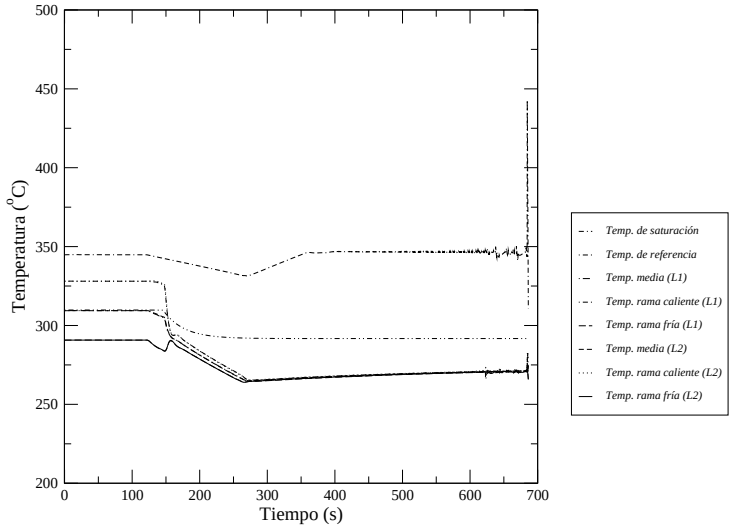
Gráfica 3.81: Rotura aislable en el colector. Potencia del reactor.



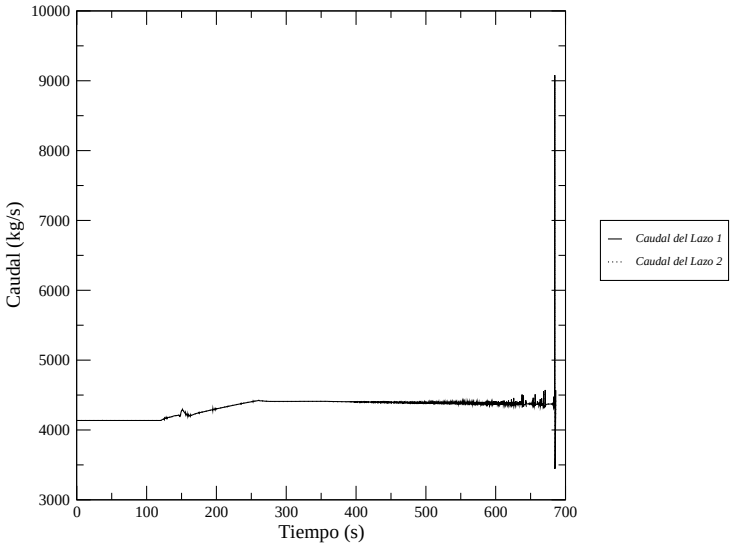
Gráfica 3.82: Rotura aislable en el colector. Velocidad de las RCP.



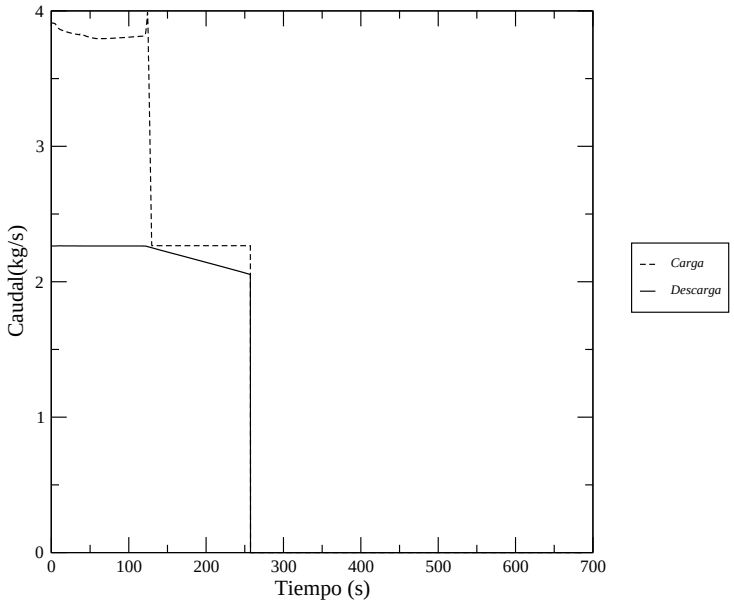
Gráfica 3.83: Rotura aislable en el colector. Presión del RCS.



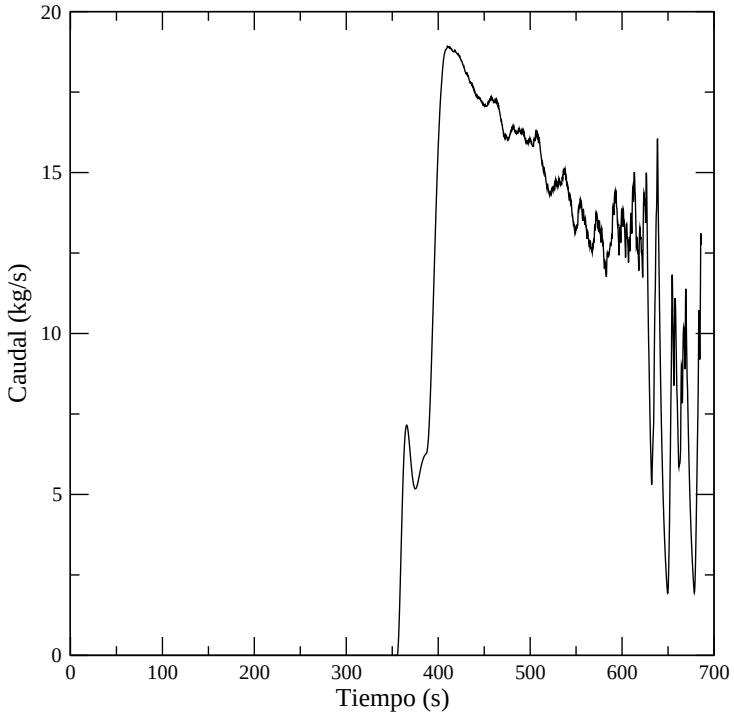
Gráfica 3.84: Rotura aislable en el colector. Temperaturas del RCS.



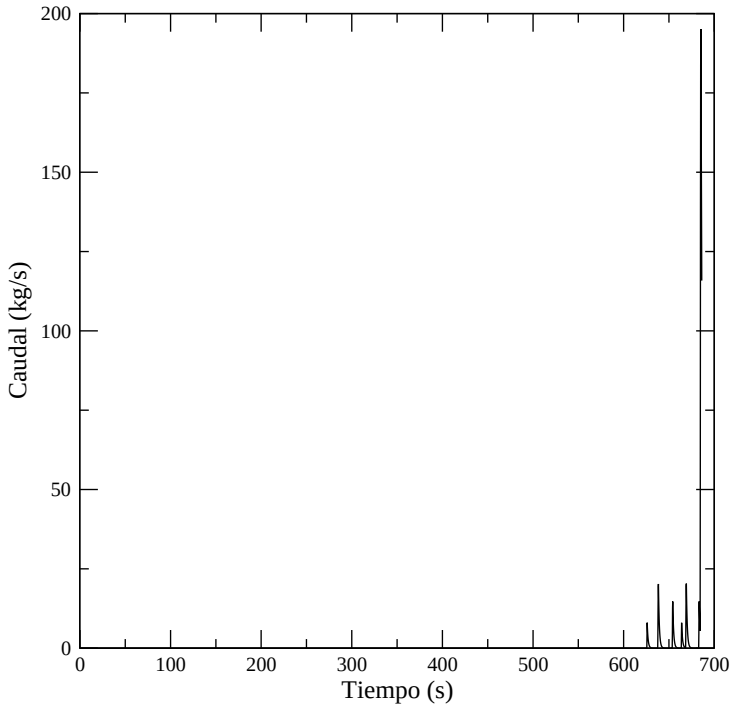
Gráfica 3.85: Rotura aislable en el colector. Caudales de los lazos del primario.



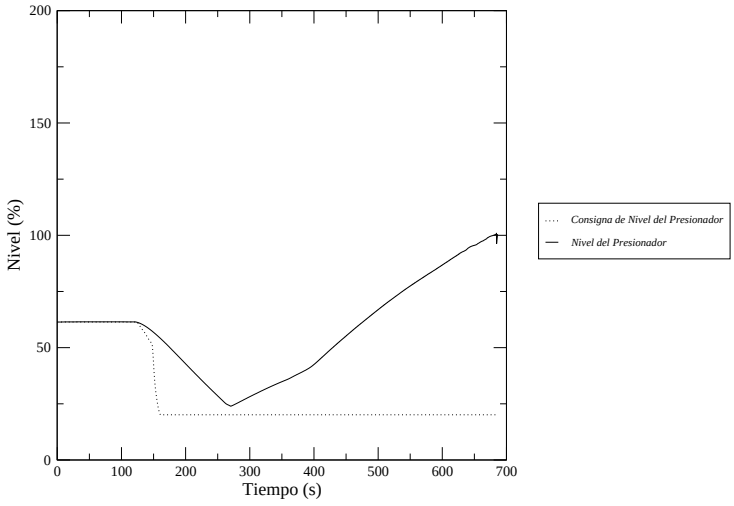
Gráfica 3.86: Rotura aislable en el colector. Caudales de la carga y la descarga del CVCS.



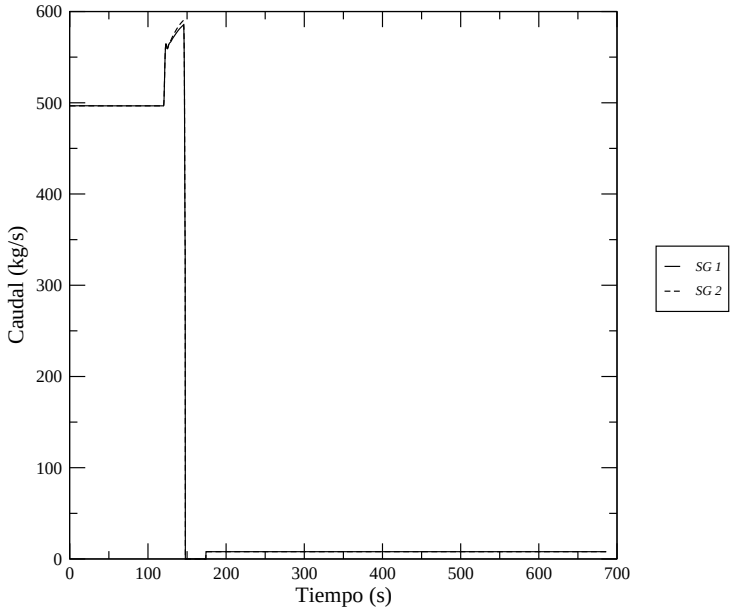
Gráfica 3.87: Rotura aislable en el colector. Caudal de la ducha del PZR.



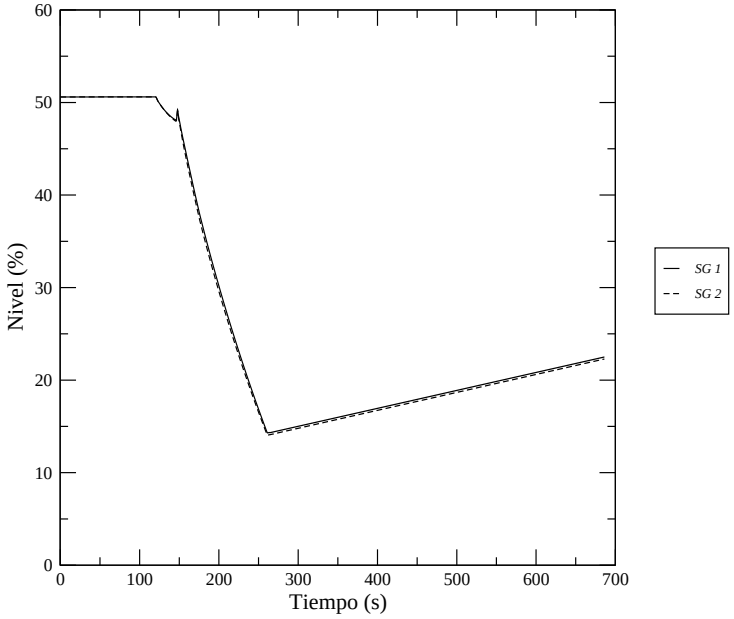
Gráfica 3.88: Rotura aislable en el colector. Caudal de las válvulas de alivio y seguridad del PZR.



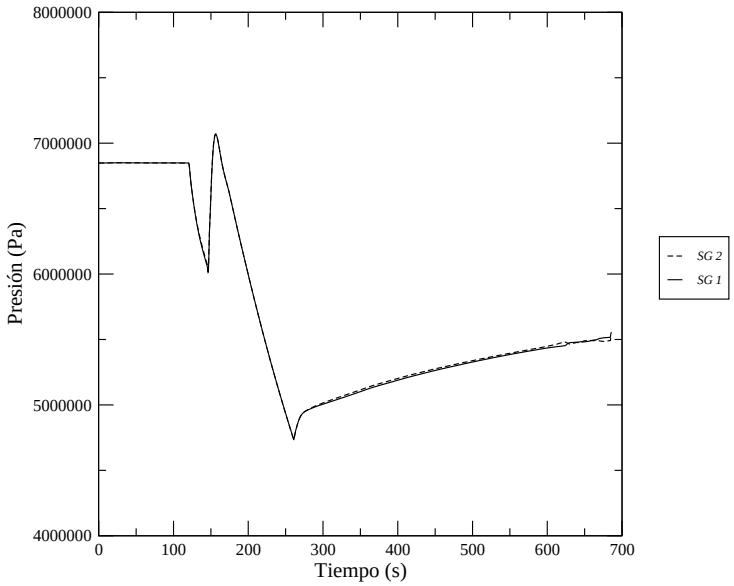
Gráfica 3.89: Rotura aislable en el colector. Nivel del PZR y consigna del nivel del PZR.



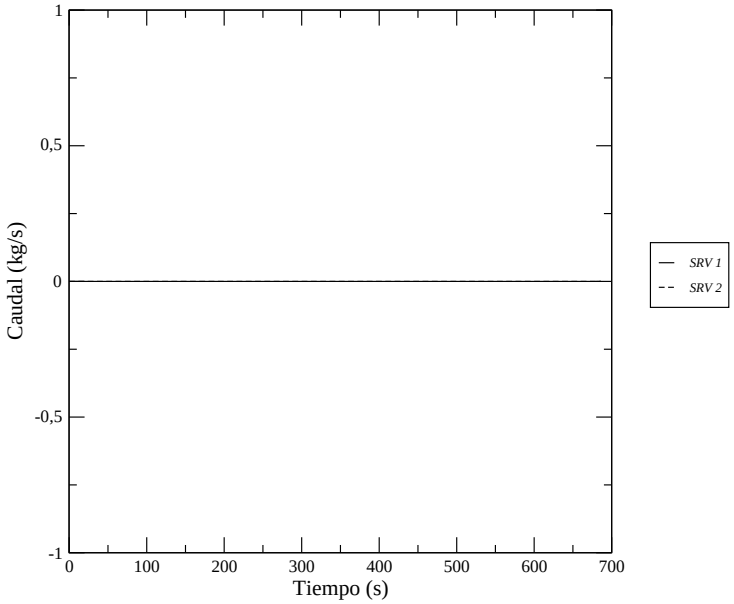
Gráfica 3.90: Rotura aislable en el colector. Caudales del agua de alimentación de los generadores de vapor.



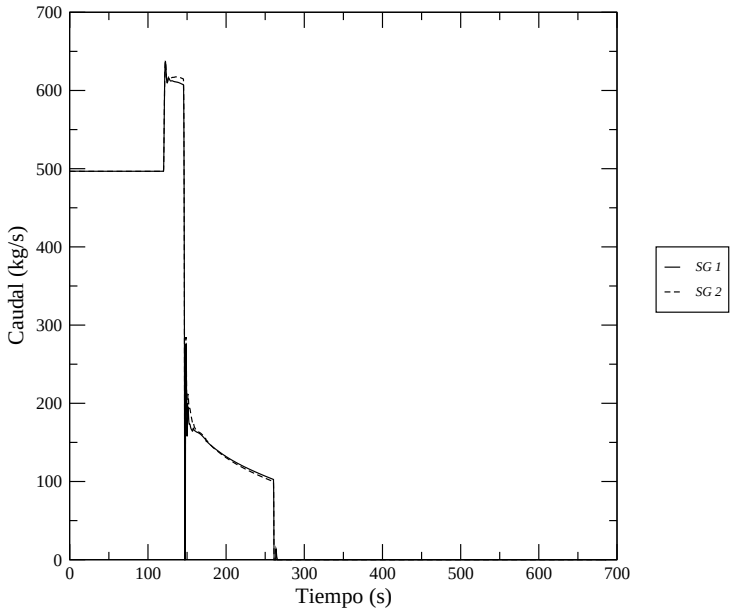
Gráfica 3.91: Rotura aislable en el colector. Niveles de los generadores de vapor.



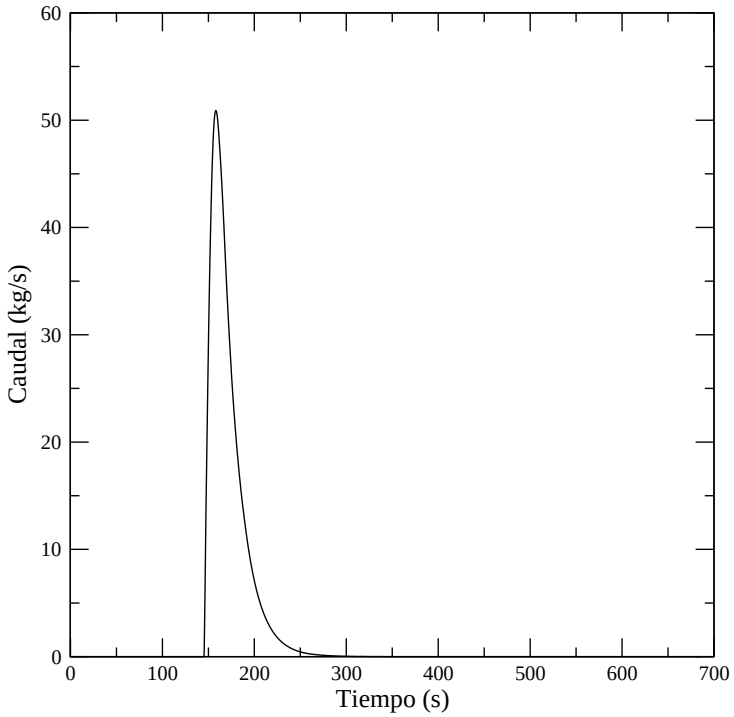
Gráfica 3.92: Rotura aislable en el colector. Presión en los generadores de vapor.



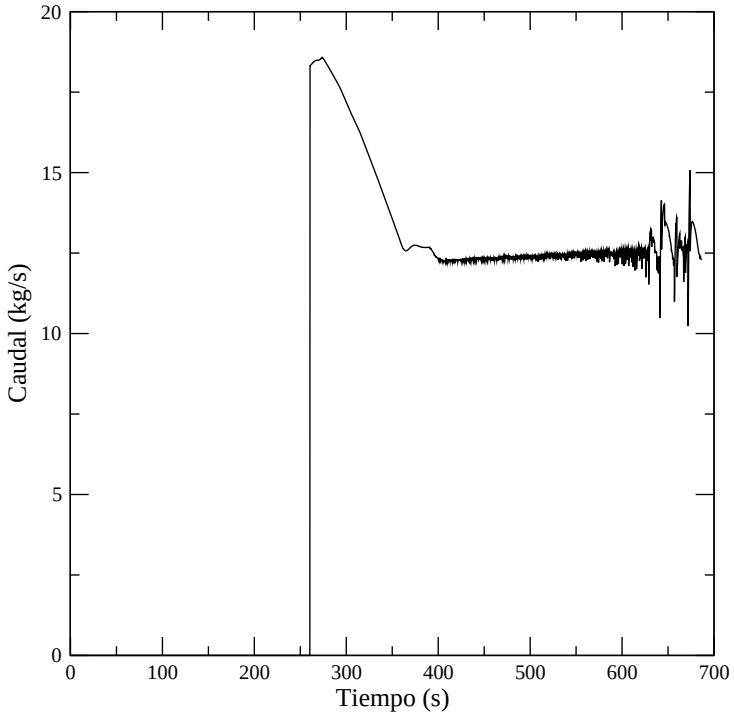
Gráfica 3.93: Rotura aislable en el colector. Caudal de las válvulas de alivio y seguridad de los generadores de vapor.



Gráfica 3.94: Rotura aislable en el colector. Caudales de vapor de los generadores de vapor.



Gráfica 3.95: Rotura aislable en el colector. Caudal de alivio al condensador.



Gráfica 3.96: Rotura aislable en el colector. Caudal de la inyección de seguridad.

3.4 Conclusiones relativas al modelo de planta PWR-W

Durante la realización del trabajo se superaron diversas limitaciones del simulador TRETA realizando mejoras en el código, destacando:

- Un modelo lineal de secado de tubos en el módulo de cálculo del coeficiente de transferencia de calor de los generadores de vapor (UASG).
- Ajustes del módulo del cálculo del presionador relacionados con el llenado y vaciado del mismo (PRES).

Sin embargo, otras de las limitaciones encontradas en el código no fueron subsanadas por no ser prioridad del trabajo planteado. Estas han sido:

- La necesidad de incluir modelos bifásicos en los módulos encargados de calcular el transporte de las propiedades termohidráulicas del fluido (módulos PIPEI, PIDED y PIPEM). Esta limitación es de espacial importancia en transitorios con condiciones degradadas de refrigeración o los relacionados con despresurizaciones rápidas, p. ej. TLOFW o LOCA. Para paliar estas deficiencias se podría considerar la implementación de los modelos del simulador TIZONA.
- Se debe mejorar el modelo de bombas del primario, que en su estado actual impide simular secuencias en las que las que se produzca la pérdida de circulación natural.
- Tanto la arquitectura de cálculo de los elementos del modelo de un sistema, como de forma individual, los módulos PIPEI, PIPED y PIPEM, no permiten el cálculo de caudales inversos. Por ello se requiere mejorar estos módulos para que consideren esta posibilidad y considerar una solución a nivel de modelo que permita el paso de información de bloques en orden inverso a la secuencia natural de cálculo del código TRETA.
- La fuerte modularidad del código, el carácter desacoplado de los modelos y su implementación a nivel de cálculo requieren la implementación de técnicas numéricas de convergencia mediante realimentaciones. En el desarrollo del simulador TRETA se consideraron técnicas numéricas de convergencia unidimensionales, lo que aporta problemas numéricos en las simulaciones. En este sentido se tendría que considerar la posibilidad de mejorar estas técnicas dotándolas de carácter vectorial, empleando los métodos SIMPLEX y derivados o técnicas de optimización de gradiente conjugado. Además, deben mejorarse los criterios de relajación y los criterios de aplicación.
- Se debería incorporar la capacidad de variar el paso de tiempo en el *driver*, ajustándolo a las necesidades de simulación. En su defecto se debería implementar esta capacidad en el módulo encargado del cálculo del presionador, PRES.
- Posibilidad de realizar guardar puntos de la simulación por petición del usuario, mediante la información del mismo en el fichero de entrada.

En cuanto al modelo de planta desarrollado, se puede considerar:

- El ajuste de los parámetros de los controles manuales para una simulación más realista de los tiempos y el modo de control humano.
- La mejora y la validación más extensiva de los modelos de sistemas frontales, especialmente el SIS y el CVCS, y de válvulas tanto del primario como del secundario, así como el ajuste de los caudales del modelo de alivio de vapor al condensador.
- El desarrollo de un modelo de balance de planta.

Capítulo 4

Modelo de procedimientos de operación de emergencia de un PWR-W para el código COPMA-III

Índice

Las actividades llevadas a cabo para desarrollar la metodología en lo referente al modelado de procedimientos, de forma consistente con las especificaciones relativas a este aspecto que se exponen la Sección 1.3, han sido:

- Un estudio detallado de la base conceptual, de la estructura global y de los diferentes elementos que integran los EOP en las centrales PWR-W, Sección 4.1.
- La evaluación y el desarrollo de las herramientas necesarias para realizar la computerización de los EOP, Sección 4.2.
- El establecimiento de una metodología que permita la computerización de los EOP de forma sistemática, garantizando que dichas versiones computerizadas conservan la funcionalidad de los procedimientos originales y que cubren las especificaciones fijadas, Sección 4.3.
- La realización de dos aproximaciones al modelado de los EOP, Sección 4.4:
  - Un modelo de un procedimiento de operación de emergencia con alto nivel de detalle, garantizando un paralelismo tanto estructural como funcional. El objetivo era verificar que las capacidades de computerización y simulación de las herramientas empleadas eran adecuadas.
  - Un modelo de un conjunto de EOP con nivel de detalle bajo, considerando solo aquellas actuaciones de interés desde el punto de su interacción con los procesos físicos más relevantes que se dan en una central PWR-W durante los transitorios. El objetivo era obtener la funcionalidad de integración de ambos códigos de simulación, los modelos de planta y procedimientos, y su implementación.
- Finalmente, se realizó la evaluación de los problemas surgidos durante las tareas relacionadas con el desarrollo del modelo computerizado de los EOP, Sección 4.5.

En las siguientes secciones se amplían las diferentes tareas que se han enumerado.

4.1 Descripción de los procedimientos de operación de una central PWR-W

Según el estado de operación en el que se encuentre la central, Westinghouse (1994), el patrón de respuesta y funciones del operador varía, obteniendo, Figura 4.1:

- En estado de **operación normal**, la función del operador es cambiar el estado de la central de forma controlada para generar potencia eléctrica de la forma más eficiente posible. Los límites normales de operación están bien definidos en las especificaciones técnicas de funcionamiento (*Performance Technical Specification*, PTS), y los sistemas de control

de la central mantienen los parámetros de la misma dentro de los límites operacionales normales. Además, los sistemas de protección y salvaguardias están disponibles en caso de que dichos parámetros excedan los límites normales de operación.

- En el estado de **operación anormal**, la función del operador es investigar las condiciones de alarma originadas cuando los parámetros exceden los límites en operación normal. Dependiendo de la causa de la anomalía, de los sistemas de producción de potencia o en los sistemas auxiliares de la central, es posible un amplio espectro de respuestas de los sistemas de la central. El operador debe diagnosticar la condición de la central y realizar las acciones de recuperación para evitar que los parámetros excedan los límites operacionales de protección del reactor, con el objetivo de llevar estos parámetros a sus límites normales de operación. Los sistemas de protección y salvaguardias están disponibles en caso de que los parámetros excedan los límites operacionales de protección del reactor.

- En el estado de **operación de emergencia**, los parámetros han excedido los límites operacionales de protección del reactor. El estado de la central ha pasado de estar controlado por el operador a ser gobernado por los sistemas de control. Por ello, la función del operador se fundamenta en asistir las acciones automáticas. El estado operacional de emergencia incluye dos niveles de respuesta del operador: respuesta al disparo del reactor y respuesta a la inyección de seguridad.

  La respuesta del operador al disparo del reactor aumenta la eficacia de los sistemas de protección de la central, y consiste en estabilizar las condiciones de la misma y, dependiendo de la causa del disparo del reactor, iniciar la operación de recuperación. Los sistemas de salvaguardias tecnológicas están disponibles en caso de que los parámetros excedan los límites de operación de las salvaguardias.

  La respuesta del operador a una condición de inyección de seguridad (SI) aumenta la seguridad y la eficacia de los sistemas de salvaguardias y consiste en diagnosticar las condiciones de la central e iniciar las acciones de recuperación, a la vez que asegura que la seguridad de la central se mantiene de forma continua. Dependiendo de la condición de SI, la respuesta puede incluir la realineación o la parada de los sistemas de salvaguardias. En el nivel de respuesta de SI, el operador es el responsable último de la seguridad de la central ya que no dispone de sistema automáticos adicionales.

Los tres estados operacionales llevan asociados distintos niveles de respuesta del operador. Estos niveles de respuesta así como los puntos de decisión que los separan se pueden distinguirse en el esquema de la Figura 4.1. Las acciones del operador en cada nivel están dirigidas por procedimientos de operación confeccionados para cada estado operacional. Dichos procedimientos forman una red que guía las acciones del operador en cada estado operacional de la central.

Las condiciones de transición o síntomas entre los diferentes estados de operación deben ser establecidos en el diseño de los procedimientos. La frontera entre el estado normal y el de emergencia y los síntomas empleados para vigilar la condición de transición están definidos en las condiciones de entrada a los EOP. Normalmente, se emplean la actuación automática del disparo del reactor o la actuación de un sistema de salvaguardia, prestando atención a la

vigilancia de transitorios sin inserción de las barras de control (*Anticipated Transient Without Scram*, ATWS). Se permite la salida de los EOP cuando la planta ha alcanzado una condición estable y segura y el daño se haya prevenido con un margen elevado de seguridad. En el caso de que la gestión preventiva del accidente no tenga éxito, se debe considerar la transición a la toma de medidas relacionadas con la gestión de accidentes severos. Esta transición se basa en síntomas indicativos de la existencia de daño al núcleo o el hecho de que el daño al núcleo es inminente. Los parámetros de planta relacionados con estos síntomas suelen ser la temperatura a la salida del núcleo para los PWR, o el fallo en el mantenimiento de un nivel mínimo en la RPV, para el caso de los BWR. La transición al estado de operación de accidente severo puede ser irreversible o realizarse su ejecución en paralelo al seguimiento de los EOP. En este último caso, se debe verificar la compatibilidad de ambos estados de operación, y en caso de detectarse alguna incompatibilidad, se deben abandonar los EOP. La finalización y salida de las SAMG se basa en parámetros observables que indiquen que se han alcanzado condiciones seguras y estables.

Aunque el objetivo de este trabajo se centra en la integración de los EOP en la simulación de secuencias accidentales, se considera de interés aclarar que existen fuertes diferencias estructurales entre los procedimientos relacionados con los estados de operación anormal o emergencia y los propios del estado de operación de accidente severo. Mientras que la estructura de los AOP y de los EOP, en forma de secuencias prescriptivas de actuaciones, es adecuada para esos estados operacionales, es del todo ineficiente para la gestión de un accidente severo debido a:

- Las dificultades relacionadas con la evaluación del estado específico de la planta, la disponibilidad de equipos y el uso de esta información para desarrollar estrategias de recuperación.
- Las incertidumbres relacionadas con la fenomenología y la variedad de secuencias que presentan los accidentes severos.

Estos aspectos han llevado a que la mayoría de los desarrolladores de las instrucciones de gestión de accidentes severos se hayan inclinado más por la implementación de guías que por la de procedimientos, IAEA (2004). La diferencia principal entre los procedimientos y las guías es que estas últimas son orientativas y no prescriptivas, debido a las limitaciones del juicio de ingeniería que conlleva su diseño.

Habiendo establecido la diferencia principal entre los procedimientos y las guías en lo que respecta a la gestión de accidentes, a partir de este punto no se considera de interés profundizar más en el estado de operación de accidente severo, aunque se realizarán referencias siempre que se considere de importancia aclarar algún aspecto relacionado con este estado operacional.

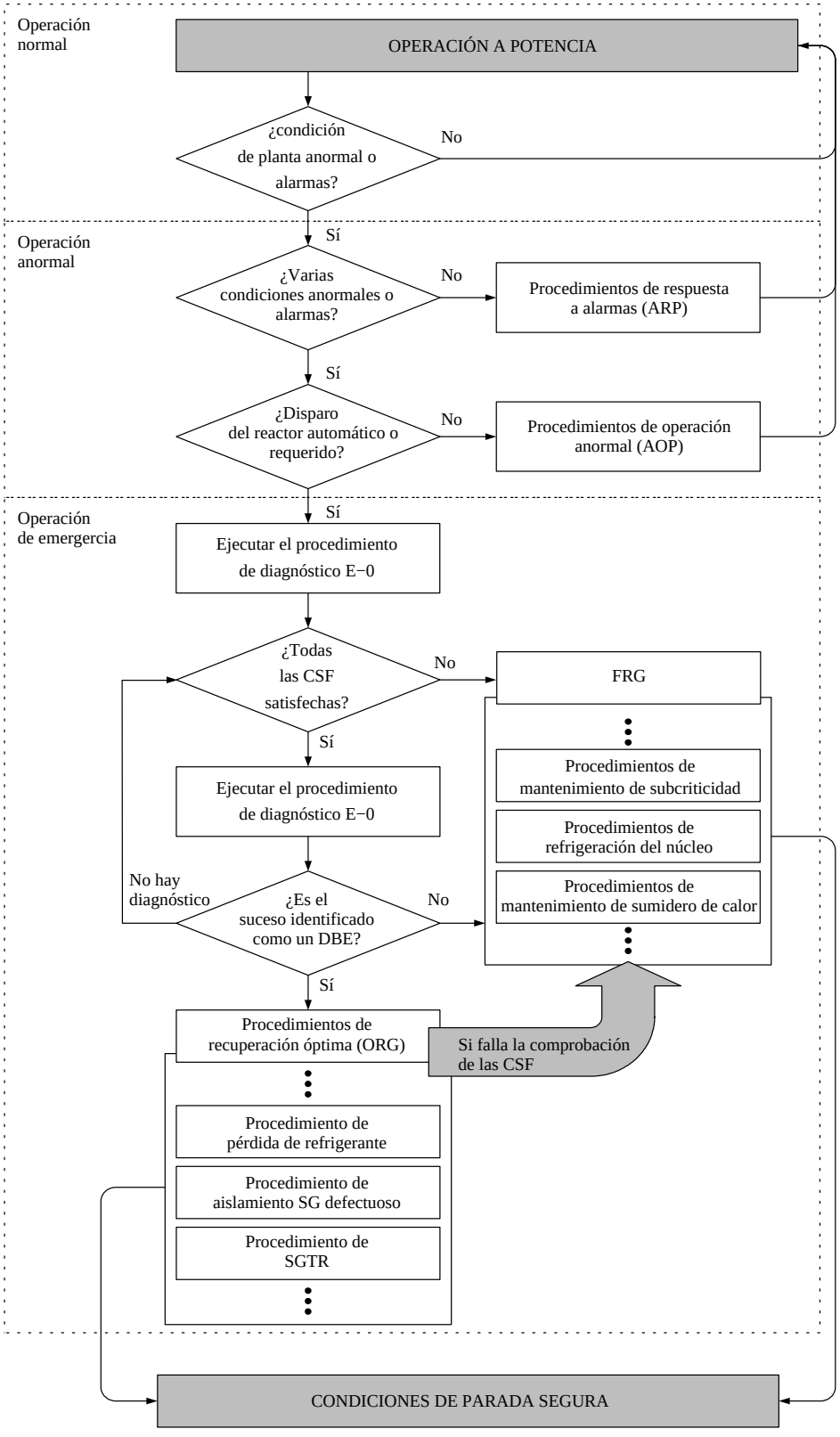


Figura 4.1: Estructura de los procedimientos de operación de una central nuclear PWR-W, Park y Jung (2006b).

<table>
<tr><th colspan="2" rowspan="2">Estado de planta</th><th rowspan="2">Estrategia</th><th rowspan="2">Procedimiento</th><th colspan="3">Práctica de procedimientos</th></tr>
<tr><th>IAEA[a]</th><th>EUA[b]</th><th>Francia[c]</th></tr>
<tr><td colspan="2">Normal</td><td>Prevenir condiciones no seguras</td><td>Instrucciones escritas</td><td colspan="3">Suceso de operación normal</td></tr>
<tr><td colspan="2">Sucesos previstos</td><td>Verificar las funciones de los sistemas normales para limitar los transitorios</td><td>Instrucciones para incidentes del sistema</td><td colspan="2">Suceso de operación anormal</td><td rowspan="4">EOP basados en síntomas</td></tr>
<tr><td colspan="2">DBA (Posible violación de las funciones de seguridad)</td><td>Verificar los parámetros característicos de las funciones de seguridad de ingeniería</td><td>EOP para alcanzar parada fría[d]</td><td>EOP basados en síntomas</td><td>EOP basados en síntomas o integrados</td></tr>
<tr><td rowspan="2">BDBA (Posible daño de las barreras de la bases de diseño)</td><td>Prevenir cond. degradadas del núcleo</td><td>Recuperar las CSF</td><td>Recuperación de funciones</td><td>AMP basadas en síntomas[e]</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>Mitigación de condiciones de fusión del núcleo</td><td>Mitigación de las consecuencias de la fusión del núcleo</td><td>Acciones de mitigación</td><td colspan="3">AMG basadas en síntomas[f]</td></tr>
</table>

[a] Informes técnicos de la serie 368.

[b] Los países con instalaciones de tecnología norteamericana tienen una implementación de los procedimientos similar, como es el caso de España.

[c] Francia usa los procedimientos denominados I y A para los BDA y los procedimientos H para los BDBA.

[d] Basados en sucesos o en síntomas.

[e] Normalmente denominadas procedimientos o guías de restablecimiento de funciones, FRG. En algunos paises son parte integral de los EOP.

[f] Denominadas generalmente como las guías de accidente severo, SAMG.

Tabla 4.1: Estructura de los procedimientos de operación en diferentes países, IAEA (2004 1998).

La implementación de los procedimientos en los diferentes estados operacionales difiere sustancialmente de un pais a otro, estando normalmente ligado al origen tecnológico de las instalaciones, Tabla 4.1. En general, se pueden distinguir tres aproximaciones en la implementación de los procedimientos de operación, IAEA (1998):

- Aproximación basada en sucesos.
- Aproximación basada en síntomas.
- Aproximación integrada.

En los siguientes apartados se explican en detalle cada una de ellas, estableciendo sus ventajas e inconvenientes.

Aproximación basada en sucesos

En los procedimientos basados en sucesos, las decisiones y las medidas para afrontar los sucesos son tomadas en función del estado de planta ligado a un conjunto de sucesos predefinidos, los cuales son considerados en el diseño de la planta. El operador, por lo tanto, debe identificar el DBE que guarda relación con el evento que acontence antes de iniciar las acciones de recuperación y mitigación.

- Ventajas:
  1. Los procedimientos son más fáciles de desarrollar e implementar.
  2. Si el suceso sigue el escenario tal como se espera, las acciones de recuperación y mitigación del operador son directas, fáciles de realizar, más eficientes, consumen menos tiempo y están optimizadas para esas condiciones específicas.
  3. En caso de un diagnóstico correcto y rápido por parte del operador, se puede prevenir la propagación de la situación del emergencia a estados de la planta más graves.
  4. En ciertos estados de operación, como en parada, donde existe un rango mayor de flexibilidad para la variación de los parámetros de la planta, los procedimientos basados en sucesos ofrecen al operador una forma más directa de realizar una recuperación óptima a condiciones seguras.
- Limitaciones:
  1. Los operadores pueden estar sujetos a sucesos inesperados, lo que implica situaciones en las que no tienen entrenamiento o procedimientos adecuados. No hay métodos para afrontar lo inesperado, ya que solo un número finito de sucesos son considerados en el SAR, estando los BDBA más allá del alcance de los procedimientos.
  2. La mayoría de los procedimientos basados en sucesos están orientados a secuencias en las que se asume que todas las acciones son exitosas y no se aportan métodos para afrontar fallos o desviaciones de dicha secuencia.

3. La recuperación o mitigación óptima solo es posible tras la identificación adecuada del tipo de suceso. Además, la necesidad de identificar el suceso lo antes posible provoca estrés en el operador.
4. Los aproximación basada en sucesos no siempre proporciona al operador una forma estructurada de realizar la fase de diagnóstico, adquiriendo una importancia considerable el conocimiento del operador, su nivel de experiencia y su condición mental y física durante el transitorio.
5. No hay relaciones o puntos de transición entre los diferentes procedimientos; por ello, no hay un método para que el operador pueda afrontar una situación de sucesos múltiples, por ejemplo, rotura de línea de vapor con LOCA o pérdida de agua de alimentación total con ATWS.

Aproximación basada en síntomas

La decisión de las medidas para afrontar los sucesos se hace en función de los síntomas del estado de la planta y los sistemas, es decir, los valores de los parámetros de seguridad y las funciones críticas de seguridad, estas últimas se explicarán más adelante. No hay necesidad de identificar el tipo de suceso que acontece antes de iniciar las actividades de recuperación o mitigación.

- Ventajas:
  1. Los procedimientos basados en síntomas resuelven muchas de las limitaciones derivadas de la aproximación basada en sucesos mediante la definición y la priorización de las funciones críticas de seguridad más importantes.
  2. La aproximación basada en síntomas sigue la tendencia natural del operador a mantener los parámetros de seguridad de los sistemas operativos dentro de una banda segura. Esto permite al operador a mantener las características óptimas de operación de los sistemas sin preocuparse acerca del escenario de accidente en que se desenvuelve la actuación.
  3. La implementación de este tipo de procedimientos requiere un conjunto más amplio de análisis termohidráulicos, resultando en una definición más completa de las características de operación de la planta.
  4. El método de vigilancia de los parámetros de planta durante la aplicación de los prodecimientos de operación basados en síntomas es complementaria a la requerida en la operación en condiciones de accidente severo, permitiendo una transición más suave entre ambos estados.
- Limitaciones:
  1. Los procedimientos basados en síntomas son más laboriosos de desarrollar, requieren un análisis técnico más detallado y requieren de un entrenamiento del operador diferente, resultando todo ello en una implementación más cara.
  2. Hay una dependencia muy fuerte entre las acciones del operador, lo que conlleva la necesidad de desarrollar acciones alternativas para facilitar la recuperación

en caso de fallar las acciones realizadas inicialmente. Este aspecto hace que se requieran análisis termohidráulicos adicionales y, en algunos casos, el uso de códigos y modelos más sofisticados.

3. La implementación de este tipo de procedimientos requiere de modificaciones en la instrumentación y de las ayudas instrumentales durante la operación, tales como indicación de nivel en vasija, vigilancia de grado de subenfriamiento y sistemas de visualización de los parámetros de seguridad, como por ejemplo el *Safety Parameter Display System* (SPDS) de Westinghouse.

Aproximación integrada

La aproximación integrada permite el uso en paralelo de ambos tipos de procedimientos, los basados en eventos y en síntomas. El diagnóstico en el que se basan las decisiones para determinar el tipo de suceso se hace en función de los síntomas, como en la aproximación basada en síntomas. Una vez que el suceso es identificado o caracterizado, la aproximación integrada emplea procedimientos basados en sucesos específicos para llevar a cabo las acciones de recuperación y mitigación. El estado general de la planta se sigue vigilando empleando un procedimiento orientado a síntomas mientras que se utilizan los procedimientos basados en sucesos para recuperar la instalación del suceso que acontece.

- Ventajas: La aproximación integrada toma los beneficios de ambas aproximaciones.
- Limitaciones: Es necesario realizar el seguimiento simultáneo de dos tipos de procedimientos.

En el caso de EUA, para proporcionar cobertura para los BDBA y escenarios no considerados se implementan parte de los EOP orientados a síntomas, formando los denominados procedimientos de recuperación de funciones (FRG), manteniendo el resto de los procedimientos orientados a eventos, formando los denominados procedimientos de recuperación óptima (ORG). Las FRG gestionan el suceso de forma independiente a su diagnóstico, favoreciendo la aproximación integrada en el desarrollo de los procedimientos[1]. Su implementación implica la vigilancia de las denominadas funciones críticas de seguridad (*Critical Safety Functions*, CSF) o de los estados de planta durante la gestión del accidente[2]. En este sentido, se garantiza que el objetivo establecido en la defensa en profundidad para la fase preventiva de la gestión del accidente

[1]El grupo de trabajo que estudió el accidente de TMI-2 constató que los EOP orientados a sucesos debían ser completamente reformados de forma que se pudiesen afrontar sucesos que no estuviesen previstos, analizados o considerados en el diseño de los mismos, NRC (1979). De hecho, de la necesidad constatada por este estudio surgió la aproximación orientada a síntomas implementada posteriormente de forma parcial o total en el conjunto de los EOP.

[2]En parte debido a diferencias de diseño, la implementación de los procedimientos orientados a síntomas es radicalmente diferente en las tecnologías de PWR y BWR. Mientras que los BWR se basan en síntomas paramétricos, basados en lecturas de instrumentos como el nivel o la presión en vasija, los PWR se basan en síntomas funcionales, basados en abstracciones de las funciones de seguridad que pueden llegar a implicar varios sistemas y, potencialmente, multitud de parámetros. En este trabajo nos centraremos en los diseños de PWR.

Estado de operación	Tipo de instrucciones	Denominación	Tipo de suceso
Normal	Instrucciones	Instrucciones de operación	Todos
Alarmas	Procedimientos basados en sucesos	Procedimientos de respuesta a alarmas (ARP)	Todos
Anormal	Procedimientos basados en sucesos	Procedimientos de operación anormal (AOP)	Todos
Emergencia	Procedimientos basados en sucesos	Procedimientos de operación de emergencia (EOP)	DBA
	Procedimientos basados en síntomas	Procedimientos de restablecimiento de funciones (FRG)	BDBA
Accidente severo	Guías de operación basadas en síntomas	Guías de gestión de accidente severo (SAMG)	BDBA

Tabla 4.2: Resumen de los procedimientos empleados en la operación de una central PWR-W.

es alcanzado, independientemente de la posibilidad de ocurrencia de los DBA y BDBA. Además, en el caso de las actuaciones consideradas para los BDBA, se considera el uso de todo el equipamiento disponible en la central, incluyendo aquellos que no son parte de los sistemas de seguridad. El resultado final es el conjunto de procedimientos que se resume en la Tabla 4.2, con la estructura de la Figura 4.1.

En los que respecta a la gestión de accidentes tanto preventiva (EOP) como de mitigación (SAMG), la implementación de procedimientos basada en síntomas se considera una buena práctica para el desarrollo de los procedimientos, y esa es la política en algunos países, siendo un ejemplo de ello el caso de Francia.

Como ya se ha comentado anteriormente, y de forma general, la implementación de los procedimientos suele estar ligada al origen de la tecnología de las instalaciones. Así, para el caso de España, la implementación en la centrales PWR-W de tecnología americana suele basarse en una aproximación integrada, y será la que se tratará en las secciones siguientes. Además, y debido a que el interés del trabajo se centra en exclusivamente en el desarrollo de versiones computerizadas de los EOP, el resto de procedimientos de los diferentes estados de operación no se tratarán.

4.1.1 Los EOP de tecnología PWR-W: estructura global y dependencias

De la introducción realizada en la sección anterior se puede concluir que, generalmente, las emergencias en centrales nucleares pueden dividirse en dos categorías, Figura 4.2:

- La primera categoría incluye los DBA que pueden ser identificados reconociendo sus síntomas característicos por ciertos parámetros de relevancia o por la historia operativa reciente de la instalación.

  Los EOP diseñados para esta categoría se denominan las guías de recuperación óptima (*Optimal Recovery Guideline*, ORG). En general, las ORG forman un conjunto de procedimientos optimizados para llevar a la planta a parada segura.

Las ORG son iniciadas cuando el reactor ha disparado o ha actuado el sistema de refrigeración del núcleo. De forma inmediata, se verifican las señales de actuación automáticas y se inicia el proceso de diagnosis del suceso. Cuando se identifica la naturaleza del suceso, el operador es dirigido al procedimiento de recuperación aplicable. Hay tres niveles de diagnosis integrados en las ORG: el diagnóstico temprano (E-0, realizado al inicio), el contínuo (integrado en los procedimientos) y el rediagnóstico (ES-0.1, a voluntad del operador).

- La segunda categoría se corresponde con los BDBA, es decir, aquellos sucesos que son imposibles de identificar de forma precisa debido a que su fenomenología es demasiado compleja y normalmente no se dispone de ningún análisis previo de la misma. Los sucesos incluidos en esta categoría suelen ser DBA múltiples o fallos de instrumentación que distorsionan el conjunto de síntomas de un suceso que un principio podría ser diagnosticado.

  Los procedimientos implementados para afrontar este tipo de situaciones son los denominados procedimientos de restablecimiento de funciones (*Function Recovery Guidelines*, FRG), que diseñadas en base a parámetros de la planta y la disponibilidad de equipos proporcionan una gestión no optimizada pero global e independiente de los sucesos que hayan ocurrido, tanto al inicio del transitorio como durante la gestión del mismo.

  Para alcanzar este objetivo, el conjunto de funciones debe ser definido en base a los parámetros que son críticos desde el punto de vista de seguridad de la planta. Estas son las denominadas funciones críticas de seguridad, CSF. A cada una de las CSF se le asigna una FRG para restaurarla dentro de los límites definidos en el diseño de la planta.

Como se puede comprobar, los objetivos de diseño de las ORG y las FRG difieren conceptualmente. En el caso de las primeras, se establece como piedra angular el concepto de operación de emergencia basado en la recuperación óptima, mientras que para las segundas, se emplea el concepto de restablecimiento de funciones críticas de seguridad.

El concepto de recuperación óptima está relacionado con una estrategia predefinida de recuperación, asociada a unos síntomas, para alcanzar el estado final óptimo de la central. Estas estrategias son las ORG. El estado final óptimo es aquel que minimiza tanto la emisión de radiación como los daños a equipos, funcionando los últimos de forma que se puedan mantener unas condiciones estables a largo plazo. Los síntomas de los transitorios de emergencia están afectados por multitud de factores (condiciones iniciales, suceso desencadenante, etc.), sin embargo, los transitorios más probables, es decir, los correspondientes al estudio base de diseño, muestran síntomas característicos que se pueden clasificar dentro de cuatro categorías básicas, Tabla 4.3:

- **Categoría de no accidente** (Categoría 0): en la cual los límites de protección del reactor se sobrepasan pero no se llega a los límites de salvaguardias. Está ligada al disparo del reactor o una actuación de la SI. Se incluyen en esta categoría los procedimientos de respuesta a un disparo del reactor, pérdida total de corriente alterna y enfriamiento por circulación natural (E-0 y sub-procedimientos asociados (ES) y los **Procedimientos de Acción de Contingencia de Emergencia (ECA)** ECA-0.0, ECA-0.1 y ECA-0.2).

- Tres **categorías de accidente**: en las que los límites de salvaguardias se exceden debido a los transitorios asociados con los tres sucesos iniciadores de accidente más importantes de los reactores de agua a presión (PWR):

    1. **Pérdida de refrigerante del reactor (LOCA)**. Llevan a esta categoría el conjunto de síntomas asociados con la pérdida de refrigerante del reactor. Están incluidos los procedimientos para el enfriamiento y despresurización después de una pérdida de refrigerante del reactor, la reducción y terminación de la SI, el cambio de recirculación a largo plazo y la pérdida de la capacidad de recirculación (E-1, ES ligados, ECA-1.1 y ECA-1.2).
    2. **Pérdida de refrigerante del secundario**. Llevan a esta categoría lo síntomas asociados con la pérdida de refrigerante del secundario, incluyendo la pérdida de refrigerante del secundario de varios Generadores de Vapor (SG). Esta categoría incluye el procedimiento para el aislamiento de los SG defectuosos (E-2 y ECA-2.1).
    3. **Rotura de tubos de Generadores de Vapor**. Esta categoría hace referencia a síntomas asociados con la rotura de tubos de un generador de vapor, incluyendo la rotura de tubos de varios generadores de vapor y rotura de tubos en combinación con la pérdida de refrigerante del reactor o refrigerante secundario. También incluye el procedimiento para el enfriamiento y despresurización después de la rotura de tubos del generador de vapor, reducción y terminación de SI y fallo de la capacidad de control de la presión en el presionador (E-3, ES asociados, ECA-3.1, ECA-3.2 y ECA-3.3).

En resumen, se puede observar como para cada categoría existe un procedimiento de entrada (E) con un conjunto de subprocedimientos (ES) y una serie de procedimientos de acción de contingencia de emergencia (ECA) asociados a cada uno de ellos. Los subprocedimientos complementan a los procedimientos de entrada, proporcionando estrategias de recuperación alternativas para los escenarios dentro de la categoría de sucesos. Los procedimientos de acción de contingencia de emergencia complementan ambos, procedimientos de entrada y subprocedimientos, desarrollando la doble función de proporcionar guías para escenarios de baja probabilidad o sucesos atípicos y, a su vez, lo hacen sin complicar indebidamente las instrucciones contenidas en los procedimientos de entrada y subprocedimientos para los escenarios de sucesos más probables.

E-0	Procedimiento de Disparo del reactor y/o Inyección de Seguridad.
ES-0.0	Procedimiento de confirmación del diagnóstico.
ES-0.1	Procedimiento de recuperación del disparo de reactor.
ES-0.2	Procedimiento de enfriamiento por circulación natural.
ES-0.3	Procedimiento de enfriamiento por circulación natural con formación de vapor en la vasija (con RVLIS).
ES-0.4	Procedimiento de enfriamiento por circulación natural con formación de vapor en la vasija (sin RVLIS).
E-1	Procedimiento de pérdida de refrigerante del reactor o secundario.
ES-1.1	Procedimiento de finalización de Inyección de Seguridad
ES-1.2	Procedimiento de enfriamiento y disminución de presión tras LOCA.
ES-1.3	Procedimiento de cambio de recirculación a ramas frías.
ES-1.4	Procedimiento de cambio de recirculación a ramas calientes.
ES-1.5	Reducción de la inyección de seguridad en fase de recirculación a ramas frías.
E-2	Procedimiento de aislamiento de un Generador de Vapor defectuoso.
E-3	Procedimiento de rotura de tubos de un generador de vapor.
ES-3.1	Procedimiento de enfriamiento tras una rotura de tubos en un generador de vapor mediante llenado inverso.
ES-3.2	Procedimiento de enfriamiento tras una rotura de tubos en un generador de vapor mediante la purga.
ES-3.3	Procedimiento de enfriamiento tras una rotura de tubos en un generador de vapor mediante alivio de vapor.
ECA-0.0	Pérdida total de corriente alterna.
ECA-0.1	Recuperación tras la pérdida total de C.A. sin necesidad de inyección de seguridad
ECA-0.2	Recuperación tras la pérdida total de C.A. con necesidad de inyección de seguridad
ECA-1.1	Pérdida de recirculación de refrigerante de emergencia.
ECA-1.2	LOCA fuera del recinto de contención
ECA-2.1	Despresurización incontrolada de todos los generadores de vapor
ECA-3.1	Rotura de tubos del Generador de Vapor con LOCA. Recuperación en condiciones de subenfriamiento
ECA-3.2	Rotura de tubos del Generador de Vapor con LOCA. Recuperación en condiciones de saturación
ECA-3.3	Rotura de los tubos del Generador de Vapor sin control de presión en el presionador

Tabla 4.3: Procedimientos de recuperación óptima propios de la tecnología PWR-W.

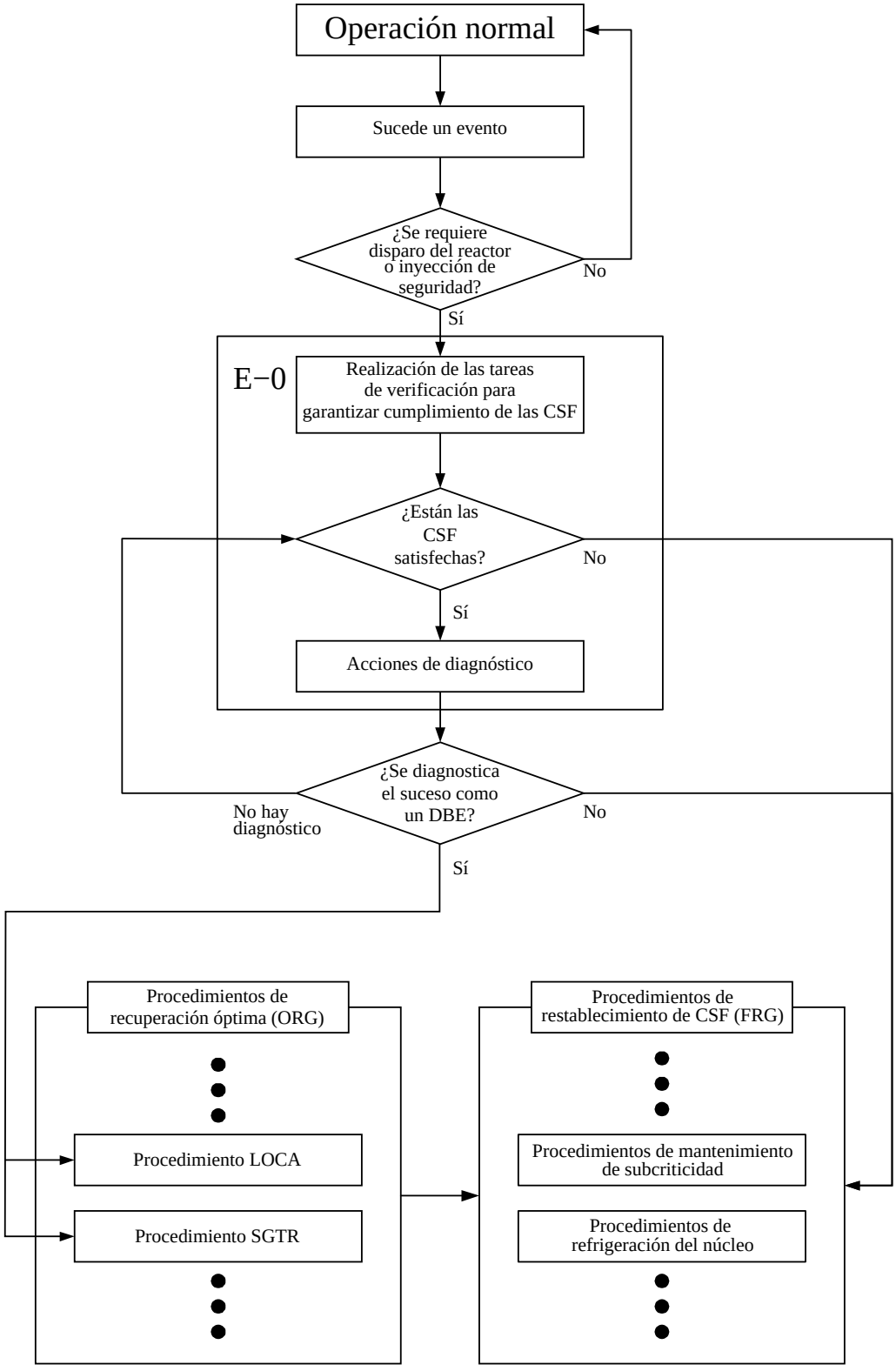


Figura 4.2: Estructura implementada en los modelos de EOP y FRG de tecnología PWR-W.

Como ya se mencionó, el objetivo de todas las acciones llevadas a cabo por el operador es alcanzar el estado final óptimo. Para garantizar la consecución de este objetivo, basado en minimizar la emisión de radiación al medio ambiente, se desarrolló el concepto de Restablecimiento de las funciones críticas de seguridad (CSF), Westinghouse (1993). Los procedimientos asociados, denominados procedimientos de restablecimiento de funciones (FRG), tienen como finalidad proteger las barreras a la liberación de radiación y conseguir el retorno de la central a un estado seguro en el que las Funciones Críticas de Seguridad se satisfagan. Para cumplir con el primer objetivo se adoptó el concepto de defensa en profundidad, es decir, proporcionar múltiples barreras a la emisión del material radiactivo, a saber:

- Las pastillas y vainas del combustible.
- La barrera de presión del sistema de refrigeración del reactor.
- El recinto de contención.
- La ubicación de la central nuclear.

Las tres primeras son barreras físicas que se oponen de forma directa al transporte de materiales radiactivos y, por ello, serán las condiciones sobre las que se trabajen las FRG, quedando la última asociada a los objetivos del Plan de emergencia Local. Cabe destacar que el empleo de las FRG queda restringido a situaciones en las que se ha producido o es necesario el disparo del reactor, quedando fuera de su aplicación las situaciones de operación normal a potencia. A partir de la enumeración de las tres barreras físicas a conservar se deduce que el conjunto mínimo de Funciones Críticas de Seguridad está formado por:

- Mantenimiento de subcriticidad.
- Mantenimiento de la refrigeración del núcleo.
- Mantenimiento del sumidero de calor.
- Mantenimiento de la integridad del RCS.
- Mantenimiento de la integridad de la contención.
- Control del inventariado de refrigerante del reactor.

El atractivo de las CSF consiste en que, para garantizar el estado de seguridad de la planta, el operador sólo debe monitorizar un conjunto reducido de parámetros, pudiendo desarrollar actividades paralelas, sin preocuparse por el suceso o sucesos que han provocado dicha situación. Para diagnosticar el estado de cumplimiento de las CSF se desarrollaron los árboles de estado. Existe un árbol de estado para cada una de las CSF, los cuales en conjunto determinan el estado de seguridad global de la central. Los árboles de estado se corresponden con unas estructuras ramificadas de decisión, atendiendo a unos pocos parámetros, cuya evaluación lógica determina de forma unívoca el estado de la CSF evaluada, Figura 4.3. Cada árbol de estado tiene un único

punto de entrada y multitud de puntos de salida, denominados terminales, que determinan que FRG será empleada para su restablecimiento, Figura 4.4. Además de identificar el estado de seguridad de la central, el árbol de estado también proporciona un método óptimo para establecer prioridades en la respuesta del operador. La asignación de esta prioridad en la evaluación de cada CSF se basa directamente en el concepto de la barrera a partir de la cual se desarrollaron. Por ello, al ser la primera barrera las pastillas y la vaina, los posibles motivos de su deterioro, criticidad y refrigeración, obtienen la prioridad más alta en este orden. Después, se garantiza la integridad del sistema de refrigeración del núcleo, atendiendo a los parámetros internos que pueden afectarla, es decir, choque térmico de la vasija, fragilización de la misma por condiciones de baja temperatura del refrigerante del reactor, etc. Por ello, a la integridad del sistema de refrigeración del reactor se le asigna el siguiente nivel de prioridad. La tercera barrera, el recinto de contención, también se estudia de la misma forma que el anterior, tomando el cuarto estado de prioridad. Finalmente, para facilitar la construcción de su correspondiente árbol de estado, el diagnóstico del inventariado del refrigerante se realiza de forma independiente y en último lugar, a pesar de ser realmente un subconjunto de la CSF de enfriamiento del núcleo. Esta última CSF contempla las situaciones en las que el inventariado de refrigerante del reactor es adecuado para satisfacer la CSF de enfriamiento del núcleo pero no dentro de los límites de la operación normal.

La asignación de prioridades queda:

1. Subcriticidad (S)
2. Enfriamiento del núcleo (C)
3. Sumidero de Calor (H)
4. Integridad (P)
5. Contención (Z)
6. Inventariado (I)

Una vez establecidas las prioridades de las CSF, también deben asignarse prioridades a los riesgos dentro de cada CSF y entre las CSF. Dado de cada árbol de estado sólo lleva a una terminal de salida en cada validación, se clasificaron los terminales de los distintos árboles de estado basándose en la severidad del riesgo. Con ello, una vez evaluadas todos ellos, se busca que el operador sea capaz de iniciar la FRG correspondiente a la CSF que implique mayor riesgo y, de forma sucesiva, recuperar la totalidad de las CSF. De esta forma, se definen cuatro condiciones de estado: extrema, severa, no satisfecha y satisfecha, para permitir la asignación de prioridades de una condición respecto a las condiciones de otras CSF. Además, dentro de cada árbol de estado se ordenan las terminales de forma descendente en importancia del riesgo que conlleven, permitiendo una clasificación dentro de las categorías de extrema, severa, no satisfecha y satisfecha (roja, naranja, amarilla y verde).

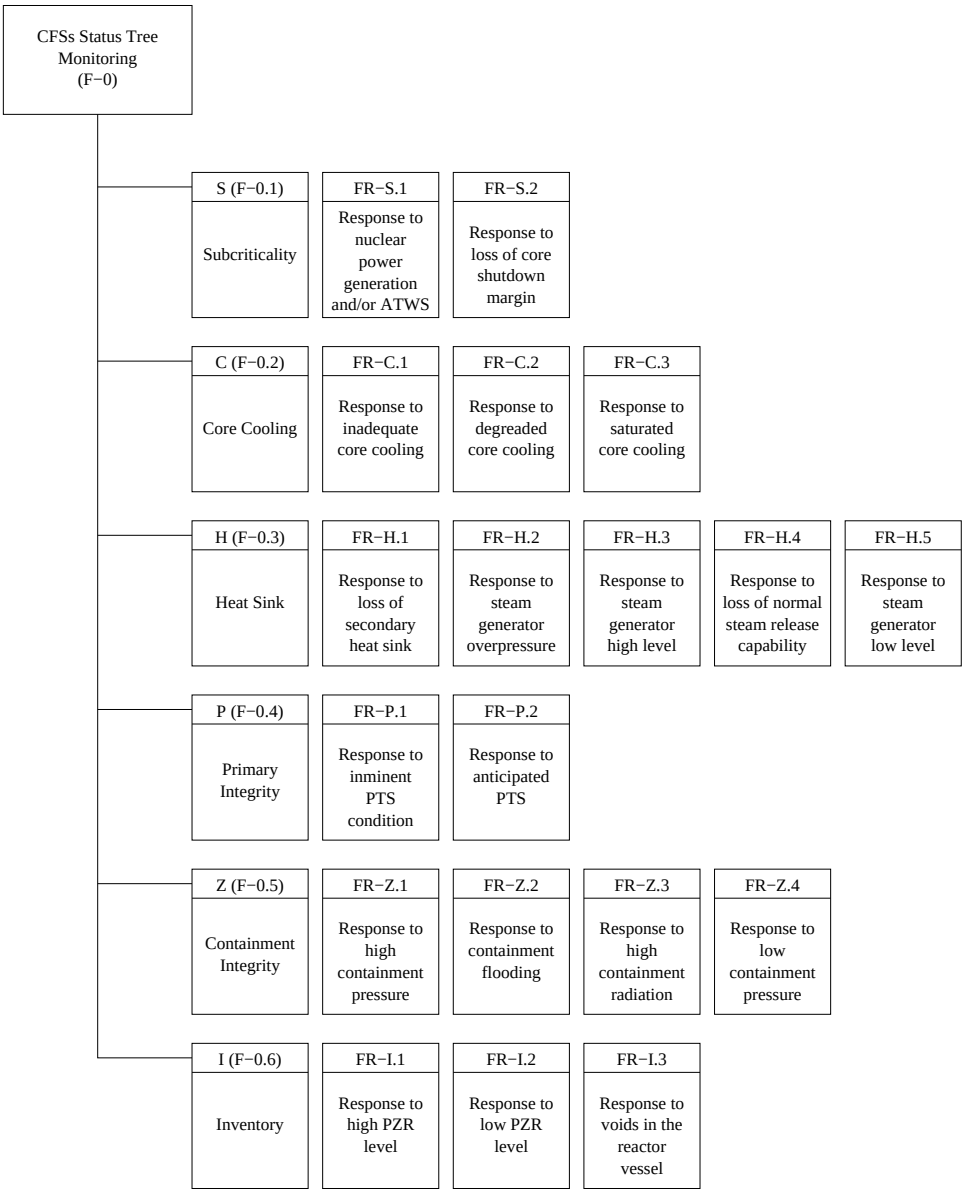


Figura 4.3: Estructura general de los árboles de estado de las CSF y FRG.

La vigilancia de los árboles de estado comienza poco después de la entrada a los EOP, en el procedimiento E-0, o tras una transición a otro EOP desde el E-0 motivada por la fenomenología del transitorio. Tras su evaluación, se determinará la prioridad de realización de las FRG necesarias, si las hubiera, y cuando se finalicen las tareas de recuperación, alcanzando el estado de condiciones satisfechas de todas las CSF, se iniciará la ORG pertinente. Existen ciertos procedimientos que priman sobre los procedimientos de recuperación de funciones por tratarse de sucesos específicos. En estos casos la prioridad se indica mediante una nota al principio del procedimiento. Generalmente, considerando esta excepción, las CSF se evalúan periódicamente cada diez o veinte minutos una vez iniciada su vigilancia cuando la severidad no pasa de no

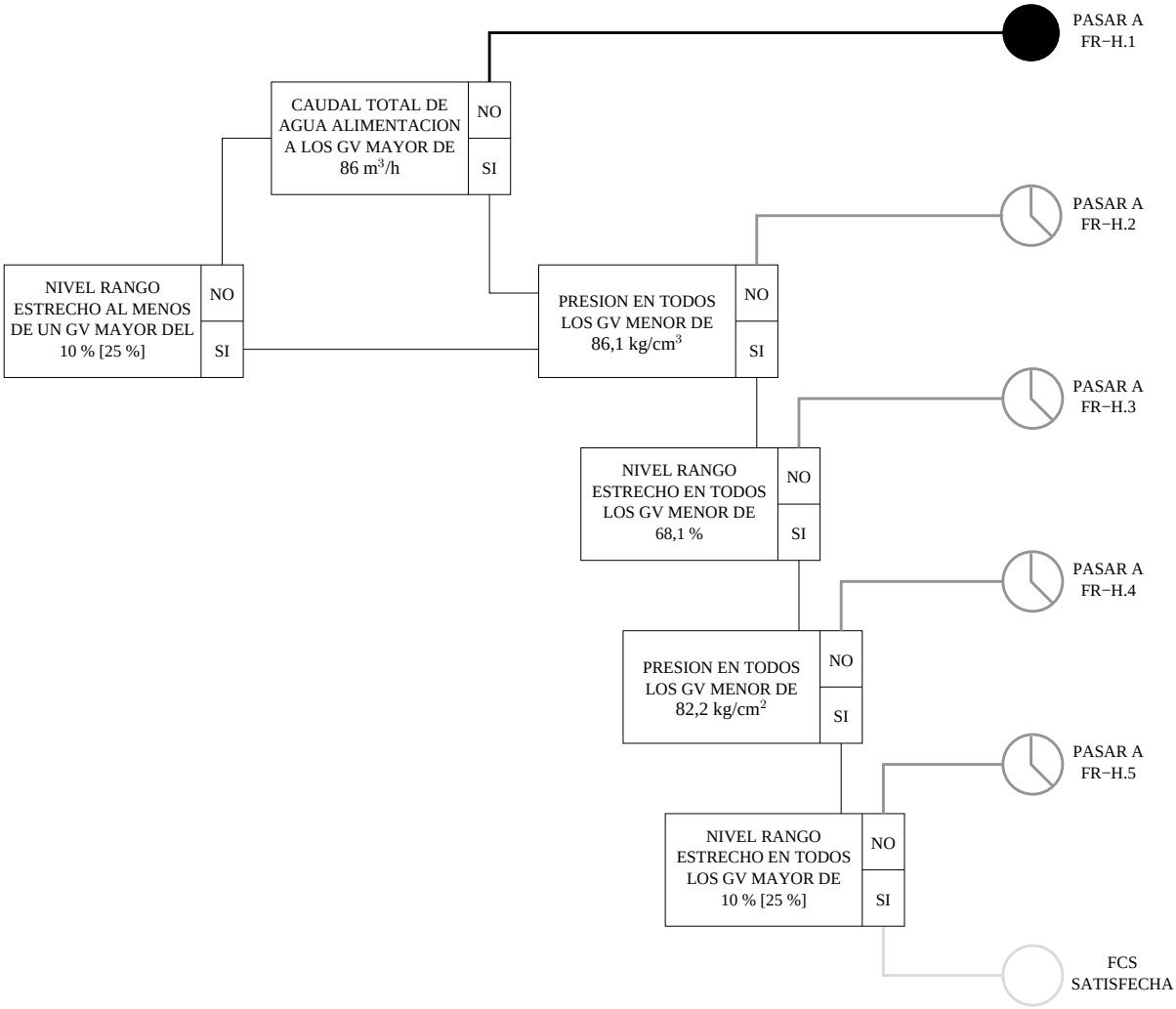


Figura 4.4: Estructura del árbol de estado de CSF de pérdida de sumidero de calor, F-0.3.

satisfecha (amarilla), y de forma continua si existe una condición severa o extrema (naranja o roja), Tecnatom (2000). El número de FRG (FR) de cada CSF (FC) se determina partiendo de la estructura de cada árbol de estado (F), Tablas 4.4 y 4.5.

Para una descripción sucinta de los distintos EOP desarrollados para la gestión de situaciones de emergencia en reactores tipo PWR-W considerando el interés de este trabajo se puede consultar el infome Expósito y Queral (2004c). En este sentido, las FRG se consideran fuera del alcance inicial, aunque a lo largo del trabajo se decidió la consideración parcial de parte de las mismas, como es el caso de la FRG relacionada con la pérdida de sumidero de calor, FR-H.1.

F-0	Árboles de estado de las funciones críticas de seguridad
F-0.1	Subcriticidad (S)
F-0.2	Enfriamiento del núcleo (C)
F-0.3	Sumidero de Calor (H)
F-0.4	Integridad (P)
F-0.5	Contención (Z)
F-0.6	Inventario (I)

Tabla 4.4: Árboles de estado de las funciones críticas de seguridad de tecnología PWR-W.

FRG	**Descripción**
FR-S.1	Respuesta a una generación no deseada de potencia y/o ATWS
FR-S.2	Respuesta a la pérdida del margen de parada
FR-C.1	Respuesta a la refrigeración inadecuada del núcleo
FR-C.2	Respuesta a la refrigeración degradada del núcleo
FR-C.3	Respuesta a la refrigeración del núcleo en saturación
FR-H.1	Respuesta ante la pérdida de sumidero de calor
FR-H.2	Respuesta a una sobrepresión en un Generador de Vapor
FR-H.3	Respuesta a un nivel alto en un Generador de Vapor
FR-H.4	Respuesta ante la pérdida de capacidad normal de alivio de vapor
FR-H.5	Respuesta a un bajo nivel en un Generador de Vapor
FR-P.1	Respuesta ante una condición inminente de choque térmico a presión en la vasija
FR-P.2	Respuesta ante una condición anticipada de choque térmico a presión en la vasija
FR-Z.1	Respuesta ante alta presión en el recinto de contención
FR-Z.2	Respuesta ante alto nivel en el recinto de contención
FR-Z.3	Respuesta ante alta radiación en el recinto de contención
FR-I.1	Respuesta ante alto nivel en el presionador
FR-I.2	Respuesta ante bajo nivel en el presionador
FR-I.3	Respuesta a la formación de vapor en la vasija del reactor

Tabla 4.5: Procedimientos de restablecimiento de funciones de tecnología PWR-W.

4.1.2 Elementos estructurales que componen los EOP

De forma genérica, en los procedimientos se pueden distinguir cinco elementos estructurales básicos, Orendi et al. (1988) y Tecnatom (2000):

- Portada.
- Pasos de instrucción.
- Figuras.
- Anexos.
- Página desplegable.

Al iniciar un procedimiento, se empieza por la portada. En ella se resume el objetivo del procedimiento, así como los síntomas de entrada o transiciones. Esta información ayuda al operador a realizar la correcta elección del procedimiento a seguir. Después de la portada, se inicia la ejecución del procedimiento. Para seguir la descripción de la estructura del procedimiento se puede ver la Figura 4.5, correspondiente a una parte de una página de un procedimiento de operación de emergencia. Aclarar que la figura muestra un ejemplo estructural de los elementos de una página de procedimiento, presentando diferencias de forma respecto a una página real.

En algunos pasos de acción puede que sea necesaria información suplementaria para la realización de las instrucciones solicitadas. Esta se presenta en forma de notas o precauciones. Las notas contienen información administrativa o de asesoramiento, mientras que las precauciones informan sobre peligros potenciales a personas o equipos. Además, también aconsejan de acciones o transiciones que puedan ser necesarias dependiendo de los cambios de las condiciones de la planta. En general, las notas y las precauciones aplican al paso al que preceden, mientras que las notas y precauciones que preceden a primer paso de acción de un procedimiento aplican durante la ejecución del mismo. Otro de los aspectos a destacar respecto a las notas y las precauciones, es que en casos excepcionales pueden informar de acciones. Normalmente suelen ser acciones continuas de carácter pasivo que aplican a todo el procedimiento, haciendo probable su olvido en el caos de que estas acciones se implementen como pasos.

Los pasos de instrucción están constituidos por las instrucciones que componen el procedimiento, presentadas al operador siguiendo una jerarquía secuencial de pasos de acción. Cada paso presenta un titulo, que describe la acción a realizar. Si se requieren multiples acciones se mostrarían como subpasos. Si la secuencia de las subtareas es importante, estas vienen especificadas con letras o números. Si la secuencia de ejecución no es importante, las tareas se especificarán con símbolos. A continuación de cada acción o validación de variables físicas va informada, en mayúsculas y separada por un guión, la respuesta esperada, aunque no se suele especificar para las manipulaciones sencillas. Todas las acciones a realizar van informadas en la columna izquierda del procedimiento. En el caso de no obtenerse alguna de las respuestas esperadas o no poder ejecutarse la acción, el operador da paso a la columna derecha de respuesta no obtenida para posibles alternativas. Esta columna se denomina como Respuesta no obtenida. Casi todos

NOTA

- LOS PASOS 1 A 4 SON DE ACCIÓN INMEDIATA
- LA PÁGINA DESPLEGABLE DEBERÁ ESTAR ABIERTA

Paso	Accion/respuesta esperada	Respuesta no obtenida
1	**Verificar disparo del reactor:** • Luces indicadoras de barras a fondo - ENCENDIDAS • Interruptores de disparo del reactor y bypass - ABIERTOS • Flujo neutrónico - DISMINUYENDO	Disparar reactor manualmente. SI NO se produce el disparo, realizar lo siguiente: 1) Comprobar inserción automática y continua de las barras de control. SI NO, iniciar inserción continua de las barras de control manualmente. 2) Simultaneo a la inserción de barras, desenergizar manualmente los centros de fuerza de alimentación a motogeneradores (MG's): • Barra 1B1A - ABRIR 52/1B1A • Barra 1B5A - ABRIR 52/1B5A 3) Pasar a EOP-1-FR-S.1, RESPUESTA ANTE UNA GENERACIÓN NO DESEADA DE POTENCIA Y/O ATWS, Paso 1.
2	**Verificar disparo de turbina:** a. Válvulas de parada - CERRADAS.	a. Disparar turbina manualmente. SI NO se produce el disparo, seleccionar control manual de turbina y cerrar válvulas de regulación en modo acción rápida. SI NO, parar y bloquear bombas de fluido electrohidráulico. SI NO, cerrar válvulas de aislamiento (MSIV) y bypass de líneas de vapor principal.

Figura 4.5: Ejemplo de la estructura de pasos de un EOP de tecnología PWR-W.

los pasos de acción contienen alguna actuación de contingencia. Si una acción de contingencia es apropiada para toda la serie de subtareas informada en la columna de la izquierda, ésta solo se informa una sola vez como una contingencia remarcada en mayúsculas y subrayada. En el caso de que no se proporcione ninguna acción de contingencia, el operador procederá al siguiente paso a subtarea informado en la columna de la izquierda.

Tras realizar la acción de contingencia especificada en la columna de la derecha, el operador procede al paso siguiente en la columna de la izquierda. Si la acción de contingencia no puede ser ejecutada o si no es exitosa, y no se informan más acciones de contingencia, el operador retorna de nuevo al paso o instrucción en la columna izquierda. Si no se especifica lo contrario, una tarea requerida debe ser completada antes de continuar con la siguiente instrucción, siendo

suficiente con iniciar la tarea y asegurarse que la progresión de la misma es satisfactoria. Este aspecto garantiza una implementación eficiente cuando las actuaciones requieren mucha dedicación en tiempo. Cualquier información que deba ser conocida por el operador, basada en el entrenamiento o la experiencia, no se incluye en los pasos. Toda información de explicación y de base de las guías se incluye en los documentos base de los procedimientos.

En cuanto a la gramática y la puntuación, cabe aclarar que las guías tienen un significado preciso para que el operador entrenado en su interpretación no dude en su ejecución. El conjunto de verbos de acción se encuentra cerrado y definido, estando las tareas del operador establecidas de forma exacta en función del verbo usado.

Se pueden distinguir tres tipos de pasos de instrucción atendiendo al modo de ejecución, a saber:

- Pasos de acción normal.
  Su ejecución contempla la actuación requerida en el momento en que se alcanza el paso. No se procede a la ejecución del paso posterior hasta que la actuación ha finalizado o hasta que, habiendo realizado un conjunto significativo de acciones relacionadas con la actuación, se comprueba que la ejecución del paso conlleva la obtención del resultado esperado.

- Pasos de acción inmediata.
  Este tipo de pasos pueden realizarse, por parte del operador, de memoria, sin necesidad de consultar el procedimiento escrito. Una vez realizados, el operador tiene la obligación de realizar una comprobación de los pasos realizados con el procedimiento escrito.

  Los pasos de acción inmediata se identifican mediante una nota anterior al primero del grupo de pasos de este tipo, definiendo a cuantos de ellos aplica.

- Pasos de acción continua.
  Son aquellos que contienen un conjunto de acciones que el operador deberá realizar de forma continuada a lo largo de la ejecución del procedimiento. Suele corresponder con pasos cuyo verbos de acción pueden ser vigilar, mantener o controlar, ligados al seguimiento del valor de un parámetro de planta.

  En los procedimientos de operación de emergencia, este tipo de pasos se distingue por tener su numeración enmarcada en un círculo sombreado.

  Cuando las condiciones de vigilancia o control del parámetro o parámetros relacionados con el paso se cumplan, las acciones asociadas a este tipo de pasos suelen ejecutarse en paralelo a las acciones asociadas a los pasos de los EOP que se estén ejecutando en ese momento.

Tanto las figuras como los anexos, son formas de completar la información suministrada al operador para realizar los pasos de acción. Son opcionales y solo se encuentran en los procedimientos en que se consideran necesarios.

El ultimo elemento a comentar corresponde con la página desplegable, ver Figura 4.6. Es optativa, en el sentido de que no todos los procedimientos disponen de ella, conteniendo información

CRITERIOS DE OPERACIÓN DE EMERGENCIA

1. **CRITERIOS DE DISPARO DE LAS BOMBAS DEL REFRIGERANTE DEL REACTOR (RCP)**

   Disparar todas las RCPs si se cumplen las DOS condiciones siguientes:

   a. Bombas de carga - AL MENOS UNA EN FUNCIONAMIENTO E INYECTANDO.

   b. Subenfriamiento del RCS basado en termopares (TC) de salida del núcleo (ICCM) - INFERIOR A 0^oC [0^oC]

2. **CRITERIOS DE CAMBIO DE SUMINISTRO DE AGUA DE ALIMENTACIÓN AUXILIAR (AF)**

   Cambiar aspiración de bombas de AF, al tanque de condensado (CST), si el nivel del tanque de AF disminuye por debajo del 10 %. Si el tanque de condensado (CST) no esta disponible, la fuente alternativa de suministro de AF sera el SW.

RELACIÓN DE PASOS DE ACCIÓN CONTINUA

Paso 12: Comprobar Presión del Recinto de Contención (RC)
Paso 17: Comprobar Temperaturas del Sistema del Refrigerante del Reactor (RCS)
Paso 19: Comprobar Necesidad de Parar Bombas del Refrigerante del Reactor (RCP)
Paso 23: Comprobar Necesidad de Reducir Caudal de Inyección de Seguridad (SI)
Paso 25: Comprobar Niveles de Todos los Generadores de Vapor (SG)

Figura 4.6: Ejemplo de la estructura de la página desplegable de un EOP de tecnología PWR-W.

genérica adicional aplicable los procedimientos asociados a la misma. Durante la ejecución del procedimiento al que esté asociada, la página desplegable debe estar visible en todo momento. El operador deberá realizar una comprobación continuada de las validaciones contenidas en ella, ejecutando las acciones correctoras que se especifiquen. Las acciones más importantes de este tipo son las transiciones a otras guías o procedimientos, las cuales permiten una respuesta inmediata a nuevos síntomas tan pronto como aparecen.

Finalmente, en cuanto al control de flujo, las transiciones a otras guías o procedimientos o a diferentes pasos de la misma guía pueden realizarse desde cualquiera de las columnas del mismo. Esas transiciones deben realizarse de forma que quede clara la aplicación de notas y precauciones que apliquen en el destino de la transición. Las tareas que se estén realizando en el momento de la transición deben finalizarse antes de llevarse a cabo la misma. Cada guía finaliza con una transición a otra guía, si se requieren más actuaciones del operador, o con una instrucción de mantenimiento de la condición de planta de forma estable y segura. A menudo en las ORG, la transición final se hace a la guía y paso en ejecución, entendiéndose por paso en ejecución al paso que estaba siendo ejecutado cuando la transición se realizó a la guía actual, pudiendo presentar una estructura anidada de varios niveles.

4.1.3 Seguimiento de los EOP en la gestión de emergencias en PWR-W

Cuando tiene lugar una situación de emergencia que provoca disparo de reactor o la actuación del sistema de refrigeración de emergencia del núcleo, la mayoría de las actuaciones consideradas en los EOP son llevadas a cabo por el personal de la sala de control principal. Normalmente, este grupo de trabajo se compone de[3], Figura 4.7:

- El jefe de turno: se suele corresponder con un operador de reactor con experiencia (*Senior Reactor Operator*, SRO). Tiene la responsabilidad de todas las actuaciones realizadas durante una emergencia.
- El operador de reactor (*Reactor Operator*, RO), encargado de realizar todas las acciones demandas por los procedimientos relacionadas con el lado primario de la planta, es decir, la isla nuclear.
- El operador de turbina (*Turbine Operator*, TO), que, al igual que el RO, es el encargado de realizar todas las acciones demandas por los procedimientos relacionadas con el lado secundario de la planta, es decir, la isla de turbina.
- En algunas plantas, no siendo habitual, suele haber una persona dedicada a la vigilancia de los parámetros de seguridad, el denominado supervisor de seguridad (*Safety Supervisor*, SS), principalmente las CSF, empleando los equipos de apoyo a la operación específicos, por ejemplo, el SPDS implementado en las plantas PWR por Westinghouse, y realizando tareas de apoyo en la realización las actuaciones de los procedimientos.

En este esquema de organización, el SRO es el responsable de realizar el seguimiento de los procedimientos, leyendo en alto de forma clara y precisa todas las actividades prescritas en los pasos de los procedimientos, que son llevadas a cabo en base a sus órdenes. De esta forma, todas las tareas de toma de decisiones y de diagnóstico están condicionadas al juicio del SRO, el cual puede realizar consultas a cualquiera de los miembros del grupo de trabajo o solicitar apoyo en la toma de decisiones de forma general al grupo en caso extraordinario. Como ya se ha comentado en la descripción de los EOP, la vigilancia del cumplimiento de las CSF es una tarea que se debe hacer garantizando cierta periodicidad, entre diez y veinte minutos. Normalmente, esta tarea la lleva a cabo el SS, pudiendo variar su asignación en función de la configuración del personal disponible en la sala de control. Bajo este esquema de operación, es razonable suponer que la mayor parte de la carga cognitiva relacionada con el diagnóstico y el seguimiento de los procedimientos es asumida por el SRO, Park y Jung (2003a) y Jung et al. (2001), y la carga de trabajo relacionada con la ejecución de las acciones se reparte entre el resto del personal.

En otras configuraciones del personal de sala de control, el papel del SS lo realiza el denominado asesor técnico del turno de operación (*Shift Technical Advisor*, STA). Este operador es el

[3]Aspectos relacionados con los turnos de operación y su transición, considerando el intercambio de información sobre la gestión del suceso y otros aspectos a cargo del supervisor del turno, no son considerados en este planteamiento. El tratamiento de los turnos de operación y su gestión se trata, por ejemplo, en Gertman et al. (2005 2001) y O'Hara et al. (2004).

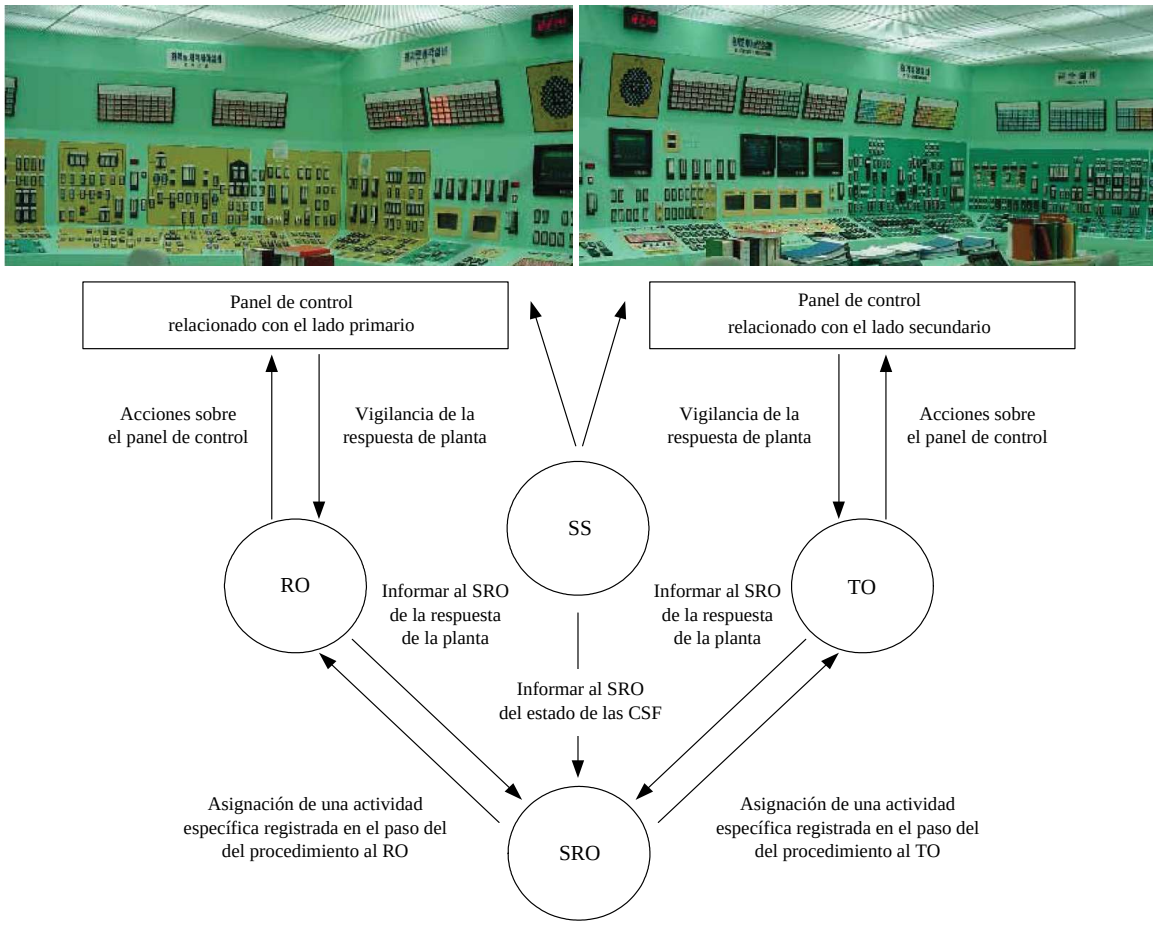


Figura 4.7: Distribución de tareas en la sala de control durante la gestión de emergencias, Park y Jung (2003b).

encargado del seguimiento de las CSF, los pasos de acción continua, la vigilancia del SPDS, la gestión del cambio de turno en colaboración con el supervisor del turno, y de realizar consideraciones generales en cuanto al seguimiento del transitorio, llegando a realizar recomendaciones en cuanto a los procedimientos a emplear en la gestión de la emergencia. Toda su actividad se canaliza, en este caso, a través del supervisor del turno, siendo éste el que supervisa la gestión de la emergencia y aprueba las decisiones realizadas por el SRO.

4.2 Herramientas para la computerización de los EOP

El conjunto de herramientas disponibles para la computerización de los EOP está condicionado por la elección del código de simulación de procedimientos, en este caso COPMA-III. Como ya se ha comentado en la Sección 2.2, dedicada a describir este simulador, el lenguaje empleado para la computerización de procedimientos es específico del núcleo y la PDB de COPMA-III, presentando estructura de tipo XML, denominándose a los fichero como procedimientos computerizados XPA. Sin embargo, considerando la posibilidad de desarrollar una herramienta de traducción sintáctica de cualquier lenguaje a XPA con relativa facilidad y la experiencia previa en la computerización de procedimientos empleando el lenguaje Prola, se consideró como mejor aproximación realizar la computerización en este lenguaje. Posteriormente, el grupo de desarrollo del sistema COPMA-III suministró una plantilla de traducción de los procedimientos Prola a estructuras XPA. De esta forma, el conjunto de herramientas necesario para la computerización de los procedimientos resultó ser, Figura 4.8:

- El editor PED-II para la computerización de los EOP en lenguaje Prola, sección 4.2.1.
- El desarrollo de un traductor Prola a Prola/XML y a XPA, compuesto de:
  - ANTLR (*ANother Tool for Language Recognition*), necesario para la conversión de formato de Prola a Prola/XML. Consiste en un analizador lexicográfico y sintáctico que se basa en gramáticas LL(k) el cual, a partir de unas reglas de un lenguaje predefinido, es capaz con convertir esa sintaxis a cualquier lenguaje, en nuestro caso a XML, Sección 4.2.2.
  - ANT en una aplicación Java para la ejecución de programas Java en cualquier entorno empleando sistemas de ficheros XML. En esta implementación se emplea para ejecutar el analizador ANTLR, Sección 4.2.2.
  - La aplicación SAXON, para la asignación de indentificadores únicos a los elementos del lengua Prola en formato XML. Es una aplicación similar a ANTLR pero con funcionalidad más avanzada, Sección 4.2.3
  - La librería de funciones CLIENTLIB del sistema COPMA-III, que empleando una plantilla de traducción de las sentencias traduce, en un principio, de cualquier lenguaje empleado en la computerización de los EOP al lenguaje propio del núcleo y la PDB de COPMA-III, Sección 4.2.4.

En las secciones siguientes se describen en detalle estas herramientas, la forma en que se han usado para computerizar los procedimientos y obtener las versiones adaptadas para su ejecución con el sistema COPMA-III.

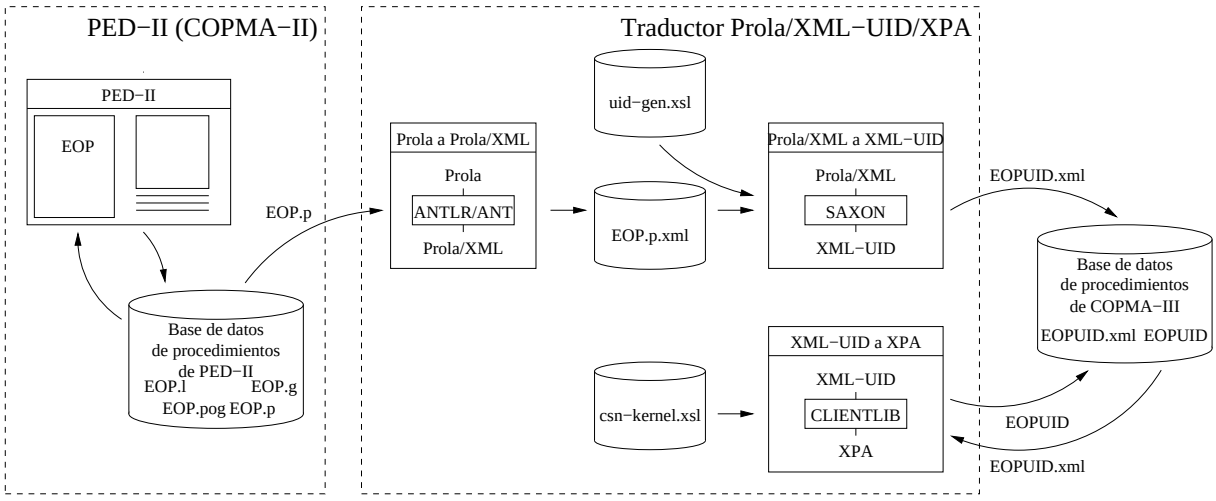


Figura 4.8: Esquema de la implementación del traductor Prola/XML/XPA.

4.2.1 El editor PED-II y el lenguaje Prola

Debido a que no es posible generar de forma automática la versión computerizada de los EOP[4], se ha empleado el editor PED-II para codificarlos en lenguaje Prola realizar modificaciones posteriores. Este editor forma parte del sistema COPMA-II, estando completamente desarrollado, Figura 4.9. Además, su funcionalidad es suficiente como para realizar versiones computerizadas de procedimientos de centrales nucleares, Veci (2000a).

Además de la edición de los EOP, el editor PED-II provee de las siguientes funciones:

- Comprobación de la sintaxis:

  Se produce una comprobación de la sintaxis cada vez que se edita una instrucción, ya sea de nueva creación o una modificación. Los errores detectados generan un aviso, indicando su localización. No se aceptan instrucciones que violen la normas de la sintaxis.

- Consistencia del flujo de control:

  Cuando se procede a salvar el procedimiento para guardarlo en la base de datos correspondiente, se notifican las inconsistencias existentes en el flujo de control (GOSUB, GOTO o INITIATE) cuyas direcciones todavía no existen, por ejemplo. Todas estas referencias a transiciones o implementadas en el flujo de control dentro del procedimiento pueden ser listadas con su localización exacta, para facilitar su corrección. Para que un procedimiento pueda ser cargado en el sistema COPMA-III no debe tener ninguna inconsistencia en el flujo de control.

[4]Existen algunos trabajos de implementación del sistema COPMA-III en distintos entornos, en los cuales se ha trabajado en esta línea, Hornaes y Hulsund (2001).

- Numeración de pasos e instrucciones:

  PED-II dispone de un sistema de numeración automático para instrucciones y pasos. También se permite elegir opcionalmente entre varias posibilidades, pero siempre se garantiza que el sistema usado es continuo y con incrementos secuenciales monótonos basados en números naturales.

  De esta manera resulta fácil identificar la estructura del procedimiento y permitir las transiciones en el flujo de control. Un identificador de paso localiza a éste dentro del procedimiento y un identificador de instrucción localiza a ésta dentro del paso. Cuando un procedimiento se modifica insertando un nuevo paso o instrucción en medio del procedimiento, los siguientes pasos o instrucciones son numeradas de nuevo automáticamente.

- Fácil representación de las condiciones de proceso:

  Las condiciones de proceso que aparecen en las instrucciones AUTOCHECK y MONITOR son complejas (incluyen términos AND, OR, NOT, etc.) y pueden ser difíciles de entender para el operador. Si están mal formuladas pueden resultar ambiguas. Una de las deficiencias más importantes y también más habituales en los procedimientos tradicionales es la existencia de expresiones lógicas pobremente estructuradas. Usando el integrador gráfico del editor, PED-II realiza una representación gráfica de dichas expresiones, a partir de símbolos para términos lógicos y puertas lógicas (AND, OR, y NOT), de tal modo que expresiones lógicas complejas pueden comprenderse con facilidad.

- Uso de etiquetas simbólicas para direccionar el flujo de control:

  Las instrucciones y los pasos puede llevar etiquetas, basadas en caracteres alfanuméricos, cuando se considere necesario al utilizar las instrucciones GOSUB, GOTO e INITIATE. El objeto del etiquetado es asegurarse de que dichas transiciones son fielmente respetadas incluso en los casos en que se hayan producido inserciones de pasos e instrucciones y las numeraciones hayan variado correlativamente. El uso de etiquetas garantiza el direccionamiento al lugar deseado con independencia del lugar de orden que ocupe en el procedimiento, en un momento determinado.

- Generación automática de un diagrama de flujo simplificado del procedimiento:

  Como se verá en la siguiente sección, PED-II genera automáticamente un fichero con la descripción del diagrama de flujo que representa el procedimiento en lenguaje Prola. Esta descripción puede ser usada para obtener una representación gráfica del procedimiento mediante un diagrama de flujo simplificado. Este hecho asegura la consistencia entre la versión de texto del procedimiento y su representación en diagrama de flujo.

Debido a que el editor PED-II es un editor gramatical y lógico de procedimientos computerizados, es decir, comprueba tanto la construcción como la relación lógica de los elementos, el producto resultante de su uso es una versión computerizada del procedimiento considerado, en texto Prola, consistente tanto estructural como en la lógica de sus elementos, fácilmente legible y preparado para ser interpretado por la herramienta de traducción a Prola/XML/XPA desarrollada al efecto.

A continuación, se explicarán en detalle el conjunto de ficheros que componen la versión computerizada de un procedimiento y que se engloban de forma genérica en la denominada base de datos de procedimientos del editor PED-II.

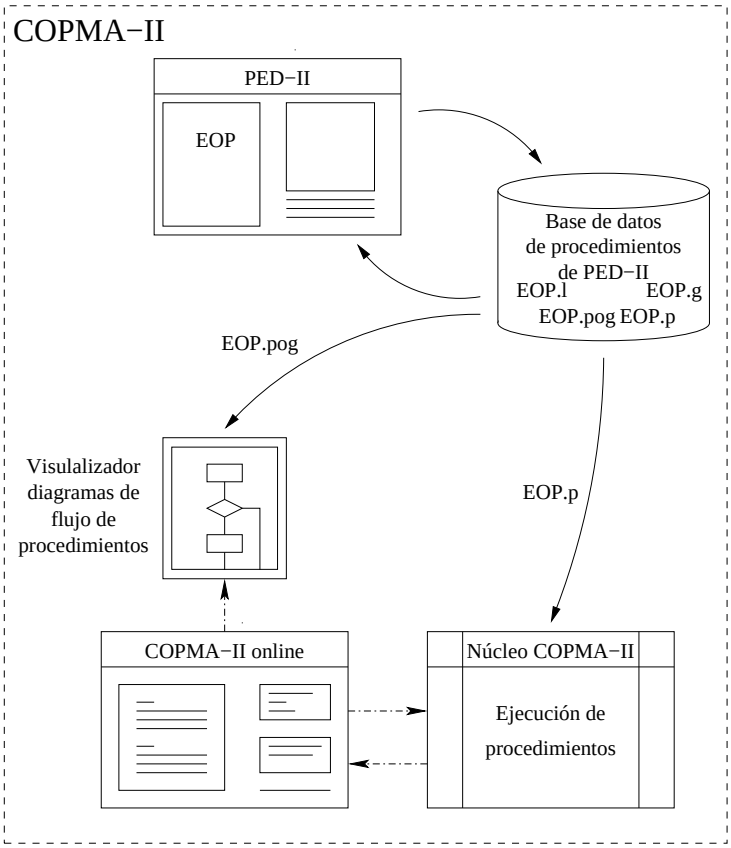


Figura 4.9: El editor PED-II y la base de datos de procedimientos del sistema COPMA-II.

4.2.1.1 Base de datos de procedimientos computerizados con PED-II

Durante la edición de los procedimientos con PED-II se generan, o actualizan si existen previamente, un conjunto de archivos que conforman la denominada base de datos de procedimientos. En el caso de su actualización, los archivos de la versión anterior se renombran secuencialmente con la extensión ’. X ’, donde X se corresponde con una secuencia de copia de seguridad de numeros naturales, comenzando por el uno.

En la operación de carga de un procedimiento mediante el editor PED-II se verifica la integridad de la información contenida en ellos, siendo condición indispensable para continuar con la edición del mismo. En este sentido, el mensaje de error suministrado por PED-II en la línea de comandos tras abortar su ejecución es lo suficiente explícito como para posibilitar la corrección del error detectado. Cabe destacar, como característica común de los cuarto archivos, que

son guardados en texto plano ASCII, lo que los hace manejables para su edición, impresión y búsqueda de errores.

Para cada procedimiento se guardan en la base de datos cuatro archivos:

- Archivo del procedimiento computerizado en Prola.
- Archivo de gráficos.
- Archivo de etiquetas.
- Archivo de estructura gráfica del procedimiento.

A continuación se detalla de forma concisa el contenido de estos archivos, adjuntando un ejemplo sencillo para cada uno de ellos.

4.2.1.1.1 Archivo del procedimiento computerizado en Prola

Este archivo tiene por extensión '.p'. En este archivo se encuentra codificada la versión Prola del procedimiento en su totalidad. Las estructuras lógicas desarrolladas de forma gráfica en las sentencias MONITOR y AUTOCHECK son traducidas e implementadas en lenguaje Prola en formato texto.

En la primera línea del archivo Prola del procedimiento, se encuentra registrado el estado de edición del mismo. Las etiquetas que identifican los diferentes estados posibles son:

- *ProcedureNotOK:ContainsLooseEndedReferences*

  Esta etiqueta se asocia con el procedimiento que contiene sentencias de referencia (tipo GOTO o GOSUB) a pasos o instrucciones aun no implementados en el procedimiento.

- *ProcedureNotOK:ContainsNonDeclaredRequieredOrOpcionalReferences*
- *ProcedureNotOK:ContainsLooseEndedExternalReferenceData*
- *ProcedureOK*

  No se han encontrado errores en el procedimiento en el momento de realizar la operación de guardado. Sólo en este caso el procedimiento está listo para ser usado por el traductor de Prola/XML/XPA.

El resultado final, al editar el archivo resultante, se puede comprobar en la Figura 4.10.

4.2.1.1.2 Archivo de gráficos

El archivo de gráficos tiene por extensión '.g'. El contenido del archivo son los gráficos asociados con las validaciones lógicas de las sentencias MONITOR y AUTOCHECK, guardados de forma vectorial. En la cabecera del archivo se suministra la estructura de los registros del mismo. Se pueden distinguir dos elementos, uno de ellos el correspondiente con los elementos lógicos (AND, OR,...) y el otro con la relación entre ellos. A cada gráfico vectorial le precede el paso y la instrucción a la que pertenece.

Como ejemplo se muestra el contenido del archivo gráfico correspondiente al procedimiento que sirvió para ilustrar el apartado anterior, Figura 4.11. Por ello, sólo se puede observar un gráfico vectorial correspondiente a la sentencia AUTOCHECK del paso uno.

4.2.1.1.3 Archivo de etiquetas

La extensión de este archivo es '.l'. El contenido del archivo es un registro secuencial, según estructura del procedimiento, de las etiquetas empleadas para cada paso y las correspondientes a las instrucciones que integran el mismo, Figura 4.12. Las etiquetas sólo son empleadas por PED-II, por lo que este archivo no es usado por COPMA-III.

4.2.1.1.4 Archivo de estructura gráfica del procedimiento

El archivo tienen por extensión '.pog'. La información contenida en este archivo se corresponde con la empleada por COPMA-II On-line para mostrar la estructura gráfica del procedimiento en la ventana *Flowchart page* al iniciar una actividad asociada al mismo, Figura 4.13.

```
************************************************************************
ProcedureOK
************************************************************************
PROCEDURE chkPED-II "Prueba de PED-II"

DESCRIPTION "Prueba de edición de ficheros generados por PED-II"

STEP 1 "Ejemplo de instrucción AUTOCHECK"
   INSTRUCTION 1 "Ejemplo de instrucción AUTOCHECK"
      AUTOCHECK
      IF     (     CHPU1 IS RUNNING
               AND CHPU2 IS STOPPED
               AND CHPU3 IS RUNNING )
         AND
         NOT (     CNTPR > 12.0
               OR  PZRL <= 2.0 )
      THEN
         GOTO 2 1
      COMMENT "Paso de prueba de la instrucción AUTOCHECK"
STEP 2 "Ejemplo de la instrucción ACTION"
   INSTRUCTION 1 "Ejemplo de la instrucción ACTION"
      ACTION
      START CHPU2
      STOP RCSPU1
STEP 3 ""
   INSTRUCTION 1 "Final"
      FINISH
ENDPROCEDURE
```

Figura 4.10: Ejemplo de archivo Prola de la base de datos de procedimientos de PED-II.

```
************************************************************************
FORMAT: STEP <step-id> INSTR <instruction-id>
        LI <logic-element-id> T <type> X <x-pos> Y <y-pos> W <width> H <height>
        LI <logic-element-id> IT <input-term-no> CLI <conn-logic-elem-id> \
           CCL <connection-coordinates-list(x y)>
************************************************************************
STEP         1 INSTR      1
  LI  1 T    E X   189 Y    90  W   15    H   10
  LI  1 IT   1 CLI  P2 CCL (  184   95  189   95 )
  LI  2 T    A X   154 Y    42  W   30    H   78
  LI  2 IT   1 CLI  P3 CCL (   76   56  141   56  154   82 )
  LI  2 IT   2 CLI  P7 CCL (  117  141  141  141  154  106 )
  LI  3 T    A X    46 Y    10  W   30    H   93
  LI  3 IT   1 CLI  I4 CCL (   20   20   46   19 )
  LI  3 IT   2 CLI  I5 CCL (   20   55   46   54 )
  LI  3 IT   3 CLI  I6 CCL (   20   90   46   90 )
  LI  7 T    N X    87 Y   116  W   30    H   50
  LI  7 IT   1 CLI  P8 CCL (   76  141   87  140 )
  LI  8 T    O X    46 Y   116  W   30    H   50
  LI  8 IT   1 CLI  I9 CCL (   20  125   46  125 )
  LI  8 IT   2 CLI I10 CCL (   20  160   46  161 )
```

Figura 4.11: Ejemplo de archivo gráfico de la base de datos de procedimientos de PED-II.

```
*************************************************************************
FORMAT (def): <step-id> {<instruction-id>} LBL <label> or (ref):
<step-id>+<instruction-id>{+THEN/+ELSE} \
                STEP <step-label> {INSTR <instr-label>}
*************************************************************************
              1     LBL InstAutocheck
              1   1 LBL AUTOCHECK
              2     LBL InsACTION
              2   1 LBL ACTION
              3     LBL Final
              3   1 LBL Final
```

Figura 4.12: Ejemplo de archivo de etiquetas de la base de datos de procedimientos de PED-II.

```
*************************************************************************
FORMAT: S <step-id> <step-name> <def-ctr-flow-id> \
          \{<branch-instr-type> \{<branch-instr-adr>\}\}* \
          <act-lvl-arrow-id> <proc-lvl-arrow-id> <no-of-branch-instr-text-lines>
        I <instr-id> \{<instr-name>\} <instr-type> <def-ctr-flow-id> \
          \{<branch-instr-type> \{<branch-instr-adr> \{<branch-instr-lbl>\}\}\}* \
          <act-lvl-arrow-id> <proc-lvl-arrow-id> <no-of-instr-text-lines>
*************************************************************************
S 1 "Ejemplo de instrucción AUTOCHECK" 1 L 2 0 2 1 I 1 "Ejemplo de
instrucción AUTOCHECK" C 2 O 2 1 T 0 2 1

S 2 "Ejemplo de la instrucción ACTION" 2 A 1 0 1 1 I 1 "Ejemplo de
la instrucción ACTION" F 2 B 1 1 0 1 1

S 3 "" 3 G 2 0 1 I 1 "Final" G 3 G 2 0 1
```

Figura 4.13: Ejemplo de archivo de estructura gráfica del procedimiento de la base de datos de procedimientos de PED-II.

4.2.1.2 El lenguaje Prola

El editor PED-II está directamente basado en el uso del lenguaje Prola (*Procedure Language*), que fue desarrollado como parte de las primeras versiones del sistema COPMA, dentro del Halden Reactor Project, HRP (1995).

Se trata de un lenguaje de propósito general que intenta servir a toda clase de procedimientos. En muchos casos, aplicar el lenguaje Prola requiere transformar algunas partes de los procedimientos para que sean más explícitas, sobre todo en lo referente a una mejor identificación de las señales de proceso, dentro de los procedimientos y componentes.

La estructura principal de un procedimiento Prola es simple, describiéndose a continuación los componentes más importantes de dicho lenguaje:

- Cada procedimiento debe tener un identificador breve y único a decisión del usuario. Este identificador debe reflejar una categorización dentro de los procedimientos, que facilitará su búsqueda. Además llevará un nombre corto y descriptivo, y opcionalmente una descripción más amplia. En el momento de la codificación de estos campos, su contenido debe orientarse para que aporte la mayor cantidad de información posible respecto al objetivo del paso en ejecución. Este punto es de importancia vital para dotar de una mayor legibilidad a la estructura del procedimiento durante su ejecución, de forma que se facilite la interpretación del proceso de ejecución y la funcionalidad de cada paso.

- El cuerpo del procedimiento podrá contener el número de pasos que se desee. Cada paso consiste en un número cualquiera de instrucciones. Para conseguir una estructura adecuada es aconsejable que cada paso contenga un conjunto de instrucciones relacionadas entre sí y seleccionar un nombre que refleje el propósito del paso. Se buscará, a su vez, que a cada paso implementado para COPMA-III se relacione de forma unívoca con un paso del procedimiento original, de forma que facilite su seguimiento.

- Este lenguaje de procedimientos contiene doce tipos diferentes de instrucciones, de las cuales únicamente diez son aplicables a los objetivos del trabajo realizado,

  1. ACTION:

     Se usa para especificar una o más acciones/manipulaciones discretas que deben ser ejecutadas sobre algún componente específico del sistema simulado. Las acciones serán ejecutadas por el núcleo de COPMA-III en el orden que se han establecido en los pasos computerizados.

  2. AUTOCHECK:

     Se usa para puntos de decisión existentes en el procedimiento cuya resolución depende de una condición que es combinación lógica y/o algebraica de variables físicas del proceso y/o estado de componentes del sistema, de los suministrados por el simulador de planta a través de la interfase de conexión. La condición puede ser evaluada automáticamente por el núcleo de COPMA-III y, según que el resultado o conclusión sea verdadero o falso, el flujo de control se dirigirá hacia los puntos indicados mediante instrucciones del tipo GOSUB, GOTO e INITIATE.

3. FINISH:
   Finaliza la actividad en curso. El concepto de actividad se presentó en la Sección 2.2.
4. GOSUB:
   Origina un salto en el flujo de control a una instrucción específica del procedimiento. Esta instrucción específica debería ser la primera de una secuencia de instrucciones que constituyen una subrutina dentro del procedimiento. Una vez finalizada dicha secuencia debe seguirle la instrucción RETURN para retornar el flujo de control a la instrucción siguiente a aquella que generó la llamada a GOSUB.
5. GOTO:
   Origina un salto en el flujo de control a una instrucción específica del procedimiento, cuando no es necesario el retorno automático al punto de partida.
6. INITIATE:
   Esta instrucción se usa para especificar al núcleo de COPMA-III que cargue automáticamente, si no está cargado ya, un procedimiento específico desde la base de datos de los procedimientos e inicie una nueva actividad para su ejecución, asociada con este procedimiento.
7. MESSAGE:
   Presenta en pantalla un mensaje (por ejemplo una precaución, un tiempo de espera o una nota) para el operador.
8. MONITOR:
   Similar a AUTOCHECK solo que la condición específica es continuamente vigilada por el núcleo de COPMA-III durante un intervalo de tiempo especificado. Este intervalo de tiempo tiene que determinarse o con límites de tiempo específicos, o usando condiciones de proceso lógicas, o bien con una combinación entre ambas formas. Una vez iniciada la vigilancia el operador puede proseguir la ejecución del procedimiento, ya que dicha vigilancia la está realizando el núcleo de COPMA-III. Tanto si se detecta que la condición se cumple dentro del intervalo de tiempo especificado, como si no se ha cumplido al finalizar el mismo, se produce una notificación al operador. Cuando el operador inspecciona una conclusión de la instrucción MONITOR puede proceder a la ejecución de la instrucción INITIATE que figura en la parte conclusa de la instrucción.
9. RETURN:
   Origina el retorno del flujo de control a la primera instrucción que sigue al último GOSUB ejecutado.
10. WAIT:
    Intenta prevenir al operador respecto de la instrucción siguiente en relación con algún intervalo de tiempo que debe esperar. Este intervalo de tiempo tiene que determinarse o con límites de tiempo específicos, o usando condiciones de proceso lógicas, o bien con una combinación de ambas. El operador puede abortar o saltar cualquier instrucción WAIT si lo considera necesario.

Prola:

```
 INSTRUCTION 2
    ACTION
    CLOSE VAL01
    COMMENT "TEXEC = 60  TASKLOAD = 33"
```

XML:

```
<INSTRUCTION number="2">
    <ACTION>
    <CLOSE> VAL01</CLOSE>
    <COMMENT> TEXEC = 60  TASKLOAD = 33
    </COMMENT>
    </ACTION>
</INSTRUCTION>
```

Figura 4.14: Similitud del formato Prola de PED-II y la estructura XML asociada.

4.2.2 Conversión de los procedimientos en lenguaje Prola a Prola basado en estructuras XML

Mientras que el editor PED-II computeriza los procedimientos en lenguaje Prola, en COPMA-III se utiliza una estructura de etiquetas XML con una implementación de elementos léxicos propios del núcleo del sistema de COPMA-III. A diferencia del caso del lenguaje Prola, en el sistema COPMA-III no existe un editor específico para los procedimientos en XML con léxico Prola, aunque si un traductor de estos procedimientos al léxico propio del núcleo de COPMA-III. Por ello, el equipo del HRP desarrolló un conversor del lenguaje Prola en formato libre al formato de estructuras propio del XML. La complejidad de la conversión es reducida, debido principalmente a que todos los elementos del lenguaje Prola se caracterizan por una estructura bien definida de fácil traducción a elementos XML, Figura 4.14. Por ello, basta implementar un conjunto de reglas que convierta las etiquetas de Prola a etiquetas en forma XML, y emplear un intérprete que las aplique.

En la implementación del conversor actual se emplean dos aplicaciones, Figura 4.15:

- ANTLR.
- ANT.

Ambas aplicaciones tienen licencia *Open Source*, pudiéndose descargar a través de internet accediendo a las direcciones *http://www.antlr.org/* y *http://ant.apache.org/*, respectivamente. A continuación, se describen estas utilidades así como de su forma de uso.

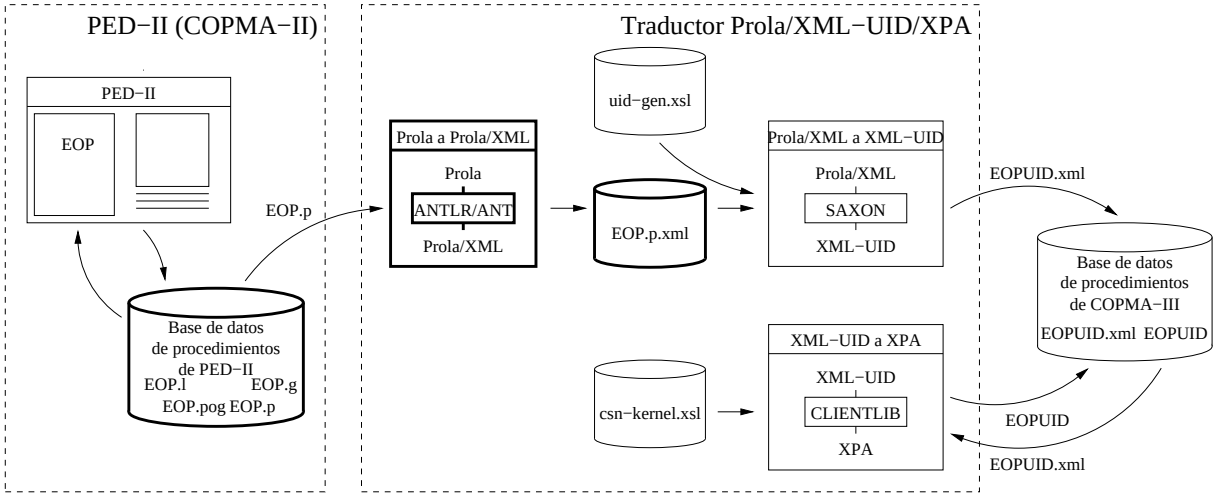


Figura 4.15: Esquema de fases de traducción de los procedimientos: conversión de Prola a Prola-XML.

4.2.2.1 ANTLR

ANTLR es un analizador lexicográfico y sintáctico que se basa en gramáticas LL(k) el cual, a partir de unas reglas de un lenguaje predefinido es capaz con convertir esa sintaxis a cualquier lenguaje, en nuestro caso a XML . ANTLR es un compilador diseñado para desarrolladores que quieren crear un traductor sintáctico. Las partes fundamentales de las que se compone este analizador lexicográfico son el scanner sintáctico (*lexer*) y el analizador sintáctico (*parser*).

4.2.2.1.1 El scanner sintáctico (*lexer*)

Los lenguajes de programación están compuestos por palabras claves y estructuras bien definidas. El objetivo final del proceso de compilación es traducir esas instrucciones de alto nivel propias del lenguaje de programación, a instrucciones de bajo nivel en lenguaje máquina o a un lenguaje de máquina virtual, necesario para la ejecución de nuestro código en una determinada arquitectura hardware. Por ejemplo, un compilador de C++ compila el código y lo traduce a lenguaje máquina para que pueda ser ejecutado sobre una plataforma hardware específica. El compilador de Java distribuido por Sun Microsystems, compila el código Java a un código máquina virtual, que es luego interpretado por la máquina virtual de Java. Este código de máquina virtual puede ser interpretado por cualquier plataforma que tenga instalada una máquina virtual de Java. El código de un programa se escribe utilizando editores de texto que nos permiten escribir las sentencias y estructuras propias del lenguaje. De esta manera, podemos considerar nuestro fichero, donde hemos escrito el código, como un conjunto de caracteres escritos en un determinado orden que terminan con el carácter EOF (End Of File). Este fichero fuente es introducido, como parámetro de entrada al scanner de sintaxis (*lexer*). El trabajo de este scanner es simplemente el de traducir este conjunto de caracteres en otro grupo de caracteres que van a

tener un significado para la siguiente fase del proceso que va a ser llevada a cabo por el *parser*. Esta modificación de la información contenida en el código fuente se realiza gracias a las reglas sintácticas que previamente se hayan definido para el *lexer*

4.2.2.1.2 El analizador sintáctico (*parser*)

El *parser* comprueba si este nuevo grupo de sentencias son correctas dentro de la nueva gramática que hemos definido (en nuestro caso si el código generado es código XML correcto). Además, el *parser* es el responsable de informar de cualquier tipo de falta de significado que pueda existir en el nuevo código generado, por ejemplo, una llamada a una función que no existe, o una función que nunca es ejecutada. Cualquier error gramatical que se detecte dentro del nuevo fichero también será informado gracias al *parser*.

4.2.2.2 ANT

ANT es una herramienta del proyecto Jakarta de Apache que se puede definir como un equivalente de make, para los desarrolladores Java, aunque debido a su implementación nada impide usarlo con otros lenguajes. Como se ha mencionado en la introducción, ANT es un código abierto y está disponible a través de internet, entre las ventajas que presenta están que usa XML como formato de sus ficheros, que esta escrito en Java por lo cual se tienen las ventajas de la multiplataforma, no haciendo falta un fichero de procesamiento por lotes para cada sistema operativo, y que es fácilmente extensible e integrable con muchas herramientas.

Un fichero ejecutable (un sencillo .bat en Windows, o un .sh en GNU/Linux) para que realice todo el proceso de ejecución y compilación de un programa necesita por ejemplo, actualizar el classpath, compilar el código, copiar algunas clases compiladas a otro directorio y generar la documentación con javadoc. Algunos IDE hacen gran parte de estas tareas, pero no en una única fase.

Para trabajar con ANT se necesitan tres elementos:

1. La propia aplicación ANT.
2. El entorno JDK, ya que ANT no deja de ser una aplicación Java.
3. Un *parser* XML, sin importar cual, teniendo la propia instalación de la aplicación uno. Es necesario pues ANT se basa en ficheros XML para su configuración.

4.2.2.2.1 El fichero build.xml

ANT se basa en ficheros XML, por ello normalmente se configura el trabajo a realizar con nuestra aplicación en un fichero llamado build.xml. Las etiquetas más importantes necesarias para el fichero build.xml son project, target, task y property,

- *Project*.

  Este es el elemento raíz del fichero XML, y como tal, sólo puede haber uno en todo el fichero, el que se corresponde a nuestra aplicación Java.

- *Target*.

  Un *target* u objetivo es un conjunto de tareas (ver el siguiente elemento, *task*) que queremos aplicar a nuestra aplicación en algún momento. Se puede hacer que unos objetivos dependan de otros, de forma que eso lo trate ANT automáticamente.

- *Task*.

  Un *task* o tarea es un código ejecutable que aplicaremos a nuestra aplicación, y que puede contener distintas propiedades (como por ejemplo el *classpath*). ANT incluye ya muchas básicas, como compilación y eliminación de ficheros temporales, pero podemos extender este mecanismo si nos hace falta. Luego veremos algunas de las disponibles.

- *Property*.

  Una propiedad o *property* es simplemente algún parámetro (en forma de par nombre-valor) que necesitamos para procesar nuestra aplicación, como el nombre del compilador, etc. ANT incluye ya las más básicas, como son BaseDir para el directorio base de nuestro proyecto, ant.file para el path absoluto del fichero build.xml, y ant.java.version para la versión de la JVM.

4.2.2.2.2 Ejemplo de fichero build.xml

A continuación se muestra un ejemplo de cómo sería un fichero build.xml,

```
<?xml version="1.0"?>

<project name="ProbandoAnt"default="compilar" basedir=".">

<!-- propiedades globales del proyecto -->

<property name="fuente" value="." />
```

Este sencillo fichero requiere poca explicación, simplemente declaramos el proyecto indicando la acción a realizar por defecto (`default=çompilar"`), e indicamos que el directorio base es el actual (`basedir="."`). Después se indica en sendas etiquetas property los directorios de origen y de destino (property name="fuente"value=".", y property name="destino"value=çlasses"), y por ultimo declaramos un target llamado `compilar`, que es el que se ha declarado como por defecto. En este objetivo tenemos una única tarea, la de compilación java, a la que por medio de los atributos srcdir y destdir le indicamos los directorios fuente y destino, que recogemos de las propiedades anteriormente declaradas con ${fuente} y {destino}. Bien, lo único que queda

es compilar el código, así que simplemente, estando situados en el directorio donde se tiene el build.xml, desde una ventana de comandos DOS o terminal GNU/Linux se puede ejecutar el siguiente comando:

```
%PATH_TO_ANT%\ant
```

donde `%PATH_TO_ANT%`representa el path absoluto de la aplicación ANT, al haberse declarado `compilar` como el objetivo por defecto. La regla general sería,

```
\%PATH_TO_ANT\%\ant nombre_objetivo
```

4.2.3 Paso de asignación de UID a la estructura XML Prola mediante SAXON

El fichero convertido de léxico Prola y estructura XML que se obtiene con el conversor no es de utilidad para el sistema COPMA-III porque el cliente MMI, el núcleo y el PDB usan estructuras XML con etiquetas únicas de elementos para el intercambio de información de forma coherente, identificando de forma unívoca los diferentes elementos de los procedimientos. Para la generación de las etiquetas únicas de los elementos de los procedimientos, denominadas UID, se emplea la herramienta SAXON con un motor de traducción del XML al XML con etiquetas UID, suministrado por el equipo del HRP, denominado uid-gen.xsl, Figura 4.16.

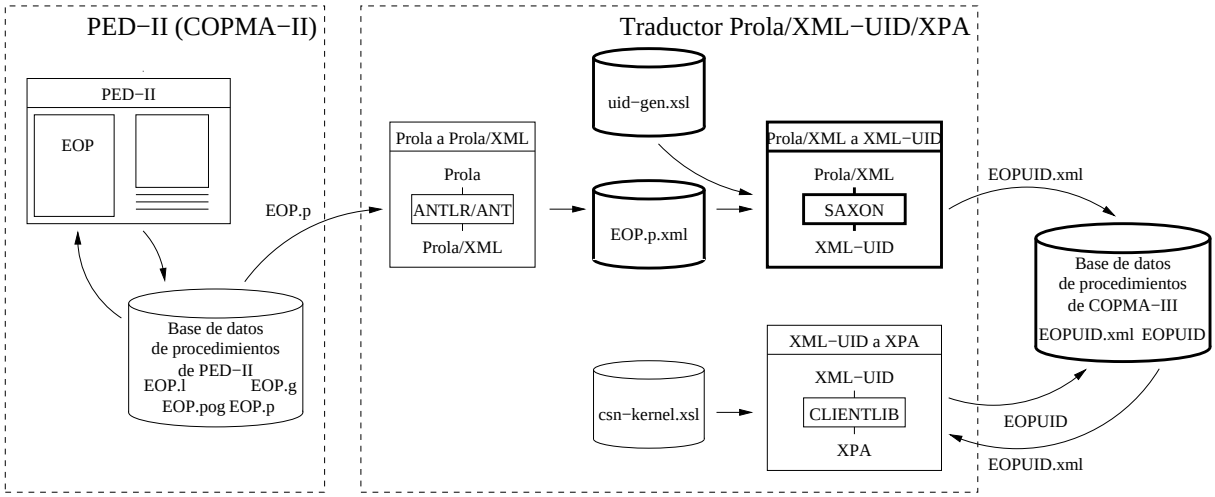


Figura 4.16: Esquema de fases de traducción de los procedimientos: adición de las etiquetas UID a la estructura Prola-XML.

El paquete de software SAXON es un conjunto de herramientas para procesar documentos XML. Sus principales componentes son:

- Un procesador XSLT, que emplea la hoja de estilos uid-gen.xsl suministrada por el HRP para incorporar las UID en la estructura XML Prola.
- Una versión mejorada del parser Ælfred, que determina la estructura del fichero XML Prola para posibilitar que el procesador XSLT incluya las UID en la estructura del fichero.
- Una librería de funciones Java.

4.2.4 Traducción del léxico Prola al propio del sistema COPMA-III mediante CLIENTLIB

Finalmente, el léxico Prola no es interpretable ni por el núcleo ni por la PDB del sistema COPMA-III, siendo necesaria la traducción a elementos lógicos propios del núcleo de COPMA-III. Para ello se emplea una plantilla de traducción de las sentencias del lengua Prola a la suministrada por el equipo del HRP, denominada csn-kernel.xsl, realizándose la traducción con el conjunto de funciones implementadas en la librería CLIENTLIB del sistema COPMA-III, Figura 4.17.

En el apartado siguiente se explica la aplicación del conjunto de herramientas que conforman el traductor del sistema COPMA-III para obtener los procedimientos en el formato requerido.

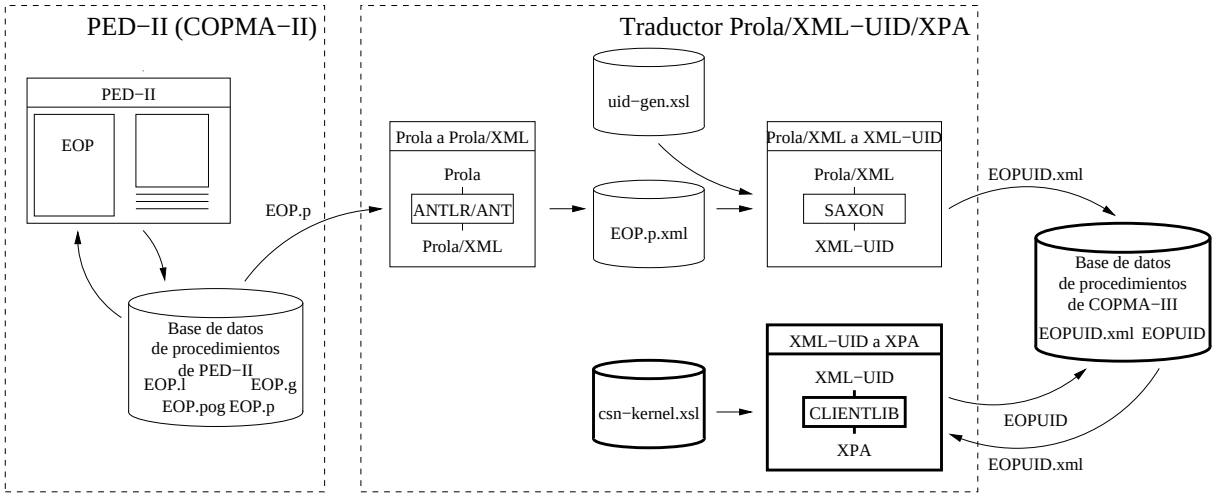


Figura 4.17: Esquema de fases de traducción de los procedimientos: traducción de la estructura Prola-XML con las UID a XPA.

4.2.5 Ejemplo de conversión de fichero Prola a XML

La traducción automática de un procedimiento Prola se puede realizar mediante un fichero de proceso por lotes del sistema operativo Windows que constase de los siguientes pasos:

- Conversión del lenguaje Prola a estructura XML.

  Primero se convierte el fichero Prola de estructura libre, a un fichero que conserva el léxico Prola pero se estructura siguiendo el estándar del lenguaje XML, Figura 4.18. Este fichero sería el punto de partida si se editasen directamente los procedimientos en XML. Consiste en código XML con una serie de etiquetas XML, e incluyendo los parámetros TEXEC y TASKLOAD perfectamente identificados como propiedades de cada instrucción del procedimiento.

  El comando a ejecutar sería:

  ```
  ant -DprolaFile="nombre_fichero_prola" run
  ```

  generando el fichero intermedio nombre_fichero_prola.p.xml.

- Generación de los elementos de identificación únicos (UID).

  Este fichero intermedio XML todavía no es de utilidad para el sistema COPMA-III porque el cliente MMI, el núcleo y el PDB usan estructuras XML con etiquetas únicas de elementos para el intercambio de información de forma coherente, es decir, con cierta sincronización. En este paso se generan las etiquetas únicas, denominadas UID, en los elementos de la estructura XML. A partir del fichero intermedio XML se obtiene una versión similar pero con el conjunto de etiquetas UID que identifican cada elemento del procedimiento, Figura 4.19. Para la generación de las etiquetas se requiere de un motor de traducción del fichero Prola en formato XML al XML con etiquetas UID, suministrado por el equipo del HRP, y denomiando uid-gen.xsl.

  El comando requerido para realizar esta acción es:

  ```
  java -classpath c:/saxon/saxon.jar;c:/saxon com.icl.saxon.StyleSheet
  -o nombre_fichero_prolaUID.xml nombre_fichero_prola.p.xml
  uid-gen.xsl
  ```

  que genera el fichero XML nombre_fichero_prolaUID.xml. Esta versión del procedimiento XML con UID ya es aplicable al MMI del sistema COPMA-III, quedando obtener la estructura XPA para el núcleo y la PDB.

- Obtención de la estructura XPA del procedimiento XML con UID.

  Finalmente, resta el paso de obtención de las estructuras XPA necesarias para el núcleo y la PDB del sistema COPMA-III. Estas estructuras XPA son ficheros de estructura XML con las mismas UID que la versión XML del procedimiento pero con elementos lógicos

propios del núcleo de COPMA-III, Figura 4.20. La conversión de los elementos Prola a elementos del núcleo se realiza mediante motor de generación de las estructuras XPA a partir del procedimiento XML UID suministrado por el equipo del HRP, denominado Csn-kernel.xsl.

El comando a ejecutar es:

```
java -cp C:\copma1_1\lib\ClientLib.jar ClientLib.MMITransform -o
nombre_fichero_prolaUID nombre_fichero_prolaUID.xml csn-kernel.xsl
```

obteniendo el fichero de estructura XPA nombre_fichero_prolaUID. Este fichero es el empleado por el núcleo y la PDB para ejecutar y realizar el seguimiento de la ejecución del procedimiento, respectivamente.

En Quiroga et al. (2006), se incluyen los motores de traducción empleados y suministrados por el equipo del HRP, así como el fichero de configuración de la aplicación ANT.

```
STEP 2 "XXXX XX"

   INSTRUCTION 1 "YYYY YY"

      AUTOCHECK

      IF     (     VALENT.opStatus IS CLOSED
               OR  VALSAL.opStatus IS OPEN )
         AND SIMTIME.value > 1000.0
         AND MASA.value < 0.0
      THEN
         GOTO 3 1
      ELSE
         GOTO 5 1
```

```
<STEP id="2" longid="XXXX XX">
- <INSTRUCTION num="1" longid="YYYYYY">
- <AUTOCHECK>
- <IF>
- <AND>
- <AND>
- <OR>
- <EQ>
  <Id>VALENT.opStatus</Id>
  <VALUE val="CLOSED" />
  </EQ>
- <EQ>
  <Id>VALSAL.opStatus</Id>
  <VALUE val="OPEN" />
  </EQ>
  </OR>
- <GT>
  <Id>SIMTIME.value</Id>
  <VALUE val="1000.0" />
  </GT>
  </AND>
- <LT>
  <Id>MASA.value</Id>
  <VALUE val="0.0" />
  </LT>
  </AND>
  </IF>
- <THEN>
  <GOTO id="3" from="1" />
  </THEN>
- <ELSE>
  <GOTO id="5" from="1" />
  </ELSE>
  </AUTOCHECK>
  </INSTRUCTION>
  </STEP>
```

Figura 4.18: Ejemplo de conversión de Prola (izquierda) a Prola con estructura XML (derecha).

```
<STEP id="2" longid="XXXX XX">
- <INSTRUCTION num="1" longid="YYYYYY">
- <AUTOCHECK>
- <IF>
- <AND>
- <AND>
- <OR>
- <EQ>
  <Id>VALENT.opStatus</Id>
  <VALUE val="CLOSED" />
  </EQ>
- <EQ>
  <Id>VALSAL.opStatus</Id>
  <VALUE val="OPEN" />
  </EQ>
  </OR>
- <GT>
  <Id>SIMTIME.value</Id>
  <VALUE val="1000.0" />
  </GT>
  </AND>
- <LT>
  <Id>MASA.value</Id>
  <VALUE val="0.0" />
  </LT>
  </AND>
  </IF>
- <THEN>
  <GOTO id="3" from="1" />
  </THEN>
- <ELSE>
  <GOTO id="5" from="1" />
  </ELSE>
  </AUTOCHECK>
  </INSTRUCTION>
  </STEP>
```

```
- <STEP uid="d0e14" id="2" longid="XXXX XX">
- <INSTRUCTION uid="d0e16" num="1" longid="YYYY YY">
- <AUTOCHECK uid="d0e18">
- <IF uid="d0e19">
- <AND uid="d0e20">
- <AND uid="d0e21">
- <OR uid="d0e22">
- <EQ uid="d0e23">
  <Id uid="d0e24">VALENT.opStatus</Id>
  <VALUE uid="d0e26" val="CLOSED" />
  </EQ>
- <EQ uid="d0e28">
  <Id uid="d0e29">VALSAL.opStatus</Id>
  <VALUE uid="d0e31" val="OPEN" />
  </EQ>
  </OR>
- <GT uid="d0e33">
  <Id uid="d0e34">SIMTIME.value</Id>
  <VALUE uid="d0e36" val="1000.0" />
  </GT>
  </AND>
- <LT uid="d0e37">
  <Id uid="d0e38">MASA.value</Id>
  <VALUE uid="d0e40" val="0.0" />
  </LT>
  </AND>
  </IF>
- <THEN uid="d0e41">
  <GOTO uid="d0e42" id="3" from="1" />
  </THEN>
- <ELSE uid="d0e43">
  <GOTO uid="d0e44" id="5" from="1" />
  </ELSE>
  </AUTOCHECK>
  </INSTRUCTION>
  </STEP>
```

Figura 4.19: Ejemplo de conversión de Prola con estructura XML (izquierda) a Prola XML con UID (derecha).

```
- <STEP uid="d0e14" id="2" longid="XXXX XX">
- <INSTRUCTION uid="d0e16" num="1" longid="YYYY YY">
- <AUTOCHECK uid="d0e18">
- <IF uid="d0e19">
- <AND uid="d0e20">
- <AND uid="d0e21">
- <OR uid="d0e22">
- <EQ uid="d0e23">
  <Id uid="d0e24">VALENT.opStatus</Id>
  <VALUE uid="d0e26" val="CLOSED" />
  </EQ>
- <EQ uid="d0e28">
  <Id uid="d0e29">VALSAL.opStatus</Id>
  <VALUE uid="d0e31" val="OPEN" />
  </EQ>
  </OR>
- <GT uid="d0e33">
  <Id uid="d0e34">SIMTIME.value</Id>
  <VALUE uid="d0e36" val="1000.0" />
  </GT>
  </AND>
- <LT uid="d0e37">
  <Id uid="d0e38">MASA.value</Id>
  <VALUE uid="d0e40" val="0.0" />
  </LT>
  </AND>
  </IF>
- <THEN uid="d0e41">
  <GOTO uid="d0e42" id="3" from="1" />
  </THEN>
- <ELSE uid="d0e43">
  <GOTO uid="d0e44" id="5" from="1" />
  </ELSE>
  </AUTOCHECK>
  </INSTRUCTION>
  </STEP>
```

```
<ExecutableUnit name="2-1" uid="d0e16">
<Output>
<TextNode Text="d0e16;"/>
<IPRef/>
<TextNode Text="; started ClientApplet"/>
</Output>
<Condition uid="d0e18">
<And uid="d0e20">
<And uid="d0e21">
<Or uid="d0e22">
<Equals uid="d0e23">
<Input type="RunTime"
Variable="VALENT.opStatus" From="PDB"/>
<TextNode uid="d0e26" Text="CLOSED"/>
</Equals>
<Equals uid="d0e28">
<Input type="RunTime"
Variable="VALSAL.opStatus" From="PDB"/>
<TextNode uid="d0e31" Text="OPEN"/>
</Equals>
</Or>
<Greater uid="d0e33">
<Input type="RunTime"
Variable="SIMTIME.value" From="PDB"/>
<TextNode uid="d0e36" Text="1000.0"/>
</Greater>
</And>
<Less uid="d0e37">
<Input type="RunTime"
Variable="MASA.value" From="PDB"/>
<TextNode uid="d0e40" Text="0.0"/>
</Less>
</And>
<GoTo REF="3-1">
<TextNode Text="3-1"/>
</GoTo>
<GoTo REF="5-1">
<TextNode Text="5-1"/>
</GoTo>
</Condition>
</ExecutableUnit>
```

Figura 4.20: Ejemplo de conversión de Prola XML con UID (izquierda) a XPA de COPMA-III (derecha).

4.3 Metodología de computerización de EOP de un PWR-W

Una de las tareas de mayor importancia durante este trabajo ha sido el desarrollo de una metodología de computerización de EOP que a su vez abarque su integración con el simulador de planta. Para su realización, se ha aprovechado la experiencia previa de otros trabajos, pudiendo citarse:

- Proyecto de computerización de los EOP de CN José Cabrera (PWR-W), llevado a cabo por el CSN. En este proyecto se realizó la computerización de algunas de las ORG de la central empleando el editor PED-II (E-0, E-3, ES-01 y ES-02). Las actividades desarrolladas durante el proyecto quedaron ampliamente documentadas en las referencias Veci (2000ab 1993 1994ab 1995).
- Proyecto de computerización de los EOP de CN Cofrentes (BWR-GE), colaboración entre el CSN y el DSE, Triviño et al. (1997) y Queral y García (1997). Los procedimientos computerizados fueron:
  - EOP-1-RC: Procedimiento de control del reactor.
  - EOP-1-RC/Q: Control de potencia del reactor.
  - EOP-1-RC/L: Control de nivel del reactor.
  - EOP-1-RC/P: Control de presión del reactor.
  - EOP-2-RC/P: Procedimiento simplificado de control de presión del reactor (EOP-1-RC/P).
  - EOP-C1. Contingencia 1: Control alternativo de nivel.
  - EOP-C2. Contingencia 2: Despresurización de emergencia de la RPV.
  - EOP-C3. Contingencia 3: Refrigeración del núcleo por vapor.
  - EOP-C4. Contingencia 4: Inundación de la RPV.
  - BWR6-EOP-0: Procedimiento general de vigilancia.
  - BWR6-EOP-SBO: Station Blackout (SBO).

Gracias a esta experiencia previa del departamento MOSI del CSN y del DSE, se dispuso de suficiente información como para desarrollar la nueva metodología orientada al uso del del sistema COPMA-III y el empleo del lenguaje Prola. Este trabajo se realizó en el DSE de la UPM en el marco de dos proyectos de investigación financiados por el CSN, orientados a las tecnologías PWR-W (2002-2004), Queral et al. (2002a 2003 2004b), y BWR-GE (2004-2007), Queral et al. (2004a 2005 2006).

En general, la metodología desarrolla cubre los siguientes aspectos:

- Establecer una forma de computerización adecuada para cada elemento estructural de los procedimientos: pasos, instrucciones, notas, precauciones, precauciones, páginas desplegables, pasos de acción continua, etc. Es decir, de todos los elementos que componen los EOP de un PWR-W, Sección 4.3.1.

- Identificar los sistemas y componentes demandados y las variables físicas de validación, Sección 4.3.2, realizando una relación detallada de los posibles estados y acciones sobre sistemas y componentes (acciones / manipulaciones), y de las evaluaciones sobre variables físicas. La implementación de sistemas y componentes debe realizarse de forma que cubran todos los niveles de detalle de la computerización, de forma que un cambio de criterio en un conjunto de pasos de un procedimiento no afecte al modelado de sistemas y componentes.

- Proporciona un conjunto de normas de computerización de los procedimientos para su compatibilización con los procedimientos escritos, Sección 4.3.3, de forma que un modelo computerizado de los EOP pueda ser ampliado de forma modular. Este aspecto es favorecido por la estructura de pasos de los EOP, pudiéndose definir el nivel de detalle de computerización de forma independiente en cada uno de ellos y según las necesidades de simulación.

En los siguientes apartados se hacen algunas consideraciones adicionales sobre estos aspectos.

4.3.1 Computerización de los elementos que componen los EOP.

Los EOP de un reactor de agua a presión presentan elementos estructurales propios que requieren una interpretación según exigencias del lenguaje Prola para poder codificarlos. Estos elementos estructurales, así como su estructura global, fueron introducidos en la Sección 4.1. A continuación, se tratará cada uno de ellos y la implementación a realizar de forma que conserven su funcionalidad, tanto individual como en conjunto, en los procedimientos computerizados. El conjunto de elementos se considerados consiste en:

- Pasos de acción.

- Notas y precauciones.

- Página desplegable.

- Gestión de los árboles de estado de las CSF y requerimientos de la computerización de las FRG.

4.3.1.1 Pasos de acción

En lo que respecta al formato de dos columnas característico de los EOP PWR-W, se ha constatado que permite la implementación de los pasos de acción en términos lógicos, es decir, si las condiciones especificadas en la columna la izquierda no se cumplen o no son alcanzadas, entonces se deben realizar las acciones de contingencia contempladas en la columna de la derecha, siendo por lo tanto su computerización viable de forma que no se rompa la estructura lógica del procedimiento original.

Respecto a los tipos de acciones demandadas al operador durante el seguimiento de los EOP, se han clasificado en cuatro grupos:

1. Validaciones lógicas o numéricas de variables de estado de componentes y sistemas de la planta o variables físicas, para así determinar la secuencia de actuaciones, de pasos o la llamada a otro procedimiento según proceda.

2. Vigilancia continua de variables físicas o de estado de componentes y sistemas. La intención es prever situaciones que requieran tomar acciones correctoras o cambiar la secuencia de instrucciones si se producen situaciones que lo requieran.

3. Demanda de actuaciones sobre elementos de control según sea el resultado final obtenido por las instrucciones de los grupos anteriores.

4. Cambio de la guía en ejecución a otra más apropiada, según criterios de validación sobre variables físicas o de estado de los sistemas de la planta o de sus componentes integrantes, se corresponde con acciones clasificadas en los grupos 1 y 2.

Estos tipos de actuaciones se corresponden con la funcionalidad de las instrucciones Prola AUTOCHECK, MONITOR, ACTION e INITIATE.

Dentro del primer tipo de actuación, se pueden dar cuatro tipos de estructuras lógicas, Figura 4.21, Macwan et al. (1991):

- **Tipo A**: Este tipo de pasos proporcionan al operador una salida a otro procedimiento cuando las actuaciones automáticas y las de respaldo manual fallan.

- **Tipo B**: Este tipo de pasos no proporciona una salida en caso de fallo de la función demandada. Este es el caso de las actuaciones en las que se considera posible que las actuaciones de recuperación subsiguientes sean realizadas de forma local.

- **Tipo C**: Las actuaciones que se realizan de forma incondicional.

- **Tipo D**: Estas actuaciones son usualmente procesos de diagnóstico. Normalmente se corresponde con un síntoma específico, que si se presenta, conlleva la salida a un procedimiento específico.

Considerando estos cuatro tipos de actuaciones, tipos A, B, C y D, se puede mencionar que, durante la evaluación de las validaciones lógicas demandadas en el conjunto de los procedimientos de un PWR-W, se ha comprobado que todas ellas se corresponden con algunos de los cuatro tipos definidos, siendo codificables empleando la sentencia Prola AUTOCHECK, lo que garantiza su implementación en el procedimiento codificado.

Una característica general de la realización de cualquier actuación por el personal de la sala de control es que conllevan, asociados al conjunto de las tareas que implique dicha actuación:

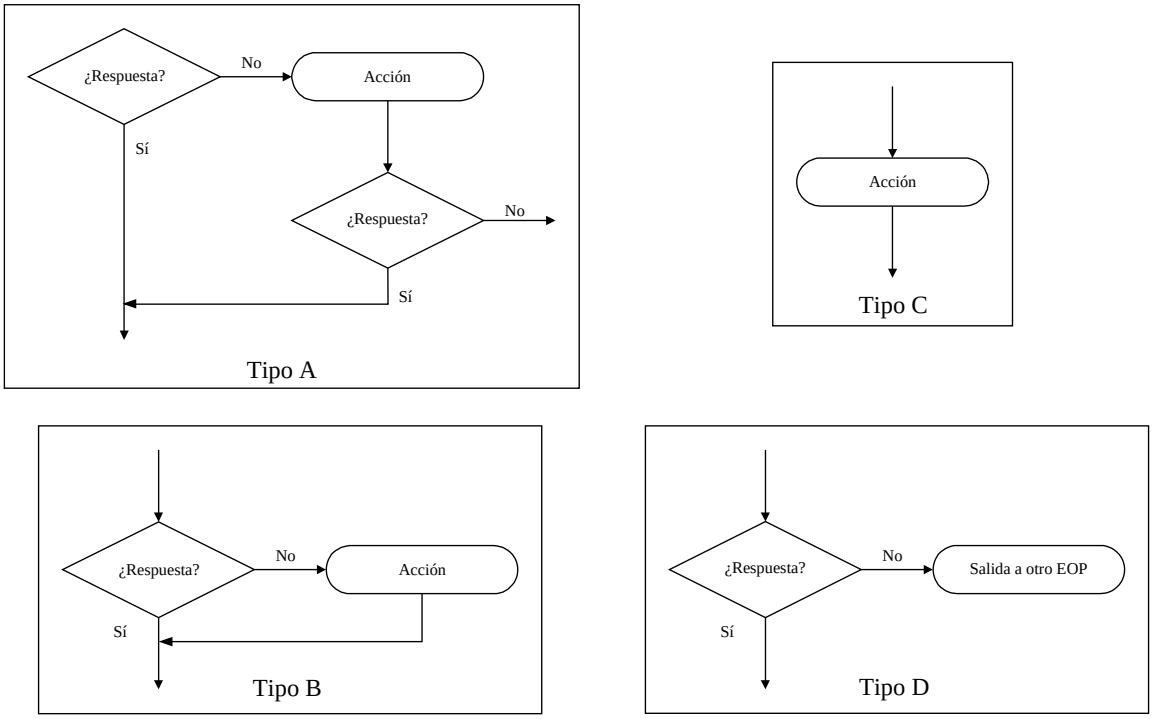


Figura 4.21: Tipos de pasos implementados en los EOP de un PWR-W atendiendo a su estructura lógica.

- Un tiempo requerido para su ejecución, ligado principalmente a la naturaleza física de dichas actuaciones.
- Una carga de trabajo, dependiente de la complejidad de las actuaciones, considerando factores cognitivos y físicos.

Para el tratamiento de ambos aspectos se han definido dos atributos, tiempo de ejecución y carga de trabajo, asociados a todo paso del procedimiento computerizado. Los valores de dichos parámetros, denominados TEXEC y TASKLOAD, deberán reflejar el tiempo en segundos que conlleva la realización de la acción registrada en el paso y la carga de trabajo porcentual que debe asumir sobre el personal de la sala de control en su realización. La forma de obtención de los valores de dichos parámetros excede los objetivos del presente trabajo, estableciéndose solamente la funcionalidad inicial de los mismos, que podrá ser mejorada en el futuro. Una valoración orientativa de las diferentes opciones se incluye en la Sección 7.2. De la experiencia adquirida durante la realización del trabajo se ha concluido que ambos parámetros deben ser globales, de forma que cuando una acción sea demanda por los procedimientos, se deberá verificar la capacidad de ejecución por parte del personal de la sala de control de dicha acción evaluando que la carga de la misma sea inferior a la carga asumible por el personal de operación. En ese caso, la acción se realizará, pasando a considerarse su carga en el total de carga de trabajo del personal durante su tiempo de realización. En caso contrario, es decir, la carga asociada a

la acción demanda excede la carga de trabajo libre del personal de la sala de control, la acción será demorada hasta que se liberen los recursos suficientes para realizarla. Cuando el tiempo de ejecución de una acción finalice, se liberará la carga de trabajo asociada a la misma, pudiéndose dar el caso de que los recursos liberados permitiesen la ejecución de una nueva acción demanda por los procedimientos vigentes.

Considerando la tipología de los pasos empleados en los EOP de un PWR-W, se debe prestar especial atención para realizar su computerización a:

- **Pasos de acción inmediata**.
  Se denominan pasos de acción inmediata aquellos que el operador puede realizar sin necesidad de recurrir a la lectura de los procedimientos escritos. En general se corresponden con un conjunto de pasos memorizados y fuertemente ejercitados por los operadores. Esta característica afecta en la computerización de los pasos al tener que considerar tanto tiempos de ejecución como cargas de trabajo mas reducidos, atributos de tiempo requerido para la ejecución y de carga de trabajo asociada, TEXEC y TASKLOAD, respectivamente.

- **Pasos de acción continua**.
  Los pasos de acción continua son aquellos que una vez ejecutados deben ser supervisados de forma continuada por el operador hasta la finalización del procedimiento en el que se encuentran. La computerización de este tipo de pasos se realiza mediante sentencias MONITOR con la misma vigencia que la actividad que ejecuta el procedimiento. Para su codificación se empleará una estructura no secuencial de dos bloques por cada paso de acción continua del procedimiento. El primero, consiste en la codificación del paso sin considerar su categoría de acción continua, terminando con el iniciado de la sentencia MONITOR correspondiente a las condiciones de evaluación y una sentencia GOTO para dar paso a la ejecución secuencial del paso siguiente, según corresponde con la estructura del procedimiento. El segundo bloque del paso incluye el conjunto de instrucciones que se ejecutan cuando la sentencia MONITOR iniciada en el bloque anterior verifique el cumplimiento de la condición de evaluación. Este conjunto de instrucciones finaliza con el reinició de la sentencia MONITOR de evaluación del paso de acción continua, si se requiere, y con la finalización de la actividad iniciada para su ejecución.

- **Pasos con evaluaciones sobre el histórico de variables físicas**.
  En los procedimientos se demandan evaluaciones de violación de tarados de ciertas variables físicas en el intervalo de tiempo precedente a su ejecución y desde que se entró en modo de operación de emergencia. Por ello, asociados a estos pasos, se deben incluir al principio del EOP E-0 un conjunto de sentencias MONITOR, una por variable física considerada, que vigilen esta circunstancia. El resultado de la violación del tarado se registrará en una variable de lógica de control, única para cada variable física, que será evaluada en el momento de la ejecución del paso.

- **Pasos que implican la realización de acciones de control** sobre el valor de ciertas variables físicas que impliquen actuación de componentes, siendo en general válvulas de control de caudal de sistemas como el FW, la ducha del presionador, etc.

Dentro del proceso de computerización, este tipo de actuaciones es el que requiere mayor atención, ya que implican por su alcance el modelado de controles de componentes en el simulador de procesos, pues se corresponden con acciones que se prolongan más allá del tiempo de actuación del paso en que se inician. Este último aspecto, unido además a que un grupo de actuaciones de control se aplica sobre las mismas variables físicas aunque en diferentes condiciones según el paso en que se ejecuten, obliga a tener una vision global en todo el conjunto de los EOP de su actuación, objetivo y rango de control sobre la variable que controlan, para ser implementadas de forma correcta.

Las especificaciones de computerización para este tipo de actuaciones son:

- Se deberá implementar un **control manual en el simulador de procesos** que, mediante una o varias variables de estado, actúe en los diferentes modos de operación demandados en los diferentes pasos implementados en el modelo de procedimientos computerizados. El valor de dichas variables de estado será la única interfase entre el control implementado en simulador de procesos y el simulador de procedimientos.
- Estas instrucciones presentarán un tiempo de ejecución asociado al inicio de la actuación de control y la verificación de que su realización es adecuada, es decir, deberá considerar **tiempos de evaluación de variables de proceso** y juicio de su evolución para determinar si se alcanzará supuestamente el objetivo especificado en el paso para dicha actuación de control.
- La **carga de trabajo** asociada a dichas instrucciones se considerará mientras la actuación de control esté vigente. Normalmente, la vigencia de este tipo de actuaciones está ligada a la ejecución del procedimiento donde se considera y, por lo tanto, a la vigencia de la actividad que ejecuta dicho procedimiento.

4.3.1.2 Notas y precauciones

De forma general, se ha decidido codificar estas instrucciones mediante sentencias MESSAGE. En el caso de encontrarse en ejecución la MMI del sistema COPMA-III durante la simulación, el texto literal contenido en estas instrucciones se mostraría en pantalla.

Cabe destacar que ciertas notas implican:

- Algún tipo de actuación similar a las especificaciones de los pasos de acción continua tratados anteriormente. Estos pasos de acción continua enunciados en forma de notas o precauciones pretenden captar la atención del operador mejor que en forma de pasos del procedimiento, es decir, solo se considera desde el punto de vista de factores humanos, y su computerización no requiere consideraciones adicionales, correspondiéndose de forma directa con las realizadas para los pasos de acción continua.
- Condiciones o modos de operación de sistemas y componentes que, por su importancia, pudiesen ser susceptibles de considerarse en la codificación. Su implementación queda supeditada a los objetivos y el alcance del nivel de detalle requerido por la simulación.

4.3.1.3 La página desplegable

La página desplegable contiene un conjunto de validaciones sobre el estado de sistemas, componentes y variables físicas, indicando a su vez las acciones a realizar en el caso de darse alguna de las condiciones consideradas. El operador está obligado a vigilar de forma continuada estas condiciones durante la ejecución del procedimiento, realizándose en aquellos momentos que por carga de trabajo o juicio personal se estime pertinente. Considerando estos aspectos, se debe codificar mediante sentencias MONITOR, ligando su vigencia a la actividad que ejecuta el procedimiento. Se implementarán tantas sentencias MONITOR como condiciones a evaluar se informen en la página desplegable. Aquellas validaciones cuya implementación se considere innecesaria para los objetivos de la simulación, se corresponderán con sentencias MESSAGE tipo *dummy*, cuya única finalidad sera la de emular el tiempo equivalente a su ejecución y la carga de trabajo ocasionada en el operador, valores informados en las variables TEXEC y TASKLOAD de la instrucción, respectivamente.

4.3.1.4 Vigilancia de los árboles de estado de las CSF y computerización de las FRG

Como ya se ha comentado en la descripción de los EOP de un PWR-W, el proceso de verificación del cumplimiento de las CSF consisten en una estructura en árbol de validaciones sobre parámetros físicos del proceso, denominados árboles de estado, que determinan el estado del cumplimiento de las CSF y qué procedimiento se debe considerar para su recuperación, denominados procedimientos de recuperación de funciones, FRG.

La computerización de dicha vigilancia de las funciones críticas de seguridad no estaba considerada dentro del alcance del trabajo, pero su implementación se consideró dentro las especificaciones de la metodología.

Tres características hacen la implementación de las FRG y de la vigilancia de las CSF diferente a la definida para las ORG:

- Su vigilancia continua, desde que se indica en el paso correspondiente del EOP E-0 o se abandona éste en una transición a otro procedimiento.
- Su carácter prioritario sobre las ORG en función del estado de las CSF.
- La jerarquía interna en función del estado de las CSF, que determina la prioridad en el seguimiento de las FRG para la recuperación de las CSF con estado degradado.

En lo que respecta a la vigilancia de los árboles de estado, puede implementarse con la funcionalidad que proporciona el lengua Prola y el sistema COPMA. Para ello, se debe realizar una versión computerizada de los árboles de estado, Figura 4.3 pág. 249, y de las FRG, que presentan una estructura similar a las ORG, por lo que no es necesario realizar consideraciones adicionales, Tabla 4.4. Tal como se ha descrito en la Sección 4.1, la vigilancia de los árboles de estado se realiza cada diez o veinte minutos durante la gestión de emergencia en fase preventiva, por lo que su implementación se podría realizar con una actividad cíclica con una sentencia WAIT condicionada a ese intervalo de tiempo.

En lo que respecta a la carga de trabajo y el tiempo de ejecución relacionados con la vigilancia de las CSF, verificando el estado de los árboles de estado, se puede considerar en primera aproximación que ambos son despreciables, debido a que su vigilancia está considerada dentro de las funciones del SPDS en los PWR-W. Es decir, los parámetros de TASKLOAD y TEXEC relacionados con las instrucciones de ejecución de la vigilancia de las CSF podrían implementarse con valores nulos.

Sin embargo, el tratamiento que requiere la jerarquía de las ORG y de las FRG, así como de la jerarquía interna de las FRG, es particular de este tipo de procedimientos. Por ello, en la versión computerizada del procedimiento debe existir un atributo de prioridad que permita la gestión de su información y otro correspondiente a su identificación dentro del conjunto de los procedimientos. Además, se debe incorporar la funcionalidad necesaria en el simulador de procedimientos para priorizar la ejecución de los mismos en función de dichos atributos. De forma adicional, para definir sus especificaciones se debe considerar que la ejecución de las FRG frente a las ORG no siempre es incondicional. En el caso de presentarse terminales en color amarillo para alguna CSF, el operador debe decidir apoyándose en un proceso de toma de decisiones, que prioriza el seguimiento de la ORG actual o el inicio de la FRG demandada. Este último aspecto implica la consideración de procesos cognitivos relacionados con la toma de decisiones e implementar una cuantificación de los parámetros considerados en los procesos cognitivos considerados. Al no estar dentro del alcance del trabajo realizado todas estas observaciones, se considera una primera aproximación a su resolución para su consideración en posibles desarrollos futuros en la Sección 7.4.

4.3.2 Identificación de sistemas, componentes demandados y variables de validación.

Previo a la computerización de los procedimientos, se estima necesario un estudio de los sistemas que actúan en los mismos, sus posibles estados y actuaciones demandadas sobre ellos y los componentes que los integran, para poder determinar el tratamiento que recibirán durante la codificación de los pasos con PED-II.

El editor PED-II necesita tener definidos las variables y componentes de proceso que van a intervenir de acuerdo al contenido de los procedimientos y deben estar identificados mediante unas claves o CharIdents. Según las necesidades de codificación los CharIdents son identificadores de componentes y variables físicas, estados de componentes y variables físicas y, en la mayoría de los casos, se codificara a nivel de sistema, por lo que el CharIdent se corresponderá con un sistema o un tren del mismo. El contenido de las variables puede ser numérico o simbólico. En general, cuando se trate de componentes o sistemas el contenido de la variables sera simbólico, representando su estado. En el caso particular de variables físicas, su valor será numérico, siendo el valor de dicha variable. Si fuese necesario realizar una validación sobre el estado de dicha variable considerando su evolución temporal, recurriríamos a un nuevo CharIdent. En general se definirá el nombre de estos elementos y un conjunto de atributos que permita realizar todas las acciones consideradas en los EOP sobre los mismos.

Según requisitos del lenguaje Prola, cada CharIdent esta formado por letras mayúsculas y numeros, iniciándose siempre con una mayúscula. La longitud maxima de la cadena es de dieciséis caracteres.

Además, se han considerado necesarias un conjunto de reglas para dotar de cierta formalidad a los aspectos prácticos de la computerización de los procedimientos:

- Identificar los sistemas, componentes y variables físicas del proceso mediante sobrenombres predefinidos que cumplan exigencias de sintaxis Prola, facilitando así la interpretación del CharIdent.
- Utilizar los números cuando se repita el sistema, componente o variable en la planta.
- Dentro de un CharIdent, la numeración afecta al conjunto de caracteres anterior a su posición.
- Primeramente, en un CharIdent, se identificará el sistema, después el componente y, finalmente, la variable.
- Si existen componentes o variables afectados por dos sistemas, se deberían informar ambos en el CharIdent, siendo el primero el sistema que reciba el servicio.

4.3.2.1 Tipos de variables definidas

Se han identificado los cuatro tipos de variables que pueden encontrarse en los pasos de los procedimientos, siendo:

- Para los sistemas y componentes, se deben considerar: variables de estado, variable de estado requerido, modo de operación (automático o manual) y parámetros físicos asociados a la operación del sistema o componente.
- Para las variables de proceso, se consideran el valor de la variable física y su estado, considerado como la tendencia de ese valor en el tiempo.

Estas variables se han definido y agrupado como estructuras, diferenciando tipos de componentes (bombas y válvulas), modos de operación de sistemas (variables generales) y variables físicas. Los campos de estas estructuras serán gestionados por el simulador de proceso o de procedimientos según corresponda, Tablas 4.6 a 4.9.

4.3.2.2 Nomenclatura utilizada en los EOP y en su computerización

Durante el estudio inicial de los EOP se observó que el texto de los procedimientos, tenía algunas deficiencias de criterio a la hora de denominar sistemas y componentes de la planta. Así, los sistemas se denominan mediante sus acrónimos anglosajones, mientras que componentes

Bombas (*pumpcomponent*)			
Gestión	**Propiedad**	**Contenido**	**Comentario**
Simulador de procesos	*speed*	Valor numérico	RPM de la bomba
	opStatus	RUNNING, STOPPED	Estado de operación de la bomba
	autoStatus	AUTO, MAN	Modo de operación de la bomba
Simulador de procedimientos	*command*	Valor numérico	Cuando el procedimiento especifica una acción sobre la bomba PUMP, el simulador de procedimientos cambia el valor de PUMP.command, en particular: - STOP PUMP.command pone PUMP.command al valor especificado en PUMP.stopval. - START PUMP.command pone PUMP.command al valor especificado en PUMP.startval.
	autoSwitch	ON, OFF	
Usuario	*startval*	Valor numérico constante	Valor contaste definido por el usuario
	stopval	Valor numérico constante	

Tabla 4.6: Estructura *pumpcomponent* y asignación de su gestión.

o partes de sistemas se denominan mediante acrónimos anglosajones o castellanos sin criterio aparente. Por ejemplo, el Generador de Vapor se denomina SG, los termopares TC (*Termocouple*) y el sistema de agua de refrigeración de componentes CCW (*Component Cooling Water*), Tabla 4.10. Para la realización del trabajo, se ha obtenido una selección genérica de claves de sistemas, componentes y variables físicas que se deberán utilizar en la creación de las variables para el desarrollo del modelo de procedimientos en el editor PED-II. La ventaja que ofrece esta nomenclatura respecto a la de los procedimientos escritos es que fue obtenida a partir de la denominación anglosajona de componentes y sistemas, lo cual evita confusiones a la hora de identificar las variables implementadas, Tabla 4.11. Esta lista de variables es similar, aunque corregida, a la empleada en la codificación de los procedimientos de la CN de Zorita.

Válvulas (*valvecomponent*)			
Gestión	**Propiedad**	**Contenido**	**Comentario**
Simulador de procesos	*position*	Valor numérico	Apertura de la válvula
	opStatus	OPEN, CLOSED, CLOSING...	Posibles estados de la válvula
	autoStatus	AUTO, MAN	Modo de operación de la válvula
Simulador de procedimientos	*command*	Valor numérico	Cuando el procedimiento especifica una acción sobre la válvula VALVE, el simulador de procedimientos cambia el valor de VALVE.command, en particular: - OPEN VALVE.command pone VALVE.command al valor especificado en VALVE.openval - CLOSE VALVE.command pone VALVE.command al valor especificado en VALVE.closeval
	autoSwitch	ON, OFF	
Usuario	*openval*	Valor numérico constante	Valor contaste definido por el usuario
	closeval	Valor numérico constante	

Tabla 4.7: Estructura *valvecomponent* y asignación de su gestión.

Magnitud Física (*physmagnitude*)			
Gestión	**Propiedad**	**Contenido**	**Comentario**
Simulador de procesos	*Value*	Valor numérico	Valor de la magnitud
	Tendency	INCREASING, DECREASING y STEADY	Tendencia, evolución temporal, de la magnitud

Tabla 4.8: Estructura *physmagnitude* y asignación de su gestión.

Variable general (*generalvariable*)			
Gestión	**Propiedad**	**Contenido**	**Comentario**
Simulador de procesos	*mode*	Valor numérico	Modo de operación del sistema. Se tiene que corresponder con alguno de los dos valores especificados en *mode1val* o *mode2val*
Simulador de procedimientos	*command*	MODE1 o MODE2	Los dos tipos de acciones sobre variables generales, MODE1 o MODE2, actúan sobre *command* asignando *mode1val* o *mode2val*, respectivamente. Por ejemplo: ACTION MODE2 SYSTEM.command, asigna a SYSTEM.command el valor especificado en *mode2val*
Usuario	*mode1val*	Valor numérico constante	Valor contaste definido por el usuario
	mode2val	Valor numérico constante	

Tabla 4.9: Estructura *generalvariable* y asignación de su gestión.

Acrónimo/Siglas	**Descripción**
AF	Sistema de agua de alimentación auxiliar (*Auxiliary Feedwater*)
AMSAC	Sistema de actuación del circuito de mitigado de ATWS (*ATWS Mitigating System Actuation Circuitry*)
BIT	Tanque de inyección de boro (*Boron injection Tank*)
C.A.	Corriente alterna
CCW	Sistema de agua de refrigeración de componentes (*Component Cooling Water*)
CST	Tanque de condensado (*Condensate Storage Tank*)
DG	Generadores diesel (*Diesel Generator*)
CSF	Funciones criticas de seguridad
FW	Sistema de agua de alimentación (*Feedwater*)
SG	Generador de vapor (*Steam Generator*)
MG	Motogenerador
MSIV	Valvula de aislamiento de las linea de vapor (*Main Steam Isolation Valve*)
MSR	Recalentadores y separadores de humedad (*Moisture Steam Reheaters*)
PORV	Válvulas de alivio (*Power Operated Relief Valve*)
RCP	Bomba de refrigerante del reactor (*Reactor Cooling Pump*)
RCS	Sistema de refrigeración del reactor (*Reactor Cooling System*)
RHR	Sistema de evacuación de calor residual (*Residual Heat Removal*)
RWST	Tanque de agua de la recarga (*Refuelling Water System Tank*)
SGTR	Rotura de tubos en un Generador de Vapor (*Steam Generator Tube Rupture*)
SI	Inyección de seguridad (*Safety injection*)
SP	Sistema de rociado de contención (*Spray*)
SW	Agua de servicios (*Service Water*)
TC	Termopares (*Termocouple*)

Tabla 4.10: Acrónimos y siglas empleados en los EOP de un PWR-W.

Acrónimo	Descripción
A	Corriente eléctrica (amperios), Acumulador [*ampere, accumulator*]
AB	Edificio Auxiliar [*auxiliary building*]
AC	Condiciones adversas [*adverse conditions*]
AFW	Agua de alimentación Auxiliar [*auxiliar feed water*]
ASP	Spray auxiliar [*auxiliar spray*]
AVG	Media [*average*]
B	Barra eléctrica [bus]
BA	Sistema ácido bórico/ácido bórico [*boric acid*]
BD	Purga [*bleed*]
BH	Calentadores de apoyo [*backup heater*]
BP	*Bypass*
BR	Interruptor [*breaker*]
C	Núcleo del reactor, Concentración [*core, concentration*]
CCW	Sistema de agua de refrigeración de componentes [*component cooling water*]
CD	Sistema de condensado [*condensate*]
CFLUX	Flujo neutrónico [*core neutron flux*]
CH	Sistema de control químico y de volumen [*chemical*]
CL	Rama fría [*cold leg*]
CM	Modo de Enfriamiento [*cooling mode*]
CNT	Contención [*containment*]
CR	Sala de Control [*control room*]
CV	Válvula de control de caudal [*control valve*]
CW	Sistema de agua de circulación y refrigeración [*cooling water*]
D	Demandado/a; Derivada [*demand, derivate*]
DG	Generador Diesel [*diesel generator*]
DL	Retardo [*delay*]
DW	Sistema de agua desmineralizada/agua desmineralizada [*demineralized water*]
E	Procedimientos de Emergencia, Emergencia [*emergency*]
EG	Generador Eléctrico [*electric generator*]
EL	Sistema eléctrico [*electric*]
ESW	Sistema de agua de servicios esenciales [*essential service water*]
EXT	Exterior [*external*]
F	Caudal [*flow*]
FIG	Figura [*figure*]
FOP	Página desplegable [*fold out page*]
FW	Agua de Alimentación [*feed water*]
H	Calentadores [*heaters*]
HL	Rama caliente [*hot leg*]
HPR	Alta presión [*high pressure*]
I	Aislamiento [*isolate*]

continua en la página siguiente

continua desde la página anterior

Acrónimo	**Descripción**
IA	Sistema de aire de instrumentos [*instrument air*]
IV	Válvula de aislamiento [*isolate valve*]
KV	Kilovoltios [*kilovolt*]
L	Nivel [*level*]
LC	Control de nivel [*level control*]
LIMINF	Límite inferior para la acción CONTROL
LIMSUP	Límite superior para la acción CONTROL
LL	Límite inferior [*low level*]
MC	Condición MONITOR [*monitor condition*]
MS	Sistema de vapor principal [*main steam*]
N	Normal/es [*normal*]
N.xx	Nota nº xx (xx = número de paso al que antecede la nota) [*note*]
NAC	Condiciones normales y adversas [*normal and adverse conditions*]
NPSH	NPSHd
NR	Rango estrecho [*narrow range*]
NUM	Número [*number*]
OK	O.K.
P	Potencia [*power*]
PASS	Toma de muestras post-accidente [*post-accident sampling system*]
POS	Posición [*position*]
PR	Presión [*pressure*]
PRCV	Válvula de control de presión [*pressure control valve*]
PREC.xx	Precaución nº xx (xx =número de paso al que antecede) [*precaution*]
PRSP	Punto de tarado de la presión [*pressure setpoint*]
PU	Bomba [*pump*]
PZR	Presionador [*pressurizer*]
RAMxx	Alarma en Monitor de radiación nº xx [*radiation alarm monitor*]
RCS	Sistema Refrigerante del Reactor [*reactor cooling system*]
RHR	Sistema de evacuación de calor residual [*residual heat removal*]
RM	Sistema de vigilancia radiológica [*radiological monitory*]
ROD	Barras de control [*rod*]
RV	Válvula de alivio [*relief valve*]
RX	Reactor [*reactor*]
S	Velocidad [*speed*]
SI	Inyección de seguridad, Sumidero [*safety injection, sink*]
SG	Generador de vapor [*steam generator*]
SL	Cierres [*seal*]
SM	Margen de Parada [*shut-down margin*]
SP	Ducha, tarado [*Spray, setpoint*]

continua en la página siguiente

continua desde la página anterior	
Acrónimo	**Descripción**
ST	Temperatura de saturación, Estado de una variable [*saturation temperature, state*]
SV	Válvula de seguridad [*safety valve*]
T	Temperatura [*temperature*]
TB	Turbina [*turbine*]
TBB	Edificio eléctrico y de turbina [*turbine building*]
TC	Termopares [*termocouple*]
TK	Tanque [*tank*]
TRIP	Disparo [*trip*]
UL	Límite superior [*upper limit*]
V	Válvula, Tensión (voltios) [*valve, volt*]
VAC	Sistema de ventilación y aire acondicionado [*ventilation and air conditioning*]
VH	Cabeza de la vasija [*vessel head*]
WR	Rango ancho [*wide range*]

Tabla 4.11: Listado de acrónimos y siglas empleados en en la computerización de los EOP.

4.3.3 Normas de codificación de los procedimientos

Para obtener una relación estrecha entre el procedimiento computerizado y el original empleando el editor PED-II, se han definido un conjunto de normas obtenidas a partir de la experiencia adquirida durante el proceso. En realidad, estas normas están sujetas a valoración personal, y pueden ser ampliadas o mejoradas.

1. El proceso de computerización se debe realizar respetando la estructura de los EOP, debiéndose estructurar en pasos que posean la misma funcionalidad y cubran los objetivos de los pasos del procedimiento escrito. Este punto se evalúa en la descripción detallada del proceso de computerización de cada procedimiento, del cual se incluye un ejemplo en Quiroga et al. (2006).

2. Durante la computerización se proporcionará una relación detallada de los criterios de validación lógica asumidos durante la interpretación de los procedimientos, incluyendo los criterios de actuación y rangos de valores de control de variables.

3. Para mantener una correlación entre el sistema de numeración de pasos de que dispone COPMA- III y la numeración de los propios EOP, se asumirá que el primer número de la numeración de pasos en COPMA-III es coincidente con el número del paso del EOP original.

4. A efectos del sistema COPMA, precauciones y notas son considerados como pasos. Para no alterar la numeración correspondiente de los pasos, se intercalarán entre los mismos

respetando sus posiciones en el procedimiento, dándoles una numeración compuesta por dos números separados por guiones, cuyo primer número es el mismo que el del paso al que preceden y un segundo número, de naturaleza decimal, referido a la nota o precaución. El último paso de esta serie decimal será el propio paso del EOP original al que preceden las nota/s y/o precuación/es. Este método se utiliza también para desarrollar la página desplegable y es aplicable también en cualquier otra circunstancia en que se haga necesario intercalar un paso aún cuando no figure como tal en un EOP.

5. Todas las instrucciones derivadas de la conclusión de cada criterio de vigilancia sobre variables del proceso o estado de componentes o sistemas, instrucciones Prola MONITOR, se deberán intentar agrupar en el paso asociado a dicha vigilancia. De esta forma, se evita romper la estructura del procedimiento, conservando la relación lógica de los elementos computerizados.

6. Se han establecido normas para la elaboración de las claves , denominadas CharIdents, que identifican componentes y variables citados en los EOP, Sección 4.3.2.

7. Se han definido los tipos de «evaluaciones» y «acciones» que se han identificado en los EOP para utilizarse en las correspondientes instrucciones AUTOCHECK, MONITOR, ACTION e INITIATE, Sección 4.2.1.2.

8. La ventana de texto COMMENT que aparece en la mayoría de las instrucciones durante su computerización en PED-II, se utilizará para incluir el texto exacto de los pasos que figuran en el EOP y la información adicional que se ha considerado de interés para poder seguir el procedimiento sin necesidad de consultas externas. También, en aquellos pasos cuya interpretación o codificación aún no esté cerrada, se aprovechará para denotar el estado de implementación del mismo.

9. Se crearán variables generales, *generalvariable*, para permitir identificar y aplicar diferentes modos de operación o control de un sistema o componente. A cada modo de los definidos se le identificará con un número entero en el simulador de procesos, siendo el módulo de comunicación entre ambos simuladores el encargado de traducir estos valores numéricos a valores simbólicos de estado de sistema. La variable de estado tiene una clave (CharIdent) siguiendo las normas generales para su nomenclatura y en la instrucción que interese se le asignará el número que le corresponda. Las funciones asignadas a cada número o estado estarán desarrolladas de forma unívoca en la documentación especifica de computerización de los procedimientos. Un ejemplo es el el control de alivio de vapor al condensador en modo presión o modo temperatura.

10. Para distinguir aquellos casos en que los valores de los puntos de tarado a evaluar son diferentes según se esté en condiciones normales o adversas, se ha establecido que a la clave correspondiente de la variable se le añada el sufijo NAC, seguido de un número correlativo para cada pareja de valores.

11. Se han definido variables para limitar la vigencia de un MONITOR, dentro de un procedimiento. Se relacionan directamente con la variable lógica de control de la variable física

monitorizada, tomando su nombre y añadiendo el sufijo de estado (ST). A dicha variable se le asigna un valor numérico para su validación lógica, siendo 1 en el caso de vigencia activa y 0 para anularla.

12. En las ocasiones en que las instrucciones sean de escasa importancia para la operación y no impliquen interacción con el modelo de planta, se utilizaran las variables TEXEC y TASKLOAD asociadas a la instrucción para emular el tiempo equivalente a su ejecución y la carga de trabajo ocasionada.

13. Las instrucciones INITIATE tienen que tener como parámetro el nombre del fichero XPA del procedimiento a ejecutar.

14. El primer paso de la versión computerizada de un EOP debe ser numerado con 1 en lugar de 1-1, que es la numeración el que el editor PED-II asigna por defecto.

4.4 Modelado de los EOP de un PWR-W

Dentro de los objetivos del trabajo se definió como uno de ellos la verificación de las capacidades de modelado de las ORG con el conjunto de herramientas escogido, basándose el lenguaje Prola y considerando que la aplicación de los modelos se debería llevar a cabo empleando el sistema COPMA-III. Para ello, primero se definieron los aspectos genéricos de un modelo de EOP para el tipo de planta considerado, Sección 4.4.1, y posteriormente se realizaron dos aproximaciones al modelado de los procedimientos y su validación funcional mediante su ejecución con el sistema COPMA-III, Sección 4.4.3:

- Un modelo de alto nivel de detalle de una ORG, en este caso se escogió el EOP E-0.
- Un modelo que abarcase un conjunto significativo de ORG, de forma que se constatase que se disponía de la funcionalidad suficiente para codificar transiciones entre diferentes ORG y que sería posible la simulación de la gestión de emergencia mediante su uso. En este caso realizó una codificación de nivel de detalle reducido.

A continuación se describe en detalle el trabajo realizado.

4.4.1 Aspectos generales del modelado de los EOP

Dentro de los aspectos generales de los modelos de EOP, se desarrollaron un conjunto de tareas genéricas cuyo producto es aplicable a la modelación de los EOP independientemente del alcance u orientación del mismo. Estas tareas han sido:

- La determinación del tipo de variables necesarias para la ejecución automatizada de los EOP, Sección 4.4.1.1.

- El modelado de sistemas y componentes de la planta, Sección 4.4.1.2.
- La codificación de los parámetros físicos del proceso relevantes para la simulación de los EOP, Sección 4.4.1.3
- El estudio de las demandas de actuación sobre sistemas y componentes específicos para controlar el rango de valores de parámetros físicos de la planta, Sección **??**.

Además, el proceso de codificación de cada EOP ha quedado documentado mediante:

- Una descripción detallada de los objetivos del EOP y la funcionalidad del mismo.
- Una relación detallada de las variables empleadas durante la computerización del procedimiento, tanto para componentes, sistemas y variables físicas.
- Una descripción detallada del proceso de computerización del procedimiento, en la cual se incluye un estudio de la totalidad de los pasos del procedimiento, realizando una descripción detallada de sus funciones y como se ha realizado su implementación, criterios de computerización y demás aspectos relacionados.
- El listado del código Prola obtenido.
- Un diagrama de flujo donde se muestre de forma gráfica la estructura del EOP computerizado. Este diagrama debe reflejar el grado de detalle del EOP computerizado.

Debido a que la extensión de esta documentación para cada EOP es excesiva, los resultados no se han incluido en este trabajo, pudiéndose consultar en las referencias Expósito y Queral (2004ab 2005a).

4.4.1.1 Relación de las variables utilizadas en la computerización de los EOP

Este sección abarca toda la información referente al conjunto de variables creadas para el modelado de variables físicas, sistemas y componentes necesarios para el modelado de los procedimientos. Adicionalmente, ha sido necesario crear otros grupos de variables para modelar aspectos específicos de los procedimientos, como las validaciones sobre el histórico de variables, Tabla 4.13, y variables de condiciones normales y anormales de operación, Tabla 4.14. Las claves desarrolladas para todas ellas han sido obtenidas aplicando el conjunto de acrónimos y siglas que se incluyen en la Sección 4.3.2.2.

Para la implementación de sistemas y componentes se ha empleado la metodología de estado presentada en la Sección 4.3.2.1, abarcando operación de válvulas, bombas y cualquier otro tipo de componente. El estado de un sistema se reflejará en el campo de la estructura denominado *opStatus*, mientras que el estado requerido por actuación del operador se identificará mediante el campo *command*. Así, por ejemplo, para el caso del sistema de agua de alimentación auxiliar,

sistema AF, se ha implementado la variable de estado AFW.*opstatus* y la variable de estado requerido AFW.*command*. El valor de la variable de estado del sistema es gestionado por TRETA, de acuerdo con el valor de estado requerido suministrado por COPMA-III. Durante el trabajo se han realizado listados de los estados considerados y requeridos de cada sistema y componente implementado, Tablas 4.15 a 4.18.

En el caso de las variables físicas, cada una tiene asociada una variable para su implementación. En algunos casos, motivado por la naturaleza de las validaciones realizadas en el procedimiento de operación de emergencia sobre dicha variable, se ha considerado necesaria la implementación de un campo en la estructura de la variable denominado *tendency*, ligado a la variable numérica de la propiedad física. Este campo, gestionado por TRETA, presenta la tendencia del valor de la variable, es decir, si es estable (*STEADY*), esta aumentando (*INCREASING*) o esta disminuyendo (*DECREASING*), Tabla 4.22.

Por último, conviene resaltar, que el valor de los campos de estas variables, relacionados con el estado actual del sistema, componente o variable física, está gestionado por TRETA, mientras que los campos de estado requerido modificados mediante el atributo *command* es gestionado por COPMA-III, ya que son el reflejo de las acciones realizadas por el operador.

A partir de la lista de acrónimos y siglas incluida en la Tabla 4.11 y empleando las normas de computerización de los procedimientos definidas, se ha obtenido el conjunto de variables a emplear en la codificación de los EOP, revisándose permanentemente según se computerizan los procedimientos.

Variable	**Descripción**
AFW.*command*	Estado requerido del sistema AFW
AFW.*opStatus*	Estado actual del sistema AFW
AFWF	Caudal del sistema AFW* para cada GV
AFWPU#.*command*	Estado requerido de las motobombas 1/2 del sistema AFW
AFWPU#.*opStatus*	Estado actual de la motobomba 1/2 del sistema AFW
AFWPU3.*command*	Estado requerido de la turbobomba del sistema AFW
AFWPU3.*opStatus*	Estado actual de la turbobomba del sistema AFW
CCW.*command*	Estado requerido del sistema CCW
CCW.*opStatus*	Estado actual del sistema CCW
CCWPU#.*command*	Estado requerido de la bomba n° # del sistema CCW (2)
CCWPU#.*opStatus*	Estado actual de la bomba n° # del sistema CCW (2)
CDPU#.*command*	Estado requerido de la bomba de condensado n° # (3)
CDPU#.*opStatus*	Estado actual de la bomba de condensado n° # (3)
CFLUX	Flujo neutrónico en el núcleo
CFLUX.*tendency*	Tendencia del flujo neutrónico en el núcleo
CHF	Caudal de SI
CHF.*tendency*	Tendencia del caudal de SI
CHPU#.*command*	Estado actual de la bomba de carga n° # (3)
CHPU#.*opStatus*	Estado actual de la bomba de carga n° # (3)
CNTI#.*command*	Estado requerido para el sistema CNTI#

continua en la página siguiente

continua desde la página anterior

Variable	**Descripción**
CNTI#.*opStatus*	Estado actual para el sistema CNTI#
CNTPR	Presión en la contención
CNTPR.*tendency*	Tendencia de la presión en la contención
CNTPRH2	Variable de control de la presión en el recinto de contención
CNTSP.*command*	Estado requerido del sistema CNTSP
CNTSP.*opStatus*	Estado actual del sistema CNTSP
CNTSPPU#.*command*	Estado requerido de la bomba n° # del sistema CNTSP (4)
CNTSPPU#.*opStatus*	Estado requerido de la bomba n° # del sistema CNTSP (4)
DSLPR#	Ritmo de variación de la presión en las líneas de vapor (3)
DSLPR#.*tendency*	Tendencia del ritmo de variación de la presión en las líneas de vapor (3)
DSLPRH	Variable de control del ritmo de variación de la presión en las MSLs
ESW.*command*	Estado requerido del sistema ESW
ESW.*opStatus*	Estado actual del sistema ESW
ESWPU#.*command*	Estado requerido de la bomba n° # del sistema ESW (2)
ESWPU#.*opStatus*	Estado actual de la bomba n° # del sistema ESW (2)
FW.*command*	Estado requerido del sistema FW
FW.*opStatus*	Estado actual del sistema FW
FWF	Caudal del sistema FW
FWF.*tendency*	Tendencia del caudal del sistema FW
FWPU#.*command*	Estado requerido de la turbobomba n° # del sistema FW (2)
FWPU#.*opStatus*	Estado actual de la turbobomba n° # del sistema FW (2)
IA.*command*	Estado requerido del sistema AI
IA.*opStatus*	Estado actual del sistema AI
MSBPIV#.*command*	Estado requerido de la MSBPIV n° # (?)
MSBPIV#.*opStatus*	Estado actual de la MSBPIV n° # (?)
MSI.*command*	Estado requerido del sistema MSI
MSI.*opStatus*	Estado actual del sistema MSI
MSIV#.*command*	Estado requerido de la válvula de aislamiento de líneas de vapor n° # (3)
MSIV#.*opStatus*	Estado actual de la válvula de aislamiento de líneas de vapor n° # (3)
MSRV#.*command*	Estado requerido de la válvula de alivio de vapor a la atmósfera n° # (3)
MSRV#.*opStatus*	Estado actual de la válvula de alivio de vapor a la atmósfera n° # (3)
MSRVCD.*command*	Estado requerido de la válvulas de alivio de vapor al condensador (8)
MSRVCD.*opStatus*	Estado actual de la válvulas de alivio de vapor al condensador (8)
MSRVMD	Modo de control del alivio de vapor al condensador
PZRL	Nivel del presionador
PZRL.*tendency*	Tendencia del nivel del presionador
PZRPR	Presión en el presionador
PZRPRNAC1	Variable de condiciones normales/anormales de PZRPR
PZRPR.*tendency*	Tendencia de la presión en el presionador
PZRRV#.*command*	Estado requerido de la válvulas de alivio del presionador n° # (2)
PZRRV#.*opStatus*	Estado actual de la válvulas de alivio del presionador n° # (2)
PZRRV#IV.*command*	Estado requerido de la PZRRV#IV (2)

continua en la página siguiente

continua desde la página anterior	
Variable	**Descripción**
PZRRV#IV.*opStatus*	Estado actual de la PZRRV#IV (2)
PZRRVTK.*command*	Estado requerido del tanque de alivio del presionador
PZRRVTK.*opStatus*	Estado actual del tanque de alivio del presionador
PZRSPV#.*command*	Estado requerido de la válvulas de ducha normal del presionador n° # (2)
PZRSPV#.*opStatus*	Estado actual de la válvulas de ducha normal del presionador n° # (2)
RADAB	Variable de control de presencia de radiación en el edificio auxiliar
RADSEC	Variable de control de presencia de radiación en el secundario
RCSAVGT	Temperatura media del primario
RCSAVGT.*tendency*	Tendencia de la temperatura media del primario
RCSCLTAVG	Temperatura media de ramas frías del primario
RCSCLTAVG.*tendency*	Tendencia de la temperatura media de ramas frías del primario
RCSPU#.*command*	Estado requerido de la bomba del primario n° # (3)
RCSPU#.*opStatus*	Estado actual de la bomba del primario n° # (3)
RCSSUBNAC1	Variable de condiciones normales/anormales de RCSSUBTC
RCSSUBTC	Subenfriamiento del RCS (termopares salida núcleo)
RCSSUBTC.*tendency*	Tendencia del subenfriamiento del RCS (termopares salida núcleo)
RHRPU#.*command*	Estado requerido de la bomba del sistema RHR n° # (2)
RHRPU#.*opStatus*	Estado actual de la bomba del sistema RHR n° # (2)
RHRPUF#	Caudal de las bombas del RHR (2)
RHRPUF#.*tendency*	Tendencia del caudal de la bomba del RHR n° # (2)
RODPOS	Posición de las barras de control
RODPOS.*opStatus*	Posición de las barras de control
RXTRIP.*command*	Estado requerido del disparo del reactor
RXTRIP.*opStatus*	Estado actual del disparo del reactor
SGLNRNAC1	Variable de condiciones normales/anormales de SG#LNR
SG#LNR	Nivel de rango estrecho del GV (3)
SG#LNR.*tendency*	Tendencia del nivel de rango estrecho del GV (3)
SG#PR	Presión en el GV (3)
SG#PR.*tendency*	Tendencia de la presión en el GV (3)
SGIS#.*command*	Estado requerido del sistema de aislamiento de los generadores de vapor
SGIS#.*opStatus*	Estado actual del sistema de aislamiento de los generadores de vapor
SI.*command*	Estado requerido del sistema de inyección de seguridad
SI.*opStatus*	Estado actual del sistema de inyección de seguridad
SLPR#	Presión en las líneas de vapor
SLPR#.*tendency*	Tendencia de la presión en las líneas de vapor
SLPRH	Variable de control de la presión en las líneas de vapor
TBTRIP.*command*	Estado requerido del disparo de turbina
TBTRIP.*opStatus*	Estado actual del disparo de turbina

Tabla 4.12: Lista detallada de las variables implementadas en la computerización de los EOP.

Variable	Descripción	Control vigencia
CNTPRH1	Presión del recinto de contención	—
CNTPRH2	Presión del recinto de contención	CNTPRH2ST
DSLPRH	Ritmo de despresurización en las líneas de vapor	DSLPRHST
SLPRH	Presión en las líneas de vapor	SLPRHST

Tabla 4.13: Variables lógicas implementadas para el control de variables físicas en el modelo de EOP.

Variable	Descripción	Valores
PZRPRNAC1	Presión en el presionador	15 [35] kg/cm^2
RCSSUBNAC1	Subenfriamiento a la salida del núcleo	0 [0] ^oC
SGLNRNAC1	Nivel de rango estrecho en los SG	10 [25] %

Tabla 4.14: Variables de condiciones normales [anormales] de operación implementadas en el modelo de EOP.

4.4.1.2 Implementación de sistemas y componentes

La información del estado de la planta se canaliza para su uso en COPMA-III mediante los campos de estado de sistemas y componentes, gestionadas por TRETA. Las actuaciones del operador dirigidas a variar el modo o el estado de operación de un sistema o componente, se registran en los campos *command* mediante la instrucción ACTION de Prola, siendo estos campos de las variables gestionados por COPMA-III. Será el código TRETA según disponibilidad de sistemas y componentes, tiempos de respuesta, etc. el que aplique los estados requeridos o demandados de sistemas y componentes según corresponda al comportamiento real de la planta.

Durante la computerización de los EOP se ha decido la implementación de los sistemas relacionados en la Tabla 4.15. En la mayoría de los casos, los sistemas definidos como tales en el modelado realizado para COPMA coinciden con sistemas reales de la planta, y su relación con el modelado de TRETA será directa. Sin embargo, por necesidades surgidas durante la computerización de los EOP, ha sido necesario modelar componentes en conjunto, definiendo sistemas ficticios que no se corresponden con sistemas reales de planta, p. ej. el sistema de aislamiento de los SG. La finalidad es una computerización más clara de los procedimientos, evitando nivel de detalle innecesario en acciones que se pueden reducir en numero sin perder su funcionalidad.

De esto se concluye, que los conceptos relacionados con esta parte del trabajo pueden llegar a exigir a veces un grado de abstracción muy fuerte respecto al proceso, componente o sistema que se quiere modelar. Por ello, un sistema, dentro del modelo de sistemas y componentes realizado en la fase de codificación de los EOP, no se corresponde necesariamente con el concepto de sistema de planta. Así, un sistema modelado en la computerización se puede corresponder con un sistema de planta, por ejemplo el AF se encuentra modelado de esta forma en la aproximación actual, y también se puede referir a un conjunto de sistemas y/o componentes que en conjunto realizan una función especifica dentro de los EOP. Este es el caso del sistema de aislamiento de las líneas de vapor, que incluye las válvulas de aislamiento de las líneas de vapor y las válvulas de control de *bypass* de las líneas de vapor. En este sentido, el modelado de sistemas de puede ser funcional, físico o incluso simplemente determina las condiciones de contorno de

cierto parte del modelo del simulador de procesos.

A continuación se muestran las Tablas 4.15 a 4.18, de estados considerados y requeridos para los sistemas y componentes implementados. La lista completa de sistemas y componentes implementados se puede consultar en las Tablas 4.19 y 4.20.

Sistema	**Estado COPMA**	**Estado TRETA**	**Descripción de estado**			
RXTRIP, TBTRIP, CNTI, MSI e IA	OFF	0	No actuado			
	ON	1	Actuado			
	BLOCKED	8	Bloqueado			
	FAILED	9	Fallo total del sistema			
SI	OFF	0	No actuado			
	ON	1XX	Fase de inyección	**Trenes operativos**		
				XX	**CVCS**	**RHR**
				32	3	2
				22	2	2
	RCCLFS	2XX	Recirculación a ramas frías	12	1	2
				02	0	2
				31	3	1
				21	2	1
	RCHLFS	3XX	Recirculación a ramas calientes	11	1	1
				01	0	1
				30	3	0
				20	2	0
				10	1	0
	FAILED	9	Fallo total del sistema			
AFW	OFF	0	No actuado			
	ON	1XX	Inyectando	**Trenes operativos**		
				XX	**TBB**	**MBB**
				12	1	2
				11	1	1
				10	1	0
				02	0	2
				01	0	1
	FAILED	9	Fallo total del sistema			
CCW, ESW	OFF	0	No actuado			
	ON	1X	Inyectando	**Trenes operativos**		
				X	**MBB**	
				2	2	
				1	1	
	FAILED	9	Fallo total del sistema			
CNTSP	OFF	0	No actuado			
	READY	1	Arrancado			
	ON	2	Actuado			
	FAILED	9	Fallo total del sistema			
FW	OFF	0	No actuado			
	ON	1X	Inyectando	**Trenes operativos**		
				X	**TBB**	
				2	2	
				1	1	
	ISOLATED	8	Aislado			
	FAILED	9	Fallo total del sistema			
SGIS#	OFF	0	No actuado			
	ON	1	Actuado			

Tabla 4.15: Estados de operación considerados para los sistemas implementados.

Sistema	Estado COPMA	Estado TRETA	Descripción del estado requerido
RXTRIP, IA, TBTRIP, CNTI y MSI	STOP	0	Parar
	START	1	Actuar
	BLOCK	8	Bloquear
SI	STOP	0	Parar
	START	1	Fase de inyección
	RCCLFS	2	Fase de recirculación a ramas frías
	RCHLFS	3	Fase de recirculación a ramas calientes
AFW	STOP	0	Parar
	START	1	Inyectar
CCW, ESW	STOP	0	Parar
	START	1	Arrancar
CNTSP	STOP	0	Parar
	RUN	1	Arrancar
	START	2	Actuar
FW	STOP	0	Parar
	START	1	Inyectar
	ISOLATE	8	Aislar

Tabla 4.16: Estados requeridos considerados para los sistemas implementados.

Componente / Variable física	Estado COPMA	Estado TRETA	Descripción
Bombas	RUNNIG	1	Arrancada
	STOPPED	0	Parada/Disparada
	BLOCKED	-1	Bloqueada/ No disponible
	FAILED	9	Fallada
Válvulas	OPEN	1	Abierta
	OPENING	2	Abriendo
	CLOSED	-1	Cerrada
	CLOSING	-2	Cerrando
	INTERM	0	Regulando
	FAILED	9	Fallada

Tabla 4.17: Estados considerados para componentes.

Componente / Variable física	Estado COPMA	Estado TRETA	Descripción
Bombas	START	1	Arrancar
	STOP	0	Parar/Disparar
Válvulas	OPEN	1	Abrir
	CLOSE	-1	Cerrar

Tabla 4.18: Estados requeridos considerados para componentes.

Sistema	Descripción
AFW	Sistema de agua de alimentación auxiliar
CCW	Sistema de agua de refrigeración de componentes
CNTI#	Fases A/B del sistema de aislamiento del recinto de contención
CNTSP	Sistema de rociado del recinto de contención
ESW	Sistema de agua de servicios esenciales
FW	Sistema de agua de alimentación
IA	Sistema de aire de instrumentos
MSI	Sistema de aislamiento de las líneas de vapor
PZRRVTK	Tanque de alivio del presionador
RXTRIP	Disparo del reactor
SI	Sistema de inyección de seguridad
TBTRIP	Disparo de turbina
SGIS#	Sistema de aislamiento de los generadores de vapor

Tabla 4.19: Sistemas implementados en COPMA-III.

Componente	Descripción
AFWPU#	Bombas del sistema AFW (2 MDP 1 TDP)
CCWPU#	Bombas del sistema CCW (2)
CDPU#	Bombas de condensado (3)
CHPU#	Bombas de carga (3)
CNTSPPU#	Bombas del sistema CNTSP (4)
ESWPU#	Bombas del sistema ESW (2)
FWPU#	Turbobombas del sistema FW (2)
MSBPIV	Válvulas de aislamiento de líneas de bypass de vapor principal
MSIV#	Válvulas de aislamiento de líneas de vapor (3)
MSRV#	Válvulas de alivio de vapor a la atmósfera (3)
MSRVCD	Válvulas de alivio de vapor al condensador (8)
PZRRV#	Válvulas de alivio del PZR (2)
PZRRV#IV	Válvulas motorizadas de aislamiento de las válvulas de alivio del PZR (2)
PZRSPV#	Válvulas de ducha normal del PZR (2)
RCSPU#	Bombas del primario (3)
RHRPU#	Bombas del sistema RHR (2)

Tabla 4.20: Componentes implementados en COPMA-III.

4.4.1.3 Implementación de parámetros físicos del proceso

Las variables físicas se corresponden con variables numéricas de COPMA-III. En los EOP se realizan dos tipos de evaluaciones sobre magnitudes físicas, distinguiendo validaciones numéricas, Tabla 4.21, que se realizaran sobre la variable numérica de la magnitud, campo *value*, y validaciones de estado de la variable, Tabla 4.22, donde se evalúa la tendencia de la magnitud, campos *tendency*. Así, por cada magnitud física implementada en COPMA-III, existirán dos campos, uno numérico y otro simbólico, valor y tendencia de la magnitud física considerada, respectivamente. La lista completa de magnitudes físicas implementadas en COPMA-III se puede consultar en la Tabla 4.23.

Variable	Evaluaciones	Evaluaciones COPMA
Caudal	$=$	$=$
Flujo neutrónico	$\neq$	$\neq$
Nivel	$><$	$><$
Presión	$\geq$	$\geq$
Temperatura	$\leq$	$\leq$

Tabla 4.21: Evaluación numérica de variables físicas.

Estado COPMA	Estado TRETA	Descripción
INCREASING	1	Aumentando
DECREASING	-1	Disminuyendo
STEADY	0	Estable

Tabla 4.22: Estados considerados para las variables físicas.

Magnitud física	Descripción
AFWF	Caudal del sistema AFW para cada SG
CFLUX	Flujo neutrónico en el núcleo
CHF	Caudal de SI
CNTPR	Presión en la contención
DSLPR#	Ritmo de variación de la presión en las líneas de vapor (3)
FWF	Caudal del sistema FW
PZRL	Nivel del presionador
PZRPR	Presión en el presionador
RCSAVGT	Temperatura media del primario
RCSCLTAVG	Temperatura media de ramas frías del primario
RCSSUBTC	Subenfriamiento del RCS (termopares salida núcleo)
RHRPUF#	Caudal de las bombas del RHR (2)
RODPOS	Posición de las barras de control
SG#LNR	Nivel de rango estrecho del SG (3)
SG#PR	Presión en el SG (3)
SLPR#	Presión en las líneas de vapor

Tabla 4.23: Magnitudes físicas implementadas en COPMA-III.

4.4.2 Ejemplo de computerización de un procedimiento

Tras haber presentado las capacidades de computerización del lenguaje Prola, se ha considerado llevar a cabo su aplicación a la codificación a un procedimiento de ejemplo para ilustrar la naturaleza del proceso de computerización de los procedimientos.

Partiendo de un procedimiento de ejemplo, Figura 4.22, primeramente se deben identificar los pasos presentes en el procedimiento, el conjunto de instrucciones que los componen, las notas y precauciones que los afectan y, finalmente, la estructura de acciones del operador consideradas en su ejecución, pudiéndose agrupar las mismas en subtareas derivadas de los pasos en función del modelado de sistemas y componentes que se haya realizado en el modelo de planta, Figura 4.23.

Una vez realizada esta actividad, se identifican las instrucciones Prola adecuadas para la computerización de las subtareas identificadas, relacionándose cada una de ellas con una instrucción en la implementación del procedimiento computerizado, Tabla 4.24. En paralelo, se identifican las variables necesarias y su tipo, relacionándolas con cada subtarea, Tabla 4.25.

Finalmente, el proceso de computerización se lleva a cabo empleando el editor PED-II, obteniendo como resultado un procedimiento computerizado que mantiene en todo lo posible la funcionalidad y estructura del procedimiento original, Figura 4.24.

Cabe comentar, que la implementación de actuaciones que impliquen manipulación de componentes, suelen conllevar de forma implícita, aunque no se especifique en los procedimientos, la comprobación de que se obtienen los resultados esperados tras la ejecución de la acción demandada en el procedimiento. Por ejemplo, tras la instrucción 12.a.2 del paso 12 del procedimiento, tal vez fuese necesario implementar la instrucción adicional 12.a.3 de comprobación sobre la velocidad angular de la bomba (AUTOCHECK sobre PISPAUX.*speed*). Normalmente, la verificación del resultado de actuaciones que no se contempla en los procedimientos suele llevar asociadas actuaciones de recuperación locales. En este sentido, su implementación desde el punto de vista del impacto sobre la actuación de sistemas y componentes en la simulación puede tener o no importancia, sin embargo es necesario considerar el tiempo demandado y la carga de trabajo asociadas a las actuaciones de verificación que se realicen en la sala de control pudiéndose modelar en caso de que no tengan impacto en el modelo de simulación como instrucciones MESSAGE.

PRECAUCIÓN

- SI EL NIVEL DEL TANQUE BP-20 ES INFERIOR AL 30 %, PASAR AL PROCEDIMIENTO DE INYECCIÓN DE EMERGENCIA EOP E-23B INMEDIATAMENTE, ABANDONANDO CUALQUIER ACTUACIÓN YA INICIADA.

Paso	Accion/respuesta esperada	Respuesta no obtenida
11	**Energizar barras C/D:** a. Arrancar generador diesel GD-3.	
12	**Verificar actuación del sistema de inyección a presión (PIS):** a. Bombas de inyección - AL MENOS UNA EN FUNCIONAMIENTO	a. Arrancar bomba auxiliar del PIS.
	b. Caudal de inyección en la descarga del PIS - SUPERIOR a 30 m^3/h	b. Verificar apertura máxima de la válvula de descarga PIS1FCV.
13*	**Comprobar presión del tanque BP-20:** a. Si la presión en el tanque BP-20 es SUPERIOR A 74 kg/cm^2 la válvula de alivio deberá estar abierta.	a. Pasar al procedimiento de despresurización de emergencia, EOP E-23A.
14	**Comprobar nivel del tanque BP-20** **- ESTABLE O AUMENTANDO**	Iniciar inyección manual de emergencia mediante la apertura de la válvula TX-20 del tanque presurizado PT-20. SI NO, Pasar a EOP E-23B, ACTUACIONES EN CASO DE PRESIÓN ALTA Y/O INVENTARIO REDUCIDO, Pasos 17 en adelante.
15	...	...

* Paso de acción continua.

Figura 4.22: Procedimiento de ejemplo para mostrar el proceso de computerización.

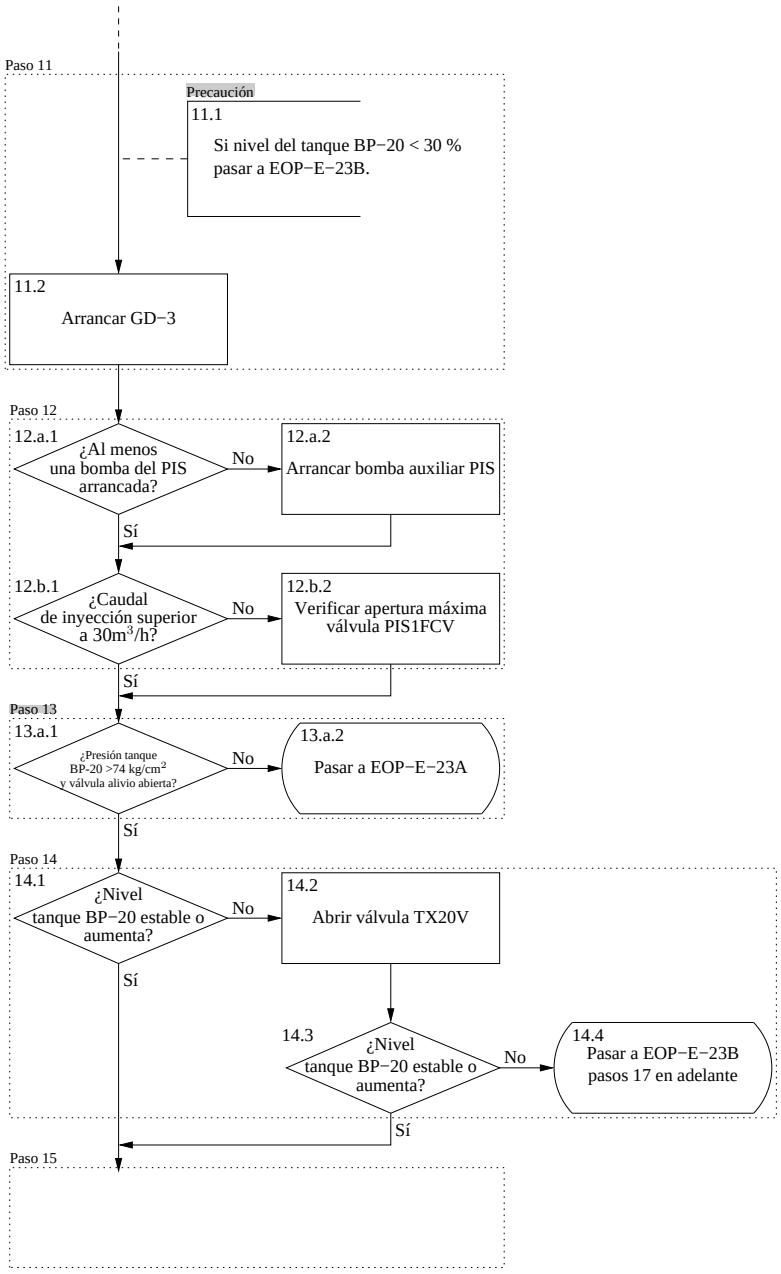


Figura 4.23: Esquema del procedimiento de ejemplo para mostrar el proceso de computerización.

Paso	Tipo de paso	Subtareas consideradas	Instrucción Prola
11	C	11.1	MONITOR
		11.2	ACTION
12	B	12.a.1	AUTOCHECK
		12.a.2	ACTION
		12.b.1	AUTOCHECK
		12.b.2	ACTION
13	D	13.a.1	MONITOR con INITIATE
14	A	14.1	AUTOCHECK
		14.2	ACTION
		14.3	AUTOCHECK
		14.4	INITIATE

Tabla 4.24: Tipos de pasos, tareas identificadas e instrucciones Prola asociadas para el procedimiento de ejemplo.

Subtareas consideradas	Instrucción Prola	Tipo de variable	Variable de ejemplo
11.1	MONITOR	*physmagnitude*	BP20LEVEL.*value*
11.2	ACTION	*generalvariable*	DG3.*mode*
12.a.2	ACTION	*pumpcomponent*	PISPAUX.*command*
14.1	AUTOCHECK	*physmagnitude*	BP20LEVEL.*tendency*

Tabla 4.25: Algunas de las tareas identificadas, instrucciones Prola y variables asociadas para el procedimiento de ejemplo.

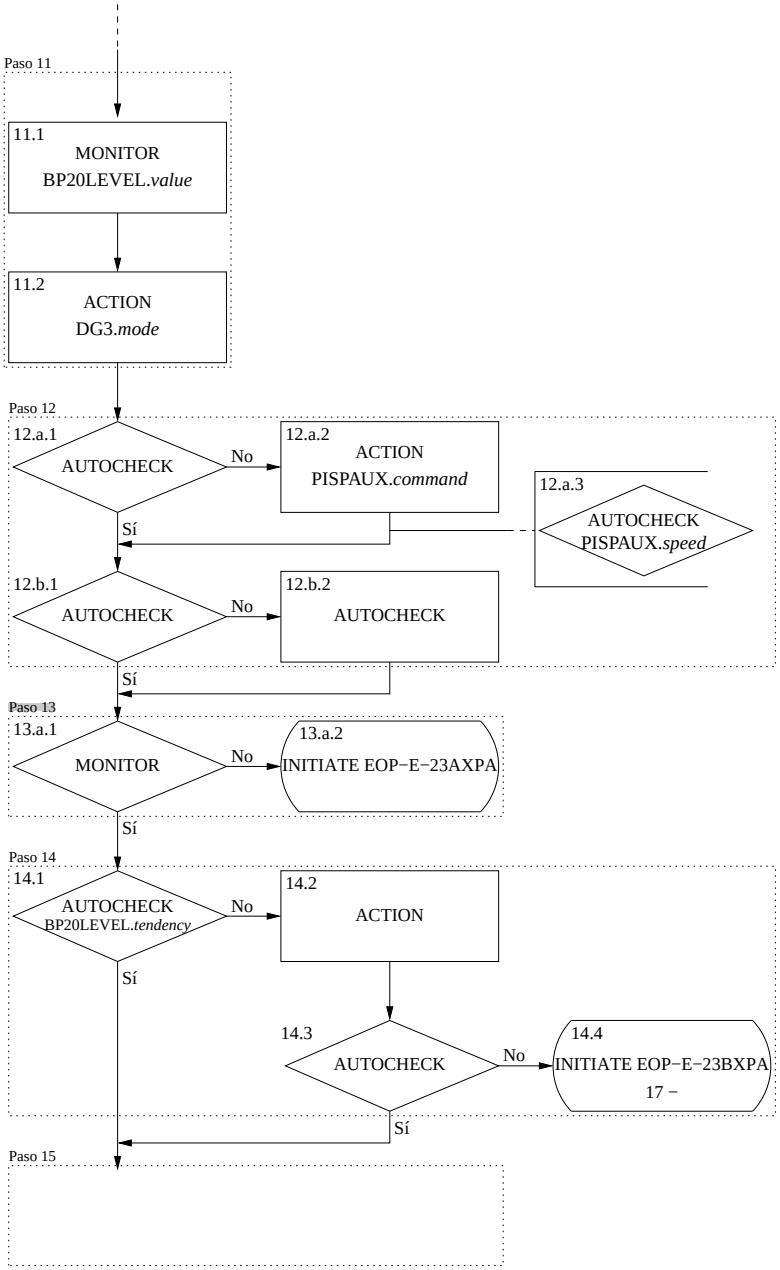


Figura 4.24: Esquema del procedimiento de ejemplo computerizado.

4.4.3 Modelos desarrollados de los EOP y pruebas realizadas

Para verificar las capacidades de modelado de las herramientas escogidas para la codificación del modelo, las funcionalidad del traductor de Prola a las estructuras XPA del núcleo, la PDB y la MMI del sistema COPMA-III, y que todo el proceso de computerización da como resultado un modelo de procedimientos funcional para el sistema COPMA-III, se desarrollaron dos aproximaciones al modelado de procedimientos, una de alto detalle y otra de bajo detalle, y un conjunto de pruebas de ejecución de los procedimientos sin acoplamiento del sistema COPMA-III a un simulador de procesos, sino realizando su ejecución mediante una consola manual desarrolla al efecto.

En lo que respecta a los modelos de EOP desarrollados, comentar que se realizó la codificación detallada de los EOP:

- E-0: Procedimiento de Disparo del reactor y/o Inyección de Seguridad.
- E-1: Procedimiento de pérdida de refrigerante del reactor o secundario.
- E-2: Procedimiento de aislamiento de un Generador de Vapor defectuoso.

La computerización se llevó a cabo realizando la codificación de los pasos de los procedimientos de forma completa, respetando su estructura y manteniendo su alcance funcional. El objetivo era comprobar las capacidades de codificación de las herramientas empleadas, el editor PED-II y el traductor de Prola a XPA, así como la flexibilidad del lenguaje Prola. El resultado de esta implementación para el conjunto de los procedimientos se en encuentra en las referencias Expósito y Queral (2004ab 2005a).

Por otro lado, se realizó la codificación de nivel de detalle reducido de un conjunto de procedimientos, considerando solo aquellas actuaciones demandadas que pudiesen tener importancia desde el punto de vista de la simulación termohidráulica. Los EOP computerizados fueron, Expósito y Queral (2006a):

- E-0: Procedimiento de Disparo del reactor y/o Inyección de Seguridad.
- E-0.1: Procedimiento de recuperación del disparo de reactor.
- E-1: Procedimiento de pérdida de refrigerante del reactor o secundario.
- ES-1.1: Procedimiento de finalización de Inyección de Seguridad.
- E-2: Procedimiento de aislamiento de un Generador de Vapor defectuoso.
- FR-H.1: Respuesta ante la pérdida de sumidero de calor.

Este modelo se describe en profundidad en el Capítulo 6, donde se aplicó a la simulación de secuencias de roturas de secundario. Mucho más sencillo que el modelo de procedimientos de alto nivel de detalle presentado en este apartado, su finalidad consiste, exclusivamente, en evaluar la funcionalidad de la herramienta.

Para la realización de las pruebas de los modelos de procedimientos computerizados sin acoplamiento con el simulador de procesos el grupo de trabajo de la UCM con el apoyo del grupo de investigación del DSE desarrolló una consola de ejecución manual de los EOP contra COPMA-III, Figura 4.25. Con esta herramienta se verificaron los diferentes modelos de procedimientos realizados obteniendo resultados satisfactorios. Como ejemplo, se incluye los resultados de una de las pruebas realizadas empleando la consola manual con el EOP E-0 en su versión de computerización detallada, visualizando el flujo de la ejecución mediante la MMI del sistema COPMA-III, Figuras 4.26 a 4.28.

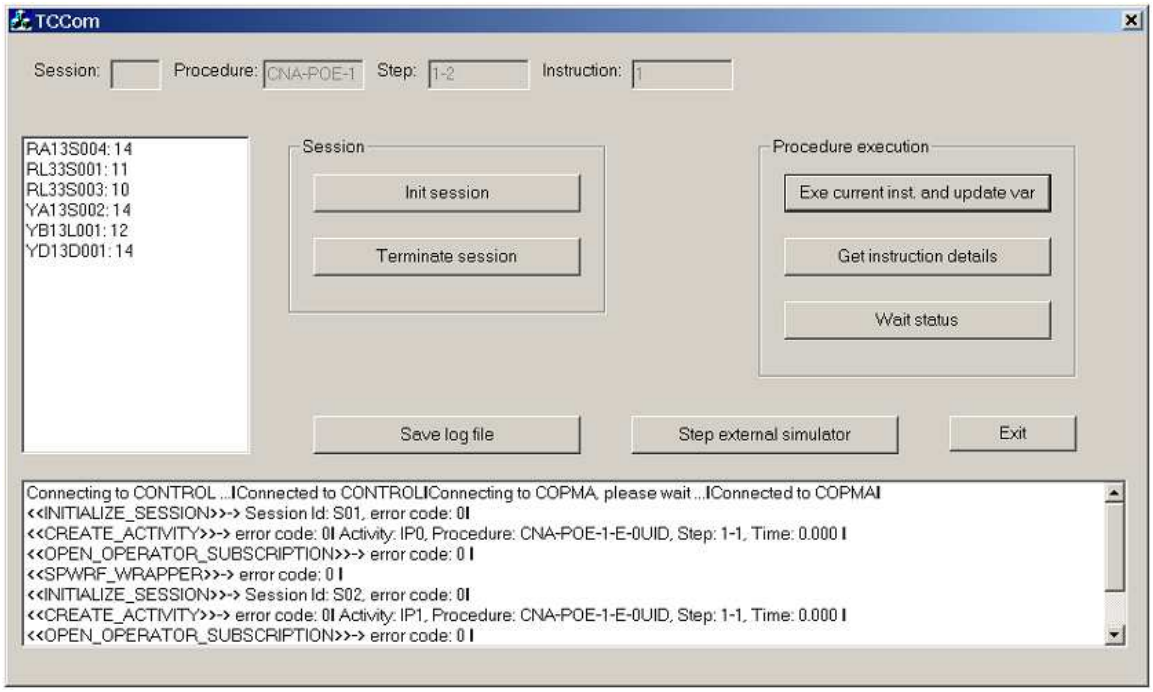


Figura 4.25: Consola desarrollada para la ejecución manual de los EOP computerizados.

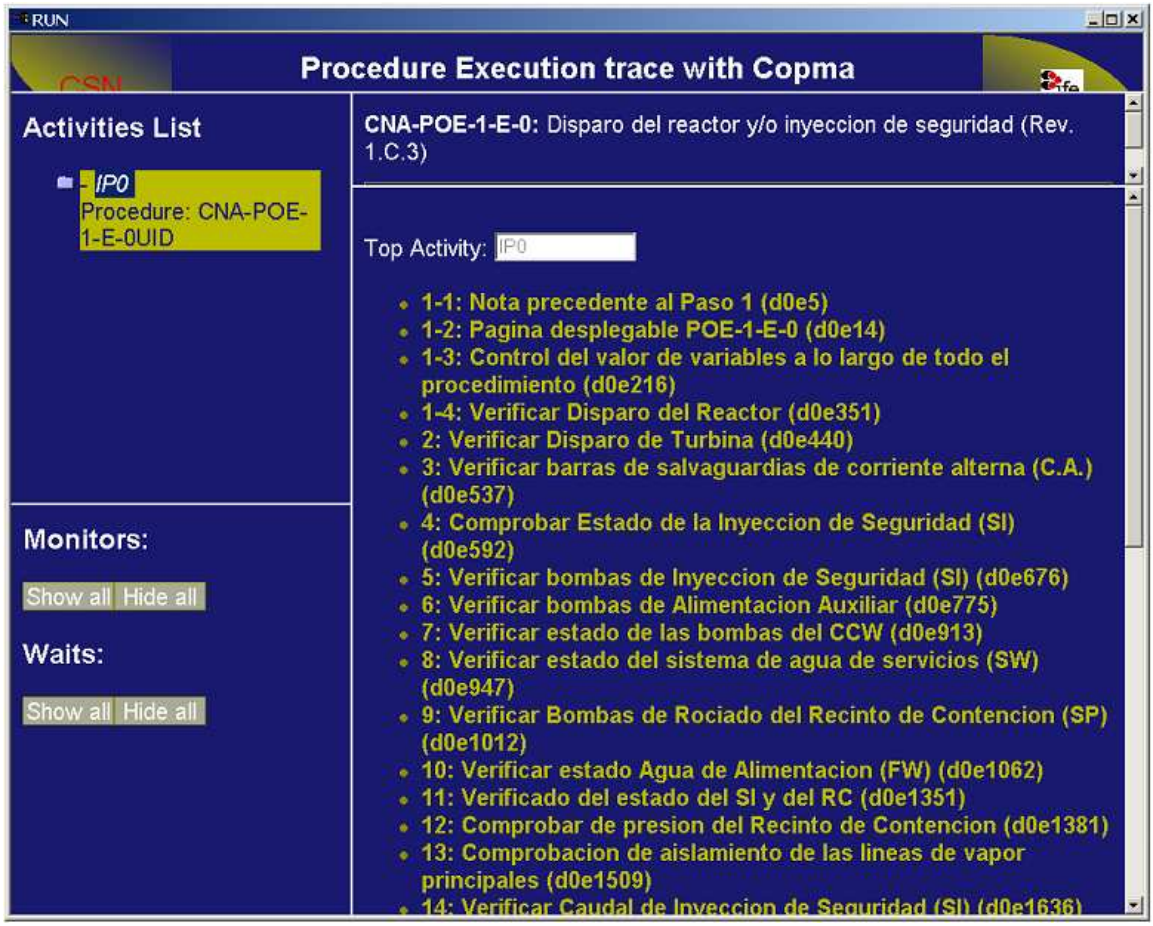


Figura 4.26: Resultados de las pruebas realizadas sobre el modelo computerizado del EOP E-0: pantalla primera.

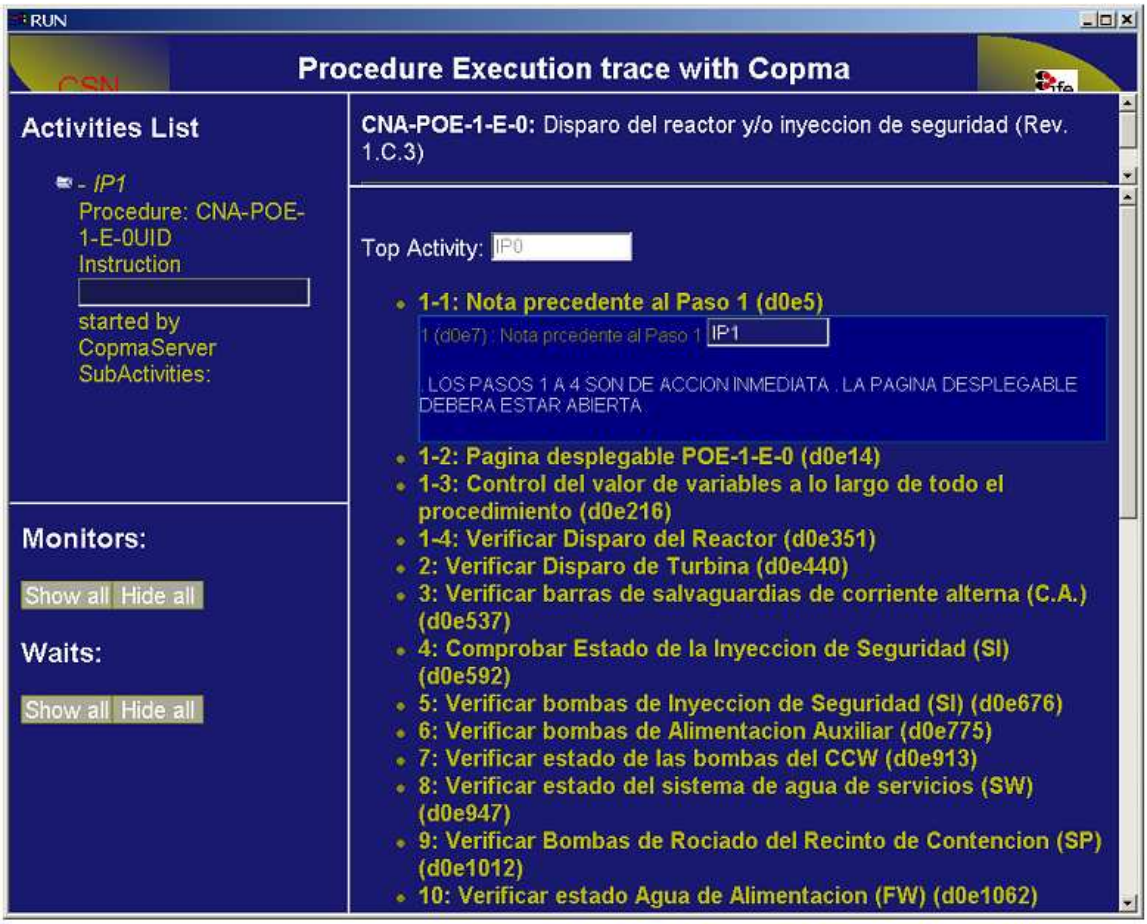


Figura 4.27: Resultados de las pruebas realizadas sobre el modelo computerizado del EOP E-0: pantalla segunda.

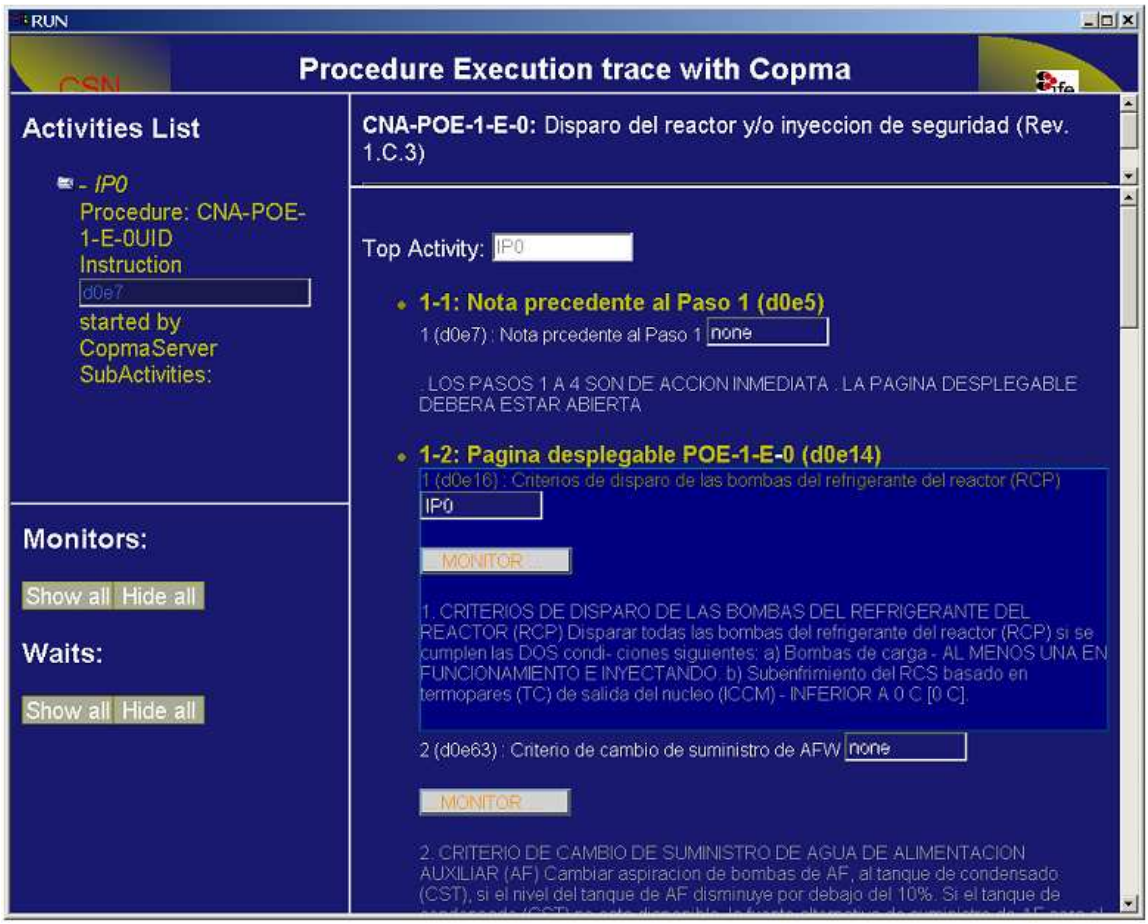


Figura 4.28: Resultados de las pruebas realizadas sobre el modelo computerizado del EOP E-0: pantalla tercera.

4.5 Conclusiones relativas a la computerización de los EOP de un PWR-W

Tras la realización del modelo de procedimientos se han determinado dos tipos de limitaciones:

- las referentes a la edición de procedimientos computerizados, relacionadas con el editor PED-II y
- las relativas a los problemas surgidos en la interpretación de los procedimientos y el proceso de su computerización.

Ambos puntos se tratan en detalle a continuación.

4.5.1 Limitaciones de la edición con PED-II y posible solución

Durante el trabajo realizado con el editor PED-II, se encontraron ciertas deficiencias en su funcionamiento que, aunque pudieron ser solventadas, han motivado el planteamiento de la necesidad de desarrollar un editor de procedimientos enfocado directamente a la edición de los mismos en formato XML. Esta opción no presenta demasiada complejidad en su desarrollo ya que existen aplicaciones tanto comerciales como GNU aptas para este fin, pudiéndose considerar como un desarrollo futuro.

4.5.2 Problemas de interpretación de los EOP

De forma general, durante la computerización de los EOP, se han encontrado problemas a la hora de determinar estrategias de actuación del operador en ciertos pasos de los procedimientos. Es así en el caso de:

- Actuaciones específicas que están estipuladas formalmente pero su contenido no consta en los procedimientos escritos.
- Actuaciones delegadas al criterio del operador.
- Vigilancia de condiciones de operación de sistemas, estado de componentes o variables físicas.
- Las actuaciones de control sobre variables físicas.
- La computerización de precauciones y notas del EOP escrito.
- Pasos cuya computerización presentan dificultades en su interpretación y/o computerización.

- Simulación de carga de trabajo y tiempo de ejecución de las acciones a realizar por el operador.

Estos aspectos se tratan de forma detallada a continuación:

1. **Actuaciones específicas que están estipuladas formalmente pero su contenido no consta en los procedimientos escritos y actuaciones delegadas al criterio del operador.**

   En el caso de las actuaciones no informadas en el procedimiento escrito o delegadas al criterio del operador, si estas actuaciones se encuentran documentadas se debería disponer de esta documentación para decidir como realizar su implementación.

2. **Vigilancia de condiciones de operación de sistemas, estado de componentes o variables físicas.**

   Los pasos de acción continua y la página desplegable han supuesto un esfuerzo considerable en computerización, pues rompen la estructura de ejecución secuencial del procedimiento, requiriendo un tratamiento en paralelo durante la ejecución. Este tratamiento en paralelo, desde el punto de vista de la simulación, supone un problema a la hora de emular la carga de trabajo y los tiempos de ejecución de estas sentencias. Por ahora no se ha encontrado un criterio definido en la ejecución de acciones de vigilancia continua en lo que respecta a este tipo de elementos estructurales de los procedimientos. Para su computerización se han empleado sentencias MONITOR. Este tipo de sentencias simulan vigilancia continua, no siendo así la vigilancia real que el operador realiza de las condiciones evaluadas en las mismas, estando supeditada a disponibilidad por carga de trabajo. Además, la vigencia de estas sentencias ha requerido la implementación de variables lógicas adicionales de control de vigencia, para finalizar el monitorizado. Todo ello, a generado una estructura de sentencias de vigilancia que se diferencia fuertemente del concepto de vigilancia a desempeñar por el operador. Queda por resolver si es correcta esta implementación. En un futuro podría considerarse otra vía, cuya discusión se debe realizar, siendo ésta la de implementar la vigilancia de los parámetros como una actividad independiente que se iniciase en momentos puntuales en los que el operador considerase que las condiciones de carga de trabajo lo permiten, llegando incluso a considerar criterios subjetivos en la asignación de prioridades.

3. **Las actuaciones de control sobre variables físicas.**

   Otro aspecto relevante, es la implementación de pasos de los EOP que impliquen dificultad funcional y/o de computerización. Estos pasos suelen caracterizarse por ser pasos que engloban un conjunto de actuaciones sobre diferentes componentes regidas por los efectos que provocan en las condiciones del sistema o una variable física, siendo actuaciones supeditadas al control de ciertas variables físicas y a la consideración del estado de planta (disponibilidad de sistemas, componentes, etc). Este es el caso de la implementación de controles manuales, implementación tratada en el Sección **??**.

4. **La computerización de precauciones y notas del EOP escrito.**

   En ciertos casos, se requiere que las actuaciones solicitadas al operador estén regidas por ciertos criterios que garanticen necesidades de funcionalidad de sistemas o de operación de la planta. Estos criterios son informados al operador mediante notas y/o precauciones, según su naturaleza, localizadas precediendo al primer paso al que afectan. Las precauciones y notas marcan unas pautas generales o normas para realizar la acción informada en el(los) paso(s) subsiguientes. El resultado final del conjunto nota/precaucion y pasos afectados es una actuación condicionada por aspectos operacionales demasiado específicos, que impiden su descripción detallada en el procedimiento escrito. Ejemplos de los casos localizados durante la computerización de los procedimientos son:

   - Nota previa al paso 19, EOP E-0.

     NOTA

     - SE DEBERÁ MANTENER EL CAUDAL DE INYECCIÓN A LOS CIERRES DE TODAS LAS BOMBAS DEL REFRIGERANTE DEL REACTOR (RCP).

     Precaución previa al paso 4, EOP E-2.

     PRECAUCIÓN

     - SI LA TURBOBOMBA DE AGUA DE ALIMENTACIÓN AUXILIAR (AF) CONSTITUYE LA ÚNICA FUENTE DE CAUDAL DE ALIMENTACIÓN DISPONIBLE, SE DEBERÁ ,MANTENER UN SUMINISTRO DE VAPOR PARA ESTE DESDE AL MENOS UNO DE LOS GENERADORES DE VAPOR (SG).

     En estos casos, tanto la exigencia del mantenimiento del caudal de sellos como el del caudal del vapor a la turbobomba de FW, pueden llevar a implicaciones indirectas en la operación de los sistemas relacionados con el cumplimiento de la misma. Este tipo de notas o precauciones llevan asociadas un conocimiento de la operación profundo, requiriendo la evaluación de su computerización la realización de consultas a operadores y/o entrenadores de operadores.

   - Precaución previa al paso 1, EOP E-2.

     PRECAUCIÓN

     - DEBERÁ QUEDAR DISPONIBLE AL MENOS UN GENERADOR DE VAPOR (SG) PARA EL ENFRIAMIENTO DEL SISTEMA DEL REFRIGERANTE DEL REACTOR (RCS).
     - CUALQUIER GENERADOR DE VAPOR (SG) DEFECTUOSO (ROTURA EN EL SECUNDARIO), DEBERÁ QUEDAR AISLADO DURANTE EL CURSO DE LAS SIGUIENTES ACCIONES DE RECUPERACIÓN , A MENOS QUE SEA EL ÚNICO DISPONIBLE Y SE NECESITE PARA EL ENFRIAMIENTO DEL SISTEMA DEL REFRIGERANTE DEL REACTOR (RCS).

     Este tipo de precauciones conlleva un conjunto de validaciones lógicas y, en algunos casos, de SA que requieren para su implementación de la consideración del conjunto de las simulaciones en las que se va a emplear el modelo de procedimientos o el

desarrollo de un modelo cognitivo de toma de decisiones considerando objetivos y metas.

Se deberá desarrollar una metodología de computerización que resuelva la problemática citada anteriormente. Para el primer caso, supondría la implementación de un conjunto de restricciones a la hora de operar sistemas y/o componentes en los pasos afectados. Desde el punto de vista de la computerización, esto implica únicamente un aumento en la complejidad de las condiciones lógicas en las actuaciones. Desde el punto de vista estructural, supondrá una distorsión del procedimiento escrito al ser computerizado, obteniendo, por contra, un EOP computerizado con mayores capacidades para la simulación de transitorios de forma genérica. Sin embargo, para el segundo grupo de elementos, se requiere de la consideración de nuevos modelos de simulación, que consideren aspectos relacionados con la toma de decisiones. Este punto, al no haberse considerado como un desarrollo inicial en la herramienta, se trata como una posible mejora futura en el capítulo 7.

5. **Pasos cuya computerización presentan dificultades en su interpretación y/o computerización.**

   Durante la computerización de los procedimientos se han localizado algunos pasos de difícil interpretación y de los cuales solo se hace una referencia, pues en estos momentos no es prioridad su estudio, al no afectar a los objetivos actuales del proceso de computerización e interpretación de los procedimientos. Por ejemplo, los pasos localizados durante la computerización del EOP E-0 fueron:

   - Paso 28 del EOP E-0: Verificar suministro de aire de instrumentos al recinto de contención.

Paso	Accion/respuesta esperada	Respuesta no obtenida
28	**Verificar suministro de aire de instrumentos al recinto de contención (RC):** (HV-1848) - ABIERTA (HV-1849) - ABIERTA	Verificar un compresor de aire en funcionamiento y establecer suministro de aire de instrumentos al recinto de contención, abriendo las válvulas (HV-1848) y (HV-1849).

   Este paso presenta como evaluación de suministro de aire de instrumentos la simple apertura de las válvulas de suministro, sin considerar el estado de los compresores. Este hecho se pone de manifiesto en la acción correctora que, en caso de no estar las abiertas dichas válvulas, solicita la verificación del estado de al menos un compresor en funcionamiento, verificación que no se realizaría en caso de que el sistema de válvulas estuviesen correctamente alineadas. Este paso **no afecta a la implementación actual** de los modelos de procedimientos.

- Paso 31 del EOP E-0: Comprobar condiciones del tanque de alivio del presionador.

Paso	Accion/respuesta esperada	Respuesta no obtenida
31	**Comprobar condiciones (Presión, temperatura y nivel) del tanque de alivio del presionador - NORMAL**	Evaluar y decidir sobre la causa de las condiciones anómalas.

En este paso no se especifican acciones a realizar en caso de darse condiciones anómalas en el tanque de alivio del presionador. Este punto **no afecta a la implementación actual**.

6. **Simulación de carga de trabajo y tiempo de ejecución de las acciones a realizar por el operador.**

   En el proceso de computerización actual se esta considerando la implementación en las instrucciones del valor de TEXEC como resultado de la ejecución de las mismas. Estos valores se obtienen de diversas fuentes, considerando bibliografía, otras simulaciones, secuencias de simulación en simuladores de sala de control, etc. Sin embargo, para los valores de TASKLOAD que simulan la carga de trabajo de las actuaciones ejecutadas en cada paso no se han considerado el desarrollo de un método de cálculo pues no estaba considerado dentro de los objetivos del trabajo. Una orientación de las posibles líneas de trabajo futuras al respecto se da en el Capitulo 7.

Las diferentes soluciones para estos problemas están siendo estudiadas, y se considerarán la mayor parte como mejoras a implementar dentro del conjunto de trabajos que se están realizando actualmente, comentándose en detalle en la Sección 7.4.

Capítulo 5

Implementación de la conexión entre los códigos TRETA y COPMA-III

Índice

En este capítulo se describe la implementación de las comunicaciones de la herramienta TRETA / COPMA-III. Como se ha descrito en el Capítulo 2, la herramienta TRETA/COPMA-III consiste en el uso conjunto del sistema computerizado de ayuda al operador para el seguimiento de procedimientos de operación COPMA-III, desarrollado dentro del HRP, y el código de simulación de plantas nucleares TRETA, desarrollado por el CSN, Hortal (1996b), Hortal (2002) y Hortal y Nilsen (2002). Las tareas llevadas a cabo para la integración de ambos códigos han sido:

- La definición de la funcionalidad de las comunicaciones, colaborando con el personal del área MOSI del CSN para definición de las especificaciones.

  Esta funcionalidad posibilita la invocación de las funciones de comunicación implementadas en la PDB de COPMA-III por parte de TRETA, permitiendo que el código de simulación de planta pueda gestionar la ejecución de los procedimientos.

- La implementación en ambos códigos de una interfase de comunicaciones basada en la librería de comunicaciones SWBus , desarrollada por del HRP. Para la integración de la API (*Application Programming Interface*) de comunicaciones en ambos códigos de simulación se ha contado, por el lado de la PDB de COPMA-III, con la colaboración del grupo del HRP y, por el lado de TRETA, con la colaboración del grupo de traba de la UCM.

  Para la implementación de la interfase se consideró que la gestión de las comunicaciones debía realizarse mediante un proceso independiente, cuyas capacidades de intercambio de información requiriese una implementación sencilla y conllevase pocas o nulas modificaciones en las especificaciones de ambos códigos. Además, una misma instancia del proceso debería gestionar la interfase y ser capaz de establecer comunicaciones entre varias instancias de ambos códigos de simulación, en una misma computadora o en una plataforma de computación distribuida. Una especificación de especial relevancia, es que este proceso de gestión de la interfase debería permitir que el código de planta y de procedimientos estableciesen comunicación de forma síncrona, es decir, todos los procesos involucrados deben intercambiar la información referente a un instante de tiempo de simulación de forma coherente y consistente, sin provocar demoras significativas del trabajo de simulación. Por ello, la implementación de las comunicaciones debe soportar la sincronización, considerando tanto los procesos de simulación involucrados como la interfase de comunicación.

- La verificación de la funcionalidad de dicha interfase. Para llevar a cabo las pruebas consideradas, se realizó una estancia en la sede del HRP en Halden, en Noruega.

  Durante dicha estancia no solo se mejoró y verificó la funcionalidad de las comunicaciones, sino que se estableció la línea de trabajo para desarrollos futuros.

En cuanto al primer punto, tal vez el más importante, relativo a la funcionalidad de las comunicaciones, se trata en la Sección 5.1. En esta sección se explica de forma detallada el establecimiento de la funcionalidad de las comunicaciones en el marco de la simulación de los

procedimientos de operación de las centrales nucleares y su integración con un simulador termohidráulico de planta. Debido a que ciertos aspectos relativos a la sincronización de los procesos encargados de la simulación afectan a la funcionalidad de las comunicaciones, también se tratará este aspecto en esta en esta misma sección. Esta tarea fue llevada a cabo por el área MOSI del CSN con la colaboración del DSE de la UPM.

En lo que respecta al resto de las especificaciones, se trata en detalle, de una forma u otra, en la sección dedicada a la implementación física de la interfase de comunicaciones, Sección 5.1.3. En dicha sección, se explica las capacidades de comunicación de la librería SWBus, como solución adoptada para implementar la interfase de comunicaciones, y como dicha librería satisface las especificaciones requeridas. La tarea de codificación de la librería de comunicaciones fue realizado por el grupo de la UCM, asistido por el DSE de la UPM.

Finalmente, se incluyen en la Sección 5.2 un ejemplo del tipo de pruebas llevadas realizadas para verificar el desarrollo de la implementación. Realizadas por el grupo de trabajo del DSE de la UPM en el transcurso de mi estancia en el HRP. Las pruebas que se incluyen en esta sección conforman un conjunto completo para la verificación de la funcionalidad de la herramienta, siendo representativas del total de las pruebas realizadas.

5.1 Funcionalidad de las comunicaciones y su implementación física

La especificación de la funcionalidad de las comunicaciones COPMA-III/TRETA tiene como objetivo definir las funciones necesarias, así como sus entradas y salidas, para las comunicaciones entre COPMA-III y TRETA. La filosofía en la especificación de la funcionalidad ha consistido en respetar en todo lo posible las características de diseño propias de los códigos TRETA y COPMA-III. Por este motivo, la primera tarea consistió en la documentación de la implementación de las comunicaciones existentes entre el núcleo de COPMA-III y otros dos módulos del sistema, la PDB y la MMI. Tras finalizar esta tarea, se constató que la mayoría de la funcionalidad de comunicaciones requerida para la implementación de la herramienta estaba desarrollada, debido a necesidades internas del sistema COPMA-III. Este hecho tiene como justificación la idea de que, conceptualmente, el código TRETA desarrolla un papel similar en la simulación al realizado por el MMI del sistema COPMA-III. Sin embargo, y debido a que el sistema COPMA-III se encontraba en fase de desarrollo durante la realización del trabajo, se detectaron ciertas deficiencias en la implementación realizada en el sistema, sirviendo el estudio realizado para mejor las capacidades de simulación de procedimientos del sistema COPMA-III.

Dentro del proceso de la funcionalidad de las comunicaciones decidió que el código de simulación TRETA sería el encargado de dirigir la ejecución de los procedimientos debido, principalmente, al hecho de que el sistema COPMA-III no poseía un reloj interno que le capacitase para la simulación autónoma. Por ello, durante la simulación y en cada paso de tiempo simulado, el intercambio de información entre los códigos TRETA y COPMA-III se estructuró como:

1. **Inicio de la simulación**. Se deben inicializar los códigos de forma consistente, aunque para mayor solidez se realizará una llamada de inicialización de las variables de simulación a la PDB de COPMA-III. El código TRETA será el encargado de dar la orden de inicialización al sistema COPMA-III con los parámetros requeridos para llevar a cabo la simulación del modelo considerado.

2. Los ciclos de simulación se componen de:

   (a) **Ejecución de los procedimientos bajo demanda de TRETA**. El código TRETA debe realizar la simulación de los procedimientos para ese intervalo de tiempo, interaccionando para ello con el sistema COPMA-III. El resultado de la simulación de los procedimientos será reportado por COPMA-III a TRETA en la última etapa de simulación de este paso de tiempo, etapa 2e.

   (b) **Simulación del proceso por parte de TRETA**. Posteriormente, el código TRETA realiza la simulación termohidráulica del modelo de planta.

   (c) **Paso de valores de variables de proceso del código TRETA a COPMA-III**. Una vez llevada a cabo la simulación termohidráulica, el código TRETA debe suministrar al núcleo de COPMA-III los valores de las variables de todas las variables definidas como necesarias, estados de sistemas/componenes y valores de magnitudes físicas.

   (d) **Evaluación de los elementos vigentes de los procedimientos por parte de COPMA-III**. Evaluación por parte del núcleo de COPMA-III del estado de la ejecución de los elementos de las actividades vigentes, comprobando las condiciones de vigilancia y espera de las mismos.

   (e) **Toma del estado de las actividades y de los valores de las variables del modelo de procedimientos de COPMA-III por parte de TRETA**. El código TRETA debe obtener de la PDB de COPMA-III el estado de componentes y sistemas que se debe considerar para la simulación de la planta en el siguiente paso de tiempo. Al requerirse un intercambio de información síncrono, esta etapa no deberá ejecutarse hasta que la etapa 2d se realice de forma completa.

3. **Finalización de la simulación**. Una vez finalizada la simulación temporal, gestionada por TRETA, se debe concluir la simulación de los procedimientos, terminando la ejecución de ambos códigos.

Para tratar las funciones especificadas para cada etapa, se presenta, primeramente, el criterio empleado para definir la funcionalidad de la ejecución automática de los procedimientos en base a los requerimientos derivados de la simulación, etapas 1, 2c, 2e y 3. Seguidamente, se añadirá a dicha funcionalidad la derivada de la estructura, dependencias y contenido de los procedimientos, etapa 2a. En lo que respecta a las etapas 2b y 2d, no se requiere la implementación de funciones de comunicaciones ya que se corresponden con etapas de simulación interna de cada código.

Finalmente, se define formalmente el conjunto las funciones a emplear para la implementación de la funcionalidad definida, la estructura de datos requerida para la gestión de la información

contenida en los procedimientos y como se ha llevado a cabo la implementación física del conjunto.

5.1.1 Funcionalidad de las comunicaciones en base a los requerimientos derivados de la simulación

En lo que respecta a las etapas relacionadas con aspectos derivados de la simulación, se ha definido el siguiente conjunto de funciones:

- Etapa 1: **inicio de la simulación**.

  Función INITIALIZE_SESSION: realiza el registro del proceso TRETA en el sistema COPMA-III, preparando al sistema COPMA-III para la simulación del modelo de planta considerado por TRETA. En este sentido, deberá informar a COPMA-III de cual será la base de datos de procedimientos a emplear y el conjunto de ficheros de configuración relacionados con su simulación.

  Función SPWRF_WRAPPER: esta función, en su primera llamada, suministra a la PDB del sistema COPMA-III el valor de todas las variables de proceso gestionadas por TRETA para la simulación que se esté llevando a cabo. De esta forma se inicializa la PDB de COPMA-III al instante inicial de la simulación. Como es lógico, esta información es suministrada de forma síncrona, es decir, se espera que a partir de esta llamada, el valor de las variables de estado demandado de componentes y sistemas sea coherente con el valor de las variables de proceso suministradas a la PDB de COPMA-III. En este sentido, **esta función es la encargada de la sincronización** de los códigos TRETA y COPMA-III.

  Función OPEN_OPERATOR_SUBSCRIPTION: en la validación de un procedimiento, normalmente no es necesario conocer la evolución de todas las variables gestionadas por la PDB de COPMA-III o TRETA. Para poder implementar este aspecto, se ha implementado una técnica de suscripción, mediante la cual TRETA solo suscribe aquellas variables, especificadas en su fichero de entrada, de la PDB de COPMA-III que van a ser entradas para el TRETA. Ese conjunto de variables, gestionadas por COPMA-III, serán las que presenten interés para la simulación en TRETA, siendo comprobadas en la etapa 2e para su envió al código TRETA en caso de que su valor haya experimentado algún cambio.

- Etapa 2c: **paso de valores de variables de proceso del código TRETA a COPMA-III**.

  Función SPWRF_WRAPPER: esta función, en las posteriores llamadas que se realicen tras la etapa 1, suministrará a la PDB el valor de las variables de proceso que hayan experimentado algún cambio en su contenido durante la simulación del proceso llevada a cabo por TRETA. Como ya se ha comentado, **esta función es la encarga de la sincronización**, por lo que se obliga a que todas las actividades del núcleo de COPMA-III se evalúen en la etapa 2d, y reporten su estado de acuerdo a los nuevos valores de las variables de proceso suministrados por TRETA en la etapa 2a.

- Etapa 2e: **toma del estado de las actividades y de los valores de las variables del modelo de procedimientos de COPMA-III por parte de TRETA**.

  Función PROC_VAR_UPDATES: esta función suministra al código TRETA las variables suscritas en la etapa 1 que hayan experimentado algún cambio en su valor.

- Etapa 3: **finalización de la simulación**.

  Función TERMINATE_SESSION: informa al sistema COPMA-III de la intención de finalizar la simulación de los procedimientos. COPMA-III debe finalizar la simulación cerrando cualquier actividad aún vigente o, en su defecto, ignorar la llamada informando de la existencia de actividades pendientes de gestionar.

5.1.2 Funcionalidad de las comunicaciones en base a los requerimientos derivados de los procedimientos

El conjunto de funciones que se requieren para la ejecución de los procedimientos por parte del núcleo de COPMA-III bajo demanda de TRETA, durante la etapa 2a, son:

- **Función GET_EVALUATIONS_AND_VALUES**: esta función se debe usar para comprobar el estado de la vigilancia de variables de proceso, MONITOR, y actualizarlo de acuerdo con las condiciones que vigilan. También da información acerca de las actividades que se encuentren en espera, realizando un chequeo de las condiciones de espera. Además, esta función devuelve los valores actualizados de las variables suscritas previamente con la llamada a OPEN_OPERATOR_SUBSCRIPTION, de la misma forma que la función PROC_VAR_UPDATES, por si esta información fuese requerida por TRETA durante la ejecución de los procedimientos.

- **Función CREATE_ACTIVITY**: esta función crea una actividad en la sesión actual para ejecutar el procedimiento especificado. Será necesario crear una actividad por cada procedimiento que se quiera ejecutar desde TRETA.

- **Función SWITCH_TO_ACTIVITY**: esta función se emplea durante la ejecución de los procedimientos para informar al núcleo de COPMA-III de la actividad, asociada a un procedimiento en ejecución, que se va a ejecutar.

- **Función GET_INSTRUCTION_DETAILS**: esta función se emplea para obtener los detalles asociados a la instrucción actual de una actividad, tales como el tipo de instrucción y los valores de los parámetros TEXEC y TASKLOAD.

- **Función EXECUTE_CURRENT_INSTRUCTION**: esta función se usa para ejecutar la instrucción actual y obtener la información relativa a la siguiente en el flujo lógico del procedimiento.

- **Función END_ACTIVITY**: esta función finaliza una actividad iniciada por CREATE_ACTIVITY.

5.1.3 Implementación física de la interfase de comunicaciones

La implementación de la interfase de comunicaciones del simulador integral se basa en tres elementos, Figura 5.1:

- El **gestor de comunicaciones**. La solución escogida en lo que respecta al protocolo de comunicaciones, tal como se introdujo en el Capítulo 2, consiste en el uso de la librería de comunicaciones *Software Bus* (SWBus), desarrollada por el HRP, del cual se realiza una descripción en la Sección 5.1.3.1.
- La implementación de la **API definida en la PDB** del sistema COPMA-III. El grupo del HRP realizó la implementación de la funcionalidad especificada en la sección anterior, de la cual se hace una definición detallada en la Sección 5.1.3.2.
- La implementación de las llamadas a dicha API en la **interfase de comunicaciones de TRETA**, basada en SWBus. Por otra parte, el grupo de trabajo de la UCM, con el apoyo del DSE de la UPM y el personal del área MOSI del CSN, realizó la codificación de las llamadas de las funciones implementadas en la PDB de COPMA-III mediante métodos de SWBus, describiéndose dicho trabajo en la Sección 5.1.3.3. La implementación se realizó en los módulos *copma3* y *CopmaCrew* del código TRETA.

En las secciones siguientes se hace una descripción detallada de los diferentes elementos presentados.

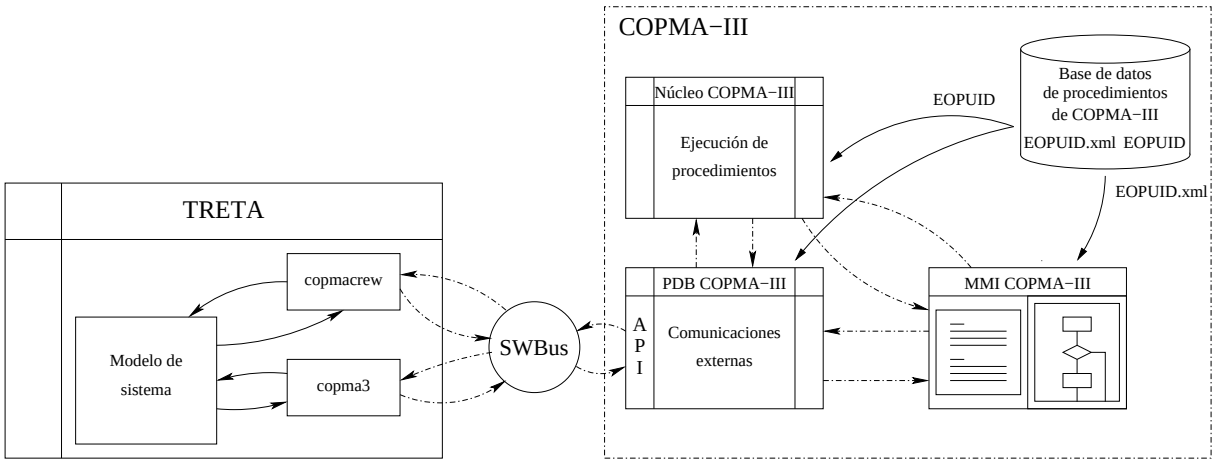


Figura 5.1: Esquema de la implementación física de la interfase TRETA / COPMA-III.

5.1.3.1 Gestión de la interfase de comunicaciones. La librería de comunicaciones SWBus

Software Bus (SWBus) es un sistema de comunicaciones basado en objetos capaz de administrar un conjunto dinámico de objetos distribuidos. Las aplicaciones que usan objetos tipo SWBus son capaces de compartir datos y funcionalidad con otros procesos corriendo en diferentes

sistemas sobre la red, Figura 5.2. Es decir, una aplicación corriendo en una máquina puede tener un conjunto de métodos y datos que pueden ser usados por otra aplicación en otra maquina diferente de forma trasparente a través de una conexión TCP/IP mediante SWBus. Para gestionar la información, SWBus usa un sistema subyacente de mensajes basados en TCP/IP, de manera que la conversión de los datos transferidos entre procesos se realiza de forma transparente para el programador mediante el uso de objetos desarrollados para su uso a alto nivel.

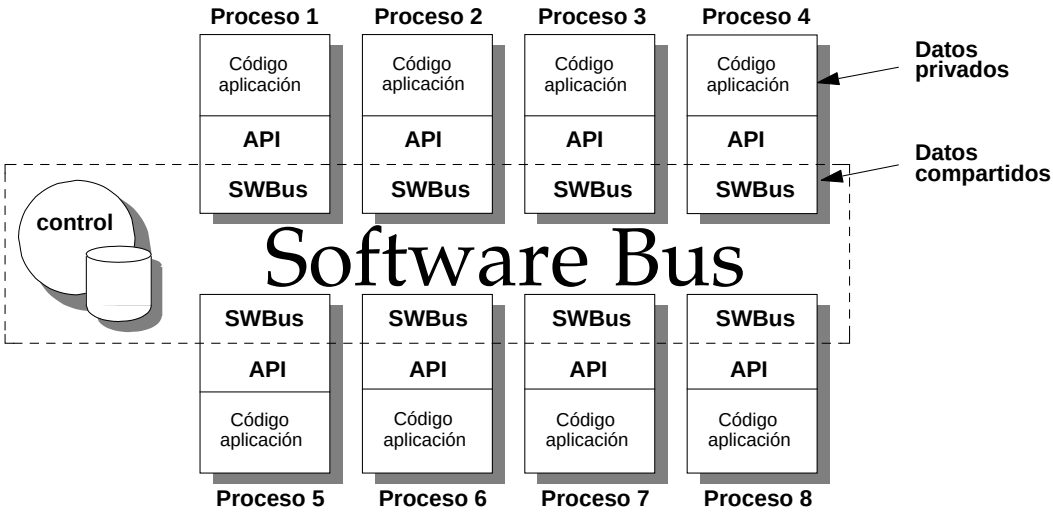


Figura 5.2: Ejemplo de estructura de implementación de SWBus.

SWBus consiste en una librería de objetos en C++ y un gestor de puertos, el cual sirve para poder comunicar los procesos que usan llamadas SWBus. La librería C de SWBus es el principal componente, permaneciendo unido a todos los procesos que usan sus servicios. La librería gestiona los objetos, la reorganización de la información que se transmite de un proceso a otro y la comunicación a muy bajo nivel entre los procesos. Además, también gestiona el flujo de programas, lo que permite a SWBus reaccionar en caso de recibir datos, y mantener un mecanismo interno de sincronización de tareas, lo que le confiere la capacidad de gestionar de forma síncrona la comunicación de procesos distribuidos. El gestor de puertos se denomina control, y puede ser ejecutado en cualquier computadora de la red. Se encarga de registrar las máquinas y los puertos mediante los nombres de los procesos suministrados por ellos mismos cuando se inicializan mediante la función SbInit, devolviendo dicha información a cualquier proceso que demande comunicarse con otro proceso registrado en SWBus. La información referente al gestor de puertos es global, por lo que un solo proceso gestiona todas las comunicaciones de la configuración. El resultado de esta integración, es una colección de procesos que comparten datos y funcionalidad.

Para escribir programas que usen la librería SWBus, se suministra un conjunto de funciones que pueden ser llamadas desde cualquier lenguaje que permita la llamada a funciones C. Estas funciones conforman una funcionalidad mínima para la implementación de interfases de comunicaciones mediante SWBus, pudiéndose ampliar si fuese necesario, HRP (2002ab).

En el caso particular de las comunicaciones TRETA / COPMA-III el uso de SWBus se puede resumir en los siguientes pasos:

- En la PDB de COPMA-III se ha integrado una interfase que emplea SWBus para escuchar y recibir información. La PDB tiene definidas en la API computerizada una serie de métodos que luego se traducen en acciones de COPMA-III, por ejemplo *ejecutar instrucción actual* (EXECUTE_CURRENT_INSTRUCTION). Asimismo, el proceso SWBus de COPMA-III tiene una lista de tipos de datos que usan los métodos mencionados.
- En TRETA se han integrado los módulos *copma3* y *copmaCrew* que también usan SWBus. Estos módulos, indicándoles en qué máquina se ejecuta la PDB del sistema COPMA-III, emplean las funciones disponibles en la API de la PDB de COPMA-III y los tipos de datos definidos para la comunicación en la ejecución de los procedimientos.

Para el inicio de las comunicaciones mediante dicha librería, se deben realizar sendas llamadas desde TRETA y la PDB de COPMA-III a la función de SWBus SbInit, con la finalidad de registrar ambos procesos en la interfase. En el caso del código TRETA, dicha llamada se realizará en la etapa 1. A partir de ese momento, TRETA puede realizar la inicialización del sistema COPMA-III y la simulación de los procedimientos.

El uso de los métodos SWBus en las comunicaciones requiere de la codificación de una interfase en C++ en ambos códigos de simulación, resultando el esquema de comunicaciones de la Figura 5.1. Los detalles de la API implementada en la PDB de COPMA-III se dan en la Sección 5.1.3.2, mientras que los referentes a la implementación de la interfase en los módulos *copma3* y *CopmaCrew* del código TRETA se dan en la Sección 5.1.3.3.

5.1.3.2 Definición de las funciones de comunicación

Dentro de las modificaciones llevadas a cabo por el grupo del HRP del sistema COPMA-III para su integración en la herramienta, se ha implementado una API de comunicaciones SWBus en la PDB, correspondiéndose con las especificaciones de funcionalidad definidas por los grupos del área MOSI del CSN y el del DSE de la UPM.

Esta API está diseñada para permitir las comunicaciones entre COPMA-III y el simulador TRETA, basándose en el conjunto de funciones ya especificado al principio de esta sección, Tabla 5.1:

1. INITIALIZE_SESSION
2. SPWRF_WRAPPER
3. OPEN_OPERATOR_SUBSCRIPTION
4. PROC_VAR_UPDATES
5. TERMINATE_SESSION

6. SWITCH_TO_ACTIVITY
7. CREATE_ACTIVITY
8. GET_INSTRUCTION_DETAILS
9. EXECUTE_CURRENT_INSTRUCTION
10. GET_EVALUATIONS_AND_VALUES
11. END_ACTIVITY

Los tipos de datos de entrada y salida de dichas funciones están basados en el uso de estructuras, definidas en el fichero **SbDataTypes.h**. La gran ventaja de este formato de datos es que permite de forma flexible y sencilla la adición de nuevos parámetros de entrada/salida, siendo necesario recompilar la aplicación solamente si se desea usar los nuevos parámetros. La asignación de las estructuras a las distintas funciones se resume en la Tabla 5.3. Las estructuras relacionados con el paso de información asociado a las variables de proceso y de procedientos, empleadas por las funciones OPEN_OPERATOR_SUBSCRIPTION, SPWRF_WRAPPER, PROC_VAR_UPDATES y GET_EVALUATIONS_AND_VALUES, contendrán la información referente a las variables simbólicas y numéricas relacionadas con componentes (*pumpcomponent* y *valvecomponent*), sistemas (*generalvariable*) y magnitudes físicas (*physmagnitude*), tal como se definieron en la Sección 4.3.2.1. La implementación física en la interfase de de estos tipos de variables se lleva a cabo en el fichero **RecordTypes.h**[1].

Toda la funcionalidad está implementada como métodos de SWBus en la PDB de COPMA-III[2], estableciéndose la implementación de funciones así como de la declaración de argumentos de entrada y salida, HRP (2002a). Todas las funciones de llamada se han definido de forma tal que, en todos los casos, el primer objeto de la salida es el código de error, Tabla 5.2. Un código de error con valor cero implica la correcta ejecución de la función llamada. Si el código de error no es cero, el resto de la información de salida no se envía. En su lugar, un mensaje informativo relativo al error encontrado puede ser informado en los campos de retorno de la función. En lo que respecta la sincronización se ha establecido un tiempo muerto, por defecto de dos segundos, que puede ser especificado en el fichero pbddata.xml. Si la sincronización no se alcanza en el tiempo especificado en timeout, se añade -10 al código de retorno de la llamada a la función. Por ejemplo, si se realiza una suscripción ilegal de una variable mediante una llamada a SPWRF_WRAPPER, el código de retorno es -6. En el caso de que se produzca de forma combinada una suscripción ilegal de una variable con superación del tiempo muerto en el intento de sincronización, el código de retorno será -16.

A continuación se describe una a una el conjunto de funciones implementadas en la API de la PDB del sistema COPMA-III.

[1] El listado de los ficheros SbDataTypes.h y RecordTypes.h se incluye en Quiroga et al. (2006)

[2] El fichero relacionado con la interfase de comunicaciones en el sistema COPMA-III se denomina pdb.dll, y se puede localizar en el directorio %CopmaRoot%/pdb donde %CopmaRoot% representa directorio donde está instalado COPMA-III.

1	INITIALIZE_SESSION
2	SPWRF_WRAPPER
3	OPEN_OPERATOR_SUBSCRIPTION
4	PROC_VAR_UPDATES
5	TERMINATE_SESSION
6	SWITCH_TO_ACTIVITY
7	CREATE_ACTIVITY
8	GET_INSTRUCTION_DETAILS
9	EXECUTE_CURRENT_INSTRUCTION
10	GET_EVALUATIONS_AND_VALUES
11	END_ACTIVITY

Tabla 5.1: Funciones que componen la API de la PDB del sistema COPMA-III.

Código de retorno (CR)	Descripción
0	OK
-1	SESSION_NOT_DEFINED
-2	PROCEDURE_DOES_NOT_EXIST
-3	ACTIVITY_NOT_DEFINE
-4	VARIABLE_NOT_DEFINED
-5	WAIT_SUSPENDED_EXECUTION
-6	ILLEGAL_VARIABLE_SUBSCRIPTION
CR - 10	SYNCHRONIZATION_TIME_OUT

Tabla 5.2: Codificación de los códigos de retorno de las funciones de la API de la PDB del sistema COPMA-III.

Función	**Estructura de entrada**	**Estructura de salida**
INITIALIZE_SESSION	struct Input1	struct Output1
SPWRF_WRAPPER	struct Input2	struct Output2
OPEN_OPERATOR_SUBSCRIPTION	struct Input3	struct Output3
PROC_VAR_UPDATES	struct Input4	struct Output4
TERMINATE_SESSION	struct Input5	struct Output5
SWITCH_TO_ACTIVITY	struct Input6	struct Output6
CREATE_ACTIVITY	struct Input7	struct Output7
GET_INSTRUCTION_DETAILS	struct Input8	struct Output8
EXECUTE_CURRENT_INSTRUCTION	struct Input9	struct Output9
GET_EVALUATIONS_AND_VALUES	struct Input10	struct Output10
END_ACTIVITY	struct Input11	struct Output11

Tabla 5.3: Estructuras de memoria empleadas por las funciones de comunicaciones.

Función INITIALIZE_SESSION

DESCRIPCIÓN:

Abre una sesión en el sistema COPMA.

ENTRADA:

1. *User*: Identificación del usuario que abre la sesión en el sistema COPMA.
2. *Path*: Ruta de la base de datos de procedimientos.
3. *Hostname*: Dirección o nombre de la computadura en la que se ejecuta el núcleo de COPMA-III.

SALIDA:

1. Código de retorno de la llamada a la función.
2. Id de la sesión iniciada.

Función SPWRF_WRAPPER

DESCRIPCIÓN:

Fija el valor de las variables del núcleo de COPMA-III. Las variables pueden ser tanto numéricas como simbólicas. Esta función se corresponde con el método nativo de actualización de variables de la PDB de COPMA-III. En la implementación actual la PDB de COPMA-III ignora el campo *value* y solo usa *strvalue*. Estos campos reflejan la estructura del tipo de variable *arrayElement* tal y como está definido en el fichero SBDataTypes.h. El campo *value* se mantiene para posibles usos futuros. No se pueden usar sinónimos, todas las variables deben tener el formato VARNAME.MEMBER de acuerdo con el fichero de configuración RecordTypes.h. Cabe resaltar que esta función es la encargada de la **sincronización** de las simulaciones del simulador de procesos y COPMA-III, obligando a que el estado de todas las actividades vigentes del núcleo de COPMA-III sea consistente con el estado del proceso, determinado por los valores numéricos y simbólicos de las variables aportadas en la llamada y, para aquellas cuyo valor no haya cambiado, las almacenadas en la PDB de COPMA-III. El tiempo límite para la sincronización se especifica en el fichero pdbdata.xml[3].

ENTRADA:

Una lista de tripletes <*variable*, *value*, *strvalue*>.

- *Variable*: nombre de la variable a ser actualizada.
- *Value*: valor a fijar (numérico).
- *Strvalue*: valor a fijar (cadena).

SALIDA:

1. Código de retorno de la llamada a la función.

[3]El listado del fichero pdbdata.xml se incluye en Quiroga et al. (2006).

Función OPEN_OPERATOR_SUBSCRIPTION

DESCRIPCIÓN:

Esta función suscribe las variables de COPMA-III a ser usadas por el código TRETA. Sólo las variables suscritas serán inspeccionadas al realizar la llamada a la función PROC_VAR_UPDATES.

Todas las suscripciones de elementos *valvecomponent* y *pumpcomponent*, definidos en el fichero RecordTypes.h debe tener formato tipo C/C++ de la forma VARNAME. MEMBER. Esto es, no se pueden usar sinónimos y todas las variables deben tener el formato tal y como se defina en el fichero de configuración RecordTypes.h.

No es posible suscribir elementos *physmagnitude*. Es posible suscribir variables simples definidas en el fichero RecordTypes.h y declaradas en el fichero .pdat que se esté usando (es decir, no tendrán implementación de sinónimo ni estructura, y solo tendrán VARNAME).

La regla general es que solo las variables que vayan a ser manipuladas por el núcleo de COPMA-III pueden ser suscritas por OPEN_OPERATOR_SUBSCRIPTION, en caso contrario se retornará un código de retorno con error -6 (ILLEGAL_VARIABLE_ SUBSCRIPTION). Todas las variables correctas se suscribirán, ignorándose las erróneas. Así, para los elementos *valvecomponent* y *pumpcomponent* solo se pueden suscribir los campos *command* y *autoSwitch* (ver RecordTypes.h). Por ejemplo, para una bomba denominada RL33S001 solo se pueden suscribir *RL33S001.command* y *RL33S001.autoSwitch*. Los valores de las variables suscritas dentro de una sesión de comunicaciones solo se retornan si han cambiado desde la última llamada a PROC_VAR_UPDATES o GET_EVALUATIONS_AND_VALUES. En la suscripción solo se considera el campo *name* (ver SbDatatypes.h).

ENTRADA:

1. *Session*: Id de identificación de la sesión abierta, tal y como es devuelto tras la llamada a INITIALIZE_SESSION.
2. <*variable*>: vector de nombres de variables a ser suscritas.

SALIDA:

1. Código de retorno de la llamada a la función.

Función PROC_VAR_UPDATES

DESCRIPCIÓN:

Esta función devuelve los valores de las variables previamente suscritas con OPEN_OPERATOR_SUBSCRIPTION. Las variables son devueltas con el mismos nombre usado en OPEN_OPERATOR_SUBSCRIPTION y la PDB de COPMA-III solo usa el campo *strval* de la estructura *arrayElement,* tal como se define en el fichero SbDatatypes.h.

ENTRADA:

1. *Session*: Id de identificación de la sesión abierta, tal y como es devuelto tras la llamada a INITIALIZE_SESSION.

SALIDA:

1. Código de retorno de la llamada a la función.
2. *NumOutputs*: un entero con el número de pares <*variable, value*>devueltos.
3. Vector <*variable, value*>: siendo *variable* el nombre de la variable cuyo valor es actualizado, y *value* el valor con que se actualiza la variable.

Función TERMINATE_SESSION

DESCRIPCIÓN:

Esta función cierra una sesión abierta por INITIALIZE_SESSION.

ENTRADA:

1. *Session*: Id de identificación de la sesión abierta, tal y como es devuelto tras la llamada a INITIALIZE_SESSION.

SALIDA:

1. Código de retorno de la llamada a la función.

Función SWITCH_TO_ACTIVITY

DESCRIPCIÓN:

Esta función cambia de la actividad actual a otra que se encuentre corriendo en la sesión actual.

ENTRADA:

1. *Session*: Id de identificación de la sesión abierta, tal y como es devuelto tras la llamada a INITIALIZE_SESSION.
2. *Activity*: Id de la actividad a la cual se desea cambiar, tal y como es devuelta por la llamada a CREATE_ACTIVITY.

SALIDA:

1. Código de retorno de la llamada a la función.

Función FUNCIÓN CREATE_ACTIVITY

DESCRIPCIÓN:

Esta función crea una actividad en la sesión actual para ejecutar el procedimiento especificado.

ENTRADA:

1. *Session*: Id de identificación de la sesión abierta, tal y como es devuelto tras la llamada a INITIALIZE_SESSION.
2. *Procedure*: Id del procedimiento a ejecutar.

SALIDA:

1. Código de retorno de la llamada a la función.
2. *Activity*: Id de la actividad creada.
3. *Procedure*: Id del procedimiento.
4. *Step*: Id del primer paso asociado al procedimiento.
5. *Time*: tiempo en el cual se inicia la actividad.

Función GET_INSTRUCTION_DETAILS

DESCRIPCIÓN:

Esta función se emplea para obtener los detalles asociados a la instrucción actual de una actividad. La primera instrucción siempre debe tener Id igual a 1, siendo este detalle de gran utilidad para iniciar la ejecución automática de los procedimientos y comprobar sus detalles.

ENTRADA:

1. *Session*: Id de identificación de la sesión abierta, tal y como es devuelto tras la llamada a INITIALIZE_SESSION.
2. *Procedure*: Id del procedimiento actual.
3. *Step*: Id del paso actual del procedimiento tal y como es devuelto por la llamada a EXECUTE_CURRENT_INSTRUCTION o CREATE_ACTIVITY.
4. *Instruction*: Id de la instrucción actual tal y como es devuelta por la llamada a EXECUTE_CURRENT_INSTRUCTION.

SALIDA:

1. Código de retorno de la llamada a la función.
2. *Type*: Tipo de instrucción de acuerdo a la Tabla 5.4.
3. *Step*: Id del paso actual del procedimiento.
4. *Instruction*: Id de la instrucción actual del prodecimiento.
5. *Texec*: tiempo de ejecución en segundos de la instrucción actual.
6. *Taskload*: porcentaje de la carga máxima (100 %) a ser asumido por el equipo de operación de la sala de control al ejecutar la instrucción actual.

Código	Instrucción
1	Action
2	Autocheck
3	Finish
4	Gosub
5	Goto
6	Initiate
7	Mancheck
8	Manual-action
9	Message
10	Monitor
11	Return
12	Wait

Tabla 5.4: Tipos de instrucciones consideradas en la función GET_INSTRUCTION_ DETAILS.

Función EXECUTE_CURRENT_INSTRUCTION

DESCRIPCIÓN:

Esta función se usa para ejecutar la instrucción actual y obtener la Id de la siguiente. La primera instrucción debe tener siempre una Id igual a 1, este detalle es muy útil para poder realizar la ejecución automática de los procedimientos.

ENTRADA:

1. *Session*: Id de identificación de la sesión abierta, tal y como es devuelto tras la llamada a INITIALIZE_SESSION.
2. *Activity*: Id de la actividad a la cual se desea cambiar, tal y como es devuelta por la llamada a CREATE_ACTIVITY.
3. *Procedure*: Id del procedimiento actual.
4. *Step*: Id del paso actual del procedimiento tal y como es devuelto por la llamada a EXECUTE_CURRENT_INSTRUCTION o CREATE_ACTIVITY.
5. *Instruction*: Id de la instrucción actual tal y como es devuelta por la llamada a EXECUTE_CURRENT_INSTRUCTION.

SALIDA:

Devuelve, además del código de retorno de la llamada, la descripción de la siguiente instrucción con el mismo formato que GET_INSTRUCTION_DETAILS.

1. Código de retorno de la llamada a la función.
2. *NextType*: Tipo de instrucción de acuerdo a la Tabla 5.4.
3. *NextStep*: Id del paso actual del procedimiento.
4. *NextInstruction*: Id de la instrucción actual del prodecimiento.
5. *NextTexec*: tiempo de ejecución en segundos de la instrucción actual.
6. *NextTaskload*: porcentaje de la carga máxima (100 %) a ser asumido por el equipo de operación de la sala de control al ejecutar la instrucción actual.
7. *NewActivityID*: Id de la nueva actividad.
8. *NewProcedureID*: Id del nuevo procedimiento.
9. *NewProcThenID*: Id del procedimiento en la rama del THEN.
10. *NewProcElseID*: Id del procedimiento en la rama del ELSE.

Función GET_EVALUATIONS_AND_VALUES

DESCRIPCIÓN:

Esta función se debe usar para comprobar el estado de la vigilancia de variables de proceso, *MONITOR,* y actualizarlo de acuerdo con las condiciones que vigilan. También da información acerca de las actividades que se encuentren en espera, realizando un chequeo de las condiciones de espera. Finalmente, esta función devuelve los valores actualizados de las variables suscritas previamente con la llamada a OPEN_OPERATOR_ SUBSCRIPTION. Como esta función incluye la funcionalidad de PROC_VAR_UPDATES, puede emplearse de forma que esta función no necesite ser implementada.

ENTRADA:

1. *Session*: Id de identificación de la sesión abierta, tal y como es devuelto tras la llamada a INITIALIZE_SESSION.

SALIDA:

Las salidas, a parte del código de retorno, son cuatro grupos de datos: las variables suscritas actualizadas, el número de condiciones de vigilancia y su estado, el número de condiciones de espera asociadas a actividades y un listado completo de las actividades que en ese momento se encuentren activas en el núcleo de COPMA-III.

1. Código de retorno de la llamada a la función.
2. Primer grupo: lista de variables suscritas y sus valores, de la misma forma que se devuelve en la función PROC_VAR_UPDATES (*NumOutputs*, vector <*variable, value*>).
3. Segundo grupo: el estado de las condiciones de vigilancia o *MONITOR*.
   - *NumMonitors*: número de *MONITOR* vigentes.
   - Vector <*monitorId, monitorStat*>: con *MonitorId* como la Id del *MONITOR* y *MonitorStat* como el estado del mismo, con la codificación 1 si el *MONITOR* está activo, 2 si el *MONITOR* concluyó con la condición *then* y 3 si el *MONITOR* concluyó con la condición *else*.
4. Tercer grupo: el estado de las condiciones de parada de actividades o *WAIT*.
   - *NumWaits*: número de actividades en estado de espera.
   - Vector <*ActivityId, StepId, InstructionId, WaitStat*>con *ActivityId* como la actividad en espera, *StepId* el paso actual de la actividad que se encuentra en espera, *InstructionId* la instrucción actual del paso especificado en *StepId* y *WaitStat* con el estado de la condición del *WAIT* codificado con un 0 si la condición no se ha cumplido y con 1 si la condición se ha cumplido.

5. Cuarto grupo: listado de las actividades relativas a procedimientos activas en el núcleo.
    - *NumActivities*: número de actividades relativas a procedimientos activas en el núcleo.
    - Vector <*Activity*, *Procedure*, *Step*, *Instruction*>con *ActivityId* como la Id de la actividad, *Procedure* como la Id del procedimiento asociado a la actividad, *StepId* el paso actual de la actividad que se encuentra en espera, *InstructionId* la instrucción actual del paso especificado en *StepId*.

Función END_ACTIVITY

DESCRIPCIÓN:

Esta función finaliza una actividad iniciada por CREATE_ACTIVITY.

ENTRADA:

1. *Session*: Id de identificación de la sesión abierta, tal y como es devuelto tras la llamada a INITIALIZE_SESSION.
2. *Activity*: Id de identificación de la actividad, tal y como es devuelto en la llamada a CREATE_ACTIVITY.

SALIDA:

1. Código de retorno de la llamada a la función.

5.1.3.3 Implementación de la interfase de comunicaciones en TRETA

La funcionalidad de comunicaciones está implementada en los módulos *copma3* y *copmacrew* del código TRETA. El reparto de funciones de ambos módulos es el siguiente:

- Las funciones principales del módulo *copma3* son:
  - La puesta a punto de las comunicaciones entre TRETA y la PDB de COPMA-III mediante la llamada a la función INITIALIZE_SESSION.
  - La inicialización de las variables de TRETA que son de interés para COPMA-III y su actualización subsiguiente calculando los estados de los componentes (válvulas, bombas,...) enviados a COPMA-III mediante la función SPWRF_WRAPPER, forzando la sincronización del estado de los elementos que componen el sistema COPMA-III con el valor de las variables de proceso aportadas por TRETA para el paso de tiempo actual.
  - La subscripción de las variables de COPMA-III que son de interés para TRETA, mediante la función OPEN_OPERATOR_SUBSCRIPTION.
  - La finalización de la simulación de los procedimientos, mediante la función TERMINATE_SESSION
- Por otro lado, el módulo *CopmaCrew* es el responsable de realizar la simulación de los procedimientos. Para ello realiza las siguientes funciones:
  - El seguimiento del estado de las actividades asignadas a la ejecución de los procedimientos, mediante la función GET_EVALUATIONS_AND_VALUES.
  - La gestión de las actividades sobre los procedimientos, mediante las funciones CREATE_ACTIVITY, SWITCH_TO_ACTIVITY y END_ACTIVITY.
  - Gestionar la ejecución de los procedimientos, atendiendo al estado de las actividades, mediante el uso de las funciones GET_INSTRUCTION_DETAILS y EXECUTE_CURRENT_INSTRUCTION.

  Con este conjunto de funciones, el módulo simula las acciones manuales del operador interaccionando con el sistema COPMA-III. De hecho, las instrucciones intercambiadas entre la PDB de COPMA-III y *CopmaCrew* son similares a los mensajes correspondientes entre el núcleo de COPMA-III y la MMI de COPMA-III.

  Además, este módulo es el responsable de decidir el momento temporal en que se llama a estas funciones (cuando se ejecuta una instrucción, cuando se pasa a otro procedimiento, etc.). Para decidirlo *CopmaCrew* usa un modelo basado en dos factores limitantes:
  - El tiempo necesario para ejecutar una instrucción, denominado TEXEC.
  - Los recursos necesarios para ejecutar un instrucción, denominado TASKLOAD.

Si hay que ejecutar una instrucción y no hay recursos suficientes, la ejecución será pospuesta temporalmente hasta que los recursos necesarios sean liberados, que sucederá cuando otras instrucciones en ejecución terminen. Cada instrucción especificada en el modelo de procedimientos computerizados presentará dos atributos denominados TEXEC y TASKLOAD para especificar estas restricciones. Cabe destacar, que la implementación completa de estas funciones no es objetivo de este trabajo, aunque se han tratado en el desarrollo de los modelos computerizados de los procedimientos y en las aplicaciones de prueba del simulador integral, Capítulos 4 y 6, respectivamente.

En resumen, las funciones que realiza el módulo son:

- Asignar a cada instrucción de los procedimientos de operación un tiempo de ejecución.
- Tener en cuenta la carga de trabajo del turno de operación para evitar un número excesivo de instrucciones simultáneas.
- Efectuar una búsqueda en los procedimientos abiertos y realizar una nueva instrucción cuando el tiempo de ejecución y la carga de trabajo lo permita.

Ambos módulos hacen uso extensivo de las funciones implementadas en la API de la PDB del COPMA-III a través de la interfase de comunicaciones, denominada TCComm, implementada en los ficheros **CopmaTretaComm.h** y **CopmaTretaComm.cpp**[4]. En estos ficheros se declaran las funciones y variables globales de TCComm, y las definiciones de las funciones de incluidas en TCComm, respectivamente. Las funciones de TCComm tienen el mismo nombre que la funciones incorporadas en la API de la PDB descrita en la Sección 5.1.3.2, correspondiéndose la llamada a las funciones siempre con la misma estructura,

```
function\_name(const SbTSTI theServer, const input\#\& In\#,
output\#\& Out\#)
```

donde # comprende las funciones 1 hasta 11, Tabla 5.1, *theServer* es una variable *SbTSTI* de SWBus que especifica la conexión COPMA-III (en la implementación actual se hace mediante la variable global *CopTreComm_Server* y la función *IniCopmaTretaComm*). La correspondencia entre variables de entrada y de salida y las funciones de TCComm esta especificada en el fichero TCCComm.h y esta hecha de acuerdo con la asignación ya realizada, Tabla 5.3.

La invocación de cualquier función de la API de la PDB empleando los métodos de la librería SWBus es similar, por lo que a continuación solo se incluye como ejemplo la función INITIALIZE_SESSION, de forma que ilustra como se realizaría para cualquier otra de las funciones implementadas.

Todas las funciones de la librería tienen tres parámetros de entrada:

- el identificador del servidor donde esta corriendo COPMA III, *SbTSTI theServer*,

[4]Los listados de los ficheros CopmaTretaComm.h y CopmaTretaComm.cpp se incluyen en Quiroga et al. (2006).

- la estructura de datos de entrada
- y la estructura de datos de salida[5].

De esta forma, la definición de las funciones queda como,

```
char* INITIALIZE_SESSION(const SbTSTI theServer,
    const struct input1 In1, struct output1 *Out1)
```

El primer paso es obtener de SWBus el *Symbol table index* (SbSTI) del objeto INITIALIZE_SESSION (en SWBus todo objeto tiene un identificador único que se usa para acceder a los datos del objeto e invocar sus métodos),

```
{
 SbTSTI stiINITIALIZE_SESSION = SbId( theServer, "INITIALIZE_SESSION" );
```

A continuación, se crea una estructura SWBus que sea fiel reflejo de la estructura in1 definida en SbDataTypes.h, en este caso la estructura se llama INPUT1 y tiene como SbTSTI a stiINPUT1,

```
SbTSTI stiINPUT1 = SbSub( SbCCEmpty, "INPUT1", SbCNull );
```

Una vez creada la estructura, se añaden los correspondientes atributos a la estructura SWBus, reproduciendo el tipo y el nombre de la estructura INPUT1. Es muy importante que el orden y el tipo de los atributos añadidos coincidan con el listado de SbDataTypes.h,

```
SbAdd( stiINPUT1, SbCCString, "User", NULL );
SbAdd( stiINPUT1, SbCCString, "Path", NULL );
SbAdd( stiINPUT1, SbCCString, "Hostname", NULL );
```

Finalmente, se crea localmente un objeto SWBus con SbTSTI inParam1 que va a ser el encargado de transmitir los datos encapsulados en la estructura INPUT1 al proceso remoto. La ligadura entre el objeto SWBus inParam1 y la estructura INPUT1 es la estructura SWBus stiINPUT1,

```
SbTSTI inParam1  =  SbCreate( SbCPLocal, stiINPUT1,   0, SbCNull, 0 )
```

El proceso se repite para la estructura OUTPUT1, que va a ser la encargada de recibir los datos devueltos tras la llamada a la función remota INITIALIZE_SESSION,

[5]La definición de las estructuras de datos, como ya se ha comentado previamente, se realiza en el fichero denominado **SbDataTypes.h**, del cual se incluye la versión actual en Quiroga et al. (2006).

```
SbTSTI stiOUTPUT1 = SbSub( SbCCEmpty, "OUTPUT1", SbCNull );
SbAdd( stiOUTPUT1, SbCCInteger, "ErrorCode", NULL );
SbAdd( stiOUTPUT1, SbCCString, "Id", NULL );
```

Igual que antes, se crea localmente un objeto SWBus con SbTSTI outParam1 que va a ser el encargado de recibir la respuesta de INITIALIZE_SESSION y encapsular estos datos en la estructura OUTPUT1. La ligadura entre el objeto SWBus outParam1 y la estructura OUTPUT1 es la estructura SWBus stiOUTPUT1,

```
SbTSTI outParam1 =  SbCreate( SbCPLocal, stiOUTPUT1,   0, SbCNull, 0 );
```

Una vez creados los objetos SWBus que van a emplear para mandar y recibir los datos de entrada y salida de INITIALIZE_SESSION, el siguiente paso es asignar al objeto SWBus inParam1 los datos que viene en la estructura INPUT1 In1. Para ello, primero se obtiene un puntero INPUT1* que apunta a los datos del objeto SWBus inParam1,

```
input1* SBDataIn1   = (input1 *)SbData( inParam1 );
```

y, a continuación, se copian uno a uno los campos de la estructura INPUT1 In1,

```
SBDataIn1->User=strdup(In1.User);         // por ejemplo "AEL" ;
SBDataIn1->Path=strdup(In1.Path);         // por ejemplo "C:\copma1_0"
SBDataIn1->HostName=strdup(In1.HostName); // por ejemplo "inuc.dse.upm.es"
```

Una vez creados los identificadores SWBus de los objeto que representan:

- el método que queremos invocar, en este caso stiINITIALIZE_SESSION,
- los datos de entrada inParam1,
- y los datos de salida outParam1,

se invoca el método remoto mediante una llamada a SbCall,

```
SbCall( stiINITIALIZE_SESSION, inParam1, outParam1 );
```

Una vez llamada la función, se recuperan los los datos aportados por la función y se copian en la estructura OUTPUT1 Out1,

```
output1* SBDataOut1 = (output1 *)SbData( outParam1 );
Out1->Session=strdup(SBDataOut1->Session);
Out1->ErrorCode=SBDataOut1->ErrorCode;
```

se prepara el registro de la llamada para la salida de control,

```
char sLog[MAX_LOG_LENGTH];
sprintf(sLog, "<<INITIALIZE_SESSION>>-> Session Id: %s,
    error code: %d\n", Out1->Session, Out1->ErrorCode);
```

y se eliminan los objetos SWBus creados,

```
SbDelete(inParam1, SbCNull);
SbDelete(outParam1, SbCNull);

require(SbDelete(stiINPUT1, SbCNull)==SbCOK,
    "Error en INITIALIZE_SESSION(): SbDelete(stiINPUT1, SbCNull)");
require(SbDelete(stiOUTPUT1, SbCNull)==SbCOK,
    "Error en INITIALIZE_SESSION(): SbDelete(stiOUTPUT1, SbCNull)");;

return strdup(sLog);
}
```

5.1.3.4 Ficheros de configuración de la interfase de los códigos TRETA y COPMA-III

Dado que el simulador TRETA y el sistema computerizado de procedimientos COPMA-III son programas muy diferentes, la representación interna de las variables usadas por cada uno es incompatible, por lo tanto siempre es necesario un mecanismo de traducción para integrar ambos entornos de simulación. Las variables de TRETA, valores numéricos que representan las diferentes magnitudes físicas simuladas, y las variables simbólicas de COPMA-III, cadenas de caracteres conteniendo nombres simbólicos, es realizada por *copma3* a través del fichero de entrada correspondiente al código TRETA, donde se indica la correspondencia entre variables numéricas y simbólicas. La relación de las variables de simulación de los procedimientos para el simulador COPMA-III se establece en el fichero **varinit.pdat**. Ambos ficheros de configuración se comentan en detalle en los apartados siguientes.

Fichero de configuración de la interfase del código TRETA

En el fichero de entrada de TRETA, Figura 5.3, se definen los bloques 10 y 1000 que actúan como interfase con COPMA-III mediante los módulos *copmacrew* y *copma3*, respectivamente. Aclarar que en el ejemplo mostrado se ha eliminado la parte del mismo que no está relacionada con las comunicaciones, relacionado con el modelo de sistema. El bloque correspondiente al módulo *copmacrew* solo incluye el nombre del equipo en el que se ejecuta el núcleo de COPMA-III y el nombre del procedimiento de arranque. El bloque 1000 es bastante más complejo y es el que configura la interfase de comunicaciones TRETA/COPMA. Los datos que el módulo lee del fichero de entrada a TRETA son los siguientes:

1. Opciones y entorno.
    - Línea 1:
        - Sincronización. Número entero. Si es 0 la simulación se realiza en tiempo real.
        - Nombre de la máquina donde está corriendo el núcleo de COPMA-III.

Tipo	Definición	Estados	Parámetros de la función
1	Variables de proceso. (Caudal, nivel, presión, etc.)	INCREASING DECREASING STEADY	1: Incremento característico en 1 s. (es decir, valor umbral de la derivada).
2	Dispositivos con posicionador. (Válvulas, interruptores, etc.)	OPEN OPENING CLOSED CLOSING INTERM	1: Umbral de dispositivo cerrado. 2: Umbral de dispositivo abierto. 3: Incremento característico en 1 s.
3	Componentes activos. (Bombas, compresores, DG, sistemas completos, etc.)	RUNNING STOPPED BLOCKED FAILED	1: Valor indicativo del estado BLOCKED. 2: Valor indicativo del estado FAILED. 3: Valor umbral de RUNNING/STOPPED.
4	Señales de iniciación; alimentación eléctrica, etc.	ON OFF READY BLOCKED	1: Valor indicativo del estado READY. 2: Valor indicativo del estado BLOCKED. 3: Valor umbral de ON/OFF.
5	Variables genéricas; modos de operación de sistemas, componentes, etc.	MODE1 MODE2	1: Valor indicativo del modo de operación 1. 2: Valor indicativo del modo de operación 2.

Tabla 5.5: Tipos de funciones aplicables en la configuración de interfase de TRETA.

2. Tratamiento de las entradas.

   Por cada entrada al módulo habrá una línea de datos conteniendo la siguiente información:

   - Linea i+1 (siendo i el número de la entrada):
     - Nombre de la variable en COPMA-III.
     - Tipo de función de estado, Tabla 5.5. Si no se aplica ninguna, poner cero o dejar vacío.

     En caso de que se aplique función de estado, se añadirá además:

     - Nombre en COPMA-III para la variable de estado asociada a la variable de proceso.
     - Parámetros específicos de la función de estado, Tabla 5.5.

3. Salidas:

   - Linea n+2 (siendo n el número de entradas): nombres de las variables de salida del módulo en COPMA-III.

Los tipos de funciones que se pueden implementar en el módulo *copma3* se corresponde con los tipos de variables definidos para la comunicación mediante la interfase, realizando la traducción de los valores numéricos de las variables de proceso de TRETA a los valores simbólicos correspondientes al simulador COPMA-III, Tabla 5.5.

```
*-----------------------------------------------------
*   CONNECTION MODULE COPMACREW
*-----------------------------------------------------
 Copmacrew interface
 10
 0
 1007
* --
 vmware-winxp  CIII-TRE-MAINIUID
*-----------------------------------------------------

.... .... .... .... .... .... ....

*-----------------------------------------------------
*   CONNECTION MODULE COPMA-III
*-----------------------------------------------------
 COPMA3-CONNECTION
 1000  0  2
 1000 1001 190 100
 57   0    0.    0.
*----
 0 vmware-winxp
*     ^--------------------------------- host
 VALENT.position 2  VALENT.opStatus 0.01  0.99  1.0
 VALSAL.position 2  VALSAL.opStatus 0.01  0.99  1.0
 MASA.value     0
 SIMTIME.value  0
*
 VALENT.command  VALSAL.command
*1000             1001
* ^-----------------^------- Output variables
*-----------------------------------------------------
```

Figura 5.3: Fichero de configuración de los módulos *copma3* y *copmacrew* de TRETA.

Fichero de configuración de la interfase del código COPMA-III

En el sistema COPMA-III, el mecanismo de intercambio de variables está basado en dos ficheros de configuración, Recordtypes.h y varinit.pdat, que son especificados en el fichero **pbdata.xml**[6]:

- **Recordtypes.h**. Este fichero se interpreta en tiempo de ejecución por parte del COPMA-III PDB empleando la función SBReadScript(), por lo tanto no se puede modificar con directivas del prepropresador de C/C++ como, por ejemplo, directivas #include. Este fichero es único y establece los tipos de variables a intercambiar entre COPMA-III y TRETA como estructuras tipo C/C++, tal como se definieron en la Sección 4.3.2.1, a saber: *valvecomponent*, *pumpcomponent*, *physmagnitude* y *generalvariables*.

- **Ficheros .pdat**. En estos ficheros de declaración de variables de COPMA-III se deben declarar todas las variables que vayan a ser usadas en el procedimiento, no siendo necesario inicializarlas ya que el módulo *copma3* de TRETA se encarga de ello en tiempo de ejecución al inicio de la simulación. La estructura de las variables debe concordar con las definiciones contenidas en RecordTypes.h. El nombre por defecto es varinit.pdat y su localización se especifica en el fichero pbddata.xml. Cada procedimiento tendrá su propio fichero .pdat. También se pueden usar varios ficheros pdat en la evaluación de un procedimiento.

  En el ejemplo de la Figura 5.4, las válvulas VALENT y VALSAL se implementan como una variable de tipo *valvecomponent* y, posteriormente, VALENT.*command* y VALENT.*command* se inicializan a CLOSE. Asimismo, se inicializan los valores de las propiedades *openval* y *closeval* para estas válvulas. Si no se inicializan, como es el caso de este ejemplo, se usará el valor por defecto especificado en Recordtypes.h. El nivel de masa denotado por MASA se implementa como una variable tipo *physmagnitude*, el nivel inicial representado por MASA.*value* se inicializa a 50 y para finalizar la variable SIMTIME se deja sin inicializar. Para finalizar se define una variable general denominada SYSTEM. Este tipo de variables se deben emplear para definer estados binarios de un conjunto de componentes o de un sistema.

Aspectos a tener en cuenta en la configuración de estos dos ficheros son:

- Los nombres de las variables son sensibles a la capitalización, es decir, desde el código TRETA no es lo mismo mandar un valor para *VALENT.value* que para *VALENT.Value*, solo es correcto la primera forma de acuerdo con las especificaciones de SbDataTypes.h y varinit.pdat.

- No se pueden usar sinónimos en los procedimientos, solamente se puede usar el nombre completo *VARNAME.PROPIEDAD*, esto es especialmente importante en las operaciones de tipo ACTION, por ejemplo, si se han definido dos variables tipo *valvecomponent*

[6]Los listados de los ficheros pbdata.xml, Recordtypes.h y varinit.pdat se incluyen en Quiroga et al. (2006).

y *pumpcomponent* y las hemos denominado como PUMP y VALVE. En este caso, las acciones CLOSE y STOP se deben escribir en el procedimiento como: CLOSE *VALVE.command* y STOP *PUMP.command*.

```
valvecomponent VALENT; valvecomponent VALSAL;

VALENT.command = "CLOSE"; VALENT.opStatus = "CLOSED";

VALSAL.command = "CLOSE"; VALSAL.opStatus = "CLOSED";

VALENT.openval = "0.99"; VALENT.closeval = "0.01";

VALSAL.openval = "0.99"; VALSAL.closeval = "0.01";

physmagnitude  MASA; physmagnitude  SIMTIME; MASA.value = "50";
```

Figura 5.4: Ejemplo de fichero de configuración de variables de COPMA-III.

5.2 Pruebas realizadas para la verificación de la funcionalidad de las comunicaciones

Los objetivos de las pruebas realizadas para la verificación de la implementación del simulador integral han consistido en:

1. **La comprobación de las comunicaciones**.

   Esta validación es estándar en todas las pruebas. Como ya se ha comentado en este capítulo, en cada ciclo de computación del simulador de planta que implique el seguimiento y la ejecución de un procedimiento, se emplea todo el conjunto de llamadas implementadas, Tabla 5.1:

   - Por un lado las funciones generales de establecimiento y finalización de las comunicaciones: INITIALIZE_SESSION y TERMINATE_SESSION.
   - La funciones relacionadas con escritura y lectura de variables: SPWRF_WRAPPER, OPEN_OPERATOR_SUBSCRIPTION y PROC_VAR_UPDATES.
   - La funciones empleadas para la ejecución y el seguimiento de las actividades sobre los procedimientos de operación: SWITCH_TO_ACTIVITY, CREATE_ACTIVITY, GET_INSTRUCTION_DETAILS, EXECUTE_CURRENT_INSTRUCTION y GET _EVALUATIONS_AND_VALUES.

   Para verificar la funcionalidad de comunicaciones de las llamadas a GET_INSTRUCTION _DETAILS y EXECUTE_CURRENT_INSTRUCTION, al igual que para la comprobación completa de la funcionalidad de la función GET_EVALUATIONS_AND_VALUES,

se hace necesaria la ejecución de procedimientos que incluyan las diferentes instrucciones implementadas en los procedimientos, es decir: INITIATE, FINISH, MESSAGE, GOTO, AUTOCHECK, ACTION, WAIT y MONITOR.

2. **La comprobación de la funcionalidad del modelado de procedimientos**.

   Para ello se han implementado y realizado un conjunto amplio de pruebas que en su conjunto abarcan toda la funcionalidad diseñada para el seguimiento y la ejecución de los procedimientos de operación, tanto para el código TRETA como para el código COPMA-III. En este apartado se incluyen cuatro ejemplos representativos:

   - Caso de **prueba instrucción WAIT**.

     Incluye la funcionalidad de las instrucciones INITIATE, FINISH, WAIT y ACTION. Permite además, verificar la gestión adecuada de actividades en espera por parte de COPMA-III y TRETA, además de su seguimiento mediante la llamada a la función GET_EVALUATIONS_AND_VALUES.

   - Caso de **prueba instrucción MONITOR**.

     Incluye la funcionalidad de las instrucciones INITIATE, FINISH, MONITOR y ACTION. Permite además, verificar la gestión adecuada de las instrucciones de vigilancia por parte de COPMA-III y TRETA, además de su seguimiento mediante la llamada a la función GET_EVALUATIONS_AND_VALUES.

   - Caso de **prueba del tipo de variable *generalvariable***.

     Incluye la funcionalidad de las instrucciones INITIATE, FINISH y WAIT, permitiendo verificar la implementación específica del tipo de variable *generalvariable*, variables generales.

   - Caso de **prueba instrucción AUTOCHECK**.

     Incluye la funcionalidad de las instrucciones INITIATE, FINISH, AUTOCHECK y ACTION.

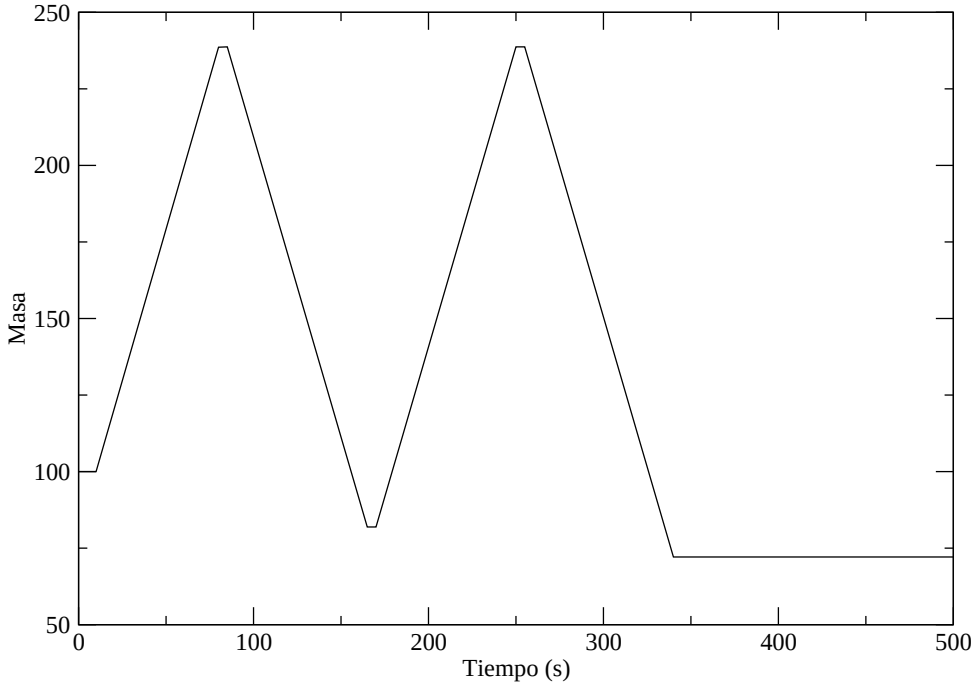
Las especificaciones de las pruebas se ha intentado mantener en común, de forma que su verificación fuese directa. De esta forma, cualquiera que sea el caso de prueba, se corresponde con un modelo puramente matemático de un sistema sencillo, compuesto por un depósito que dispone de una línea de llenado y otra de vaciado, ambas controladas por dos válvulas. El proceso consistente en el llenado y el vaciado de un depósito por un fluido, sin sobrepasar un máximo de 200 unidades de masa y un mínimo de 100 unidades de masa. El estado inicial se corresponde con las dos válvulas cerradas y el depósito con un inventario inicial de 100 unidades de masa.

La prueba genérica considerada consiste en, partiendo del depósito con 100 unidades de masa, realizar su llenado hasta 200 unidades y su posterior vaciado hasta 100 unidades, volviendo a cerrar la válvula de salida y quedando el sistema en un estado final idéntico al inicial. Para algunas pruebas, por requerimientos de las mismas, ha sido necesario simular dos ciclos de llenado. En estos casos se comentará explícitamente el motivo de esta necesidad.

5.2.1 Resultados del caso de prueba de la instrucción WAIT

En esta prueba se han modelado dos ciclos de llenado, ya que una de los objetivos es verificar la gestión correcta de condiciones de espera asociadas a distintas actividades y el inicio, la gestión y la finalización de varias actividades sobre diferentes procedimientos ejecutados en paralelo. El resultado obtenido en la ejecución de la prueba se muestra en la Gráfica 5.1, los ficheros de configuración del código TRETA y COPMA-III, así como contenido de los procedimientos empleados en la simulación: CIII-TRE-MAINI, CIIITRT-SM-TETL y CIIITRT-SM-TETL2, de los cuales se incluye la versión Prola pues es la más legible a la hora de hacer su seguimiento.

Como se puede comprobar, el código COPMA-III simula adecuadamente los dos ciclos de llenado del depósito. La diferencia de los valores límite obtenidos en la simulación frente a las condiciones de control implementadas en los procedimientos se corresponden con los valores considerados de TEXEC y TASKLOAD para las actuaciones de apertura y cierre de las válvulas. Podemos considerar como ejemplo el segundo pico de la Gráfica 5.1. La condición de llenado se cumple a las 200 unidades de masa, mientras que el depósito se llena hasta alcanzar las 238 unidades. De estas 38 unidades en exceso, 30 se corresponden a los 30 segundos de TEXEC considerado para la actuación del cierre de la válvula y las otras 8 unidades se corresponden con deficiencias en la sincronicazión de los códigos. Sin embargo, el resultado obtenido en lo que respecta a la funcionalidad es satisfactorio.



Gráfica 5.1: Resultado de la prueba de comunicaciones de la instrucción WAIT: masa de líquido en el depósito.

FICHERO DE ENTRADA DEL CÓDIGO TRETA

```
************************************************************
*
* TRETA-COPMA-III CONNECTION TEST 1
*
************************************************************
************************************************************
*
TRETA-COPMA-III CONNECTION
500 5
*
1
*----------------------
*
*-------------------------------------------------------------------------
*
*   CONNECTION MODULE COPMACREW
*
*-------------------------------------------------------------------------
 Copmacrew interface
 10
 0
 1007
* --
 vmware-winxp  CIII-TRE-MAINIUID
*-------------------------------------------------------------------------
 Simulation time
 100
 0
 27
* --
 [T]
*-------------------------------------------------------------------------
 Masa entra
 120  0  2
 1000
 27
* --
 10*[1]
*-------------------------------------------------------------------------
 Masa sale
 140 0  2
 1001
 27
* --
 10*[1]
*-------------------------------------------------------------------------
 Masa
 190 0  2
 120 140 200
 27
* --
 [1]-[2]+[3]
*-------------------------------------------------------------------------
 Masa plus
 200 0  2
 190
 27  0  100.0
* --
```

```
 [1]
*------------------------------------------------------------------------
*
*   CONNECTION MODULE COPMA-III
*
*------------------------------------------------------------------------
 COPMA3-CONNECTION
 1000  0  2
 1000 1001 190 100
 57   0    0.    0.
*----
 0 vmware-winxp
*     ^--------------------------------- host
 VALENT.position 2  VALENT.opStatus 0.01  0.99  1.0
 VALSAL.position 2  VALSAL.opStatus 0.01  0.99  1.0
 MASA.value     0
 SIMTIME.value  0
*
 VALENT.command  VALSAL.command
*1000             1001
* ^-----------------^------- Output variables
*
*------------------------------------------------------------------------
ASCII output -
20645
 200
   38
* ---
FILES/MASS.dat
(F7.2,1F6.2)
(A7,1A6)
 1  1  1
Mass
*--------------
```

FICHERO DE ENTRADA DEL CÓDIGO COPMA-III

```
valvecomponent VALENT;
valvecomponent VALSAL;

VALENT.command = "CLOSE";
VALENT.opStatus = "CLOSED";

VALSAL.command = "CLOSE";
VALSAL.opStatus = "CLOSED";

VALENT.openval = "0.99";
VALENT.closeval = "0.01";

VALSAL.openval = "0.99";
VALSAL.closeval = "0.01";



physmagnitude  MASA;
physmagnitude  SIMTIME;

MASA.value = "100";
```

PROCEDIMIENTO CIII-TRE-MAINI

```
*******************************************************************************
ProcedureOK
*******************************************************************************

PROCEDURE CIII-TRE-MAINI "PROCEDIMIENTO PRINCIPAL"

DESCRIPTION "PROCEDIMIENTO DE LANZAMIENTO"

STEP 1 "MAIN"

   INSTRUCTION 1 "MENSAJE DE INICIO"

      MESSAGE

      "SE INICIA LA EJECUCION DEL PROCEDMIENTO"

STEP 2 "EJECUCION DEL PROCEDIMIENTO"

   INSTRUCTION 1 "VERIFICAR CONDICIONES DE EJECUCION"

      INITIATE PROCEDURE CIIITRT-SM-TETLUID

STEP 3 "MAIN FUNCIONA"

   INSTRUCTION 1 "MENSAJE DE QUE TODO VA BIEN"

      MESSAGE

      "El procedimiento se esta ejecutando correctemente"

   INSTRUCTION 2 "MENSAJE DE QUE TODO VA BIEN"

      MESSAGE

      "El procedimiento se esta ejecutando correctemente. REPETIDO"

   INSTRUCTION 3 "LANZAMIENTO DEL PROCEDIMIENTO"

      INITIATE PROCEDURE CIIITRT-SM-TETL2UID

STEP 4 "FINALIZACION DEL PROCEDIMIENTO DE ARRANQUE"

   INSTRUCTION 1 "FINALIZACION DEL PROCEDIMIENTO"

      FINISH

ENDPROCEDURE
```

PROCEDIMIENTO CIIITRT-SM-TETL

```
*******************************************************************************
ProcedureOK
*******************************************************************************

PROCEDURE CIIITRT-SM-TETL "Procedimiento prueba comunicaciones
CIII/TRETA caso 1. Verificacion de WAIT y varias actividades"

STEP 1 "Mensaje"

   INSTRUCTION 1 "Mensaje"

      MESSAGE

      "Mensaje"

      COMMENT "TEXEC = 1 TASKLOAD = 10"

STEP 2 "Apertura de la valvula de entrada para llenar el deposito"

   INSTRUCTION 1 "Apertura de la valvula de entrada"

      ACTION

      OPEN VALENT.command

      COMMENT "TEXEC = 10 TASKLOAD = 50"

STEP 3 "Se vigila que el deposito se llena hasta 200 kg (en 10 s)"

   INSTRUCTION 1 "Vigilancia de llenado del deposito"

      WAIT FOR MASA.value > 200

      COMMENT "Cuando haya 200 kg se cumple (se supone tarda 10 s)
               TEXEC = 0 TASKLOAD = 0"

STEP 4 "Actuaciones asociadas a invetario de masa maximo"

   INSTRUCTION 1 "Actuaciones asociadas a inventario masico maximo"

      MESSAGE

      "Se cierra la valvula de entrada y se abre la de salida."

      COMMENT "TEXEC = 0  TASKLOAD = 0"

   INSTRUCTION 2 "Operacion de cierre"

      ACTION

      CLOSE VALENT.command

      COMMENT "TEXEC = 30 TASKLOAD = 100"

   INSTRUCTION 3 "Apertura de la valvula de salida"

      ACTION
```

```
      OPEN VALSAL.command

      COMMENT "TEXEC = 30 TASKLOAD = 100"

STEP 5 "Se vigila que el deposito se vacia hasta los 100 kg (en 10 s)"

   INSTRUCTION 1 "Vigilancia de llenado del deposito"

      WAIT FOR MASA.value < 100

      COMMENT "Cuando haya 100 kg se cumple (se supone tarda 10 s)
               TEXEC = 0 TASKLOAD = 0"

STEP 6 "Actuaciones asociadas a invetario de masa minimo"

   INSTRUCTION 1 "Actuaciones asociadas a inventario masico minimo"

      MESSAGE

      "Se cierra la valvula de salida y se finaliza el procedimiento."

      COMMENT "TEXEC = 0 TASKLOAD = 0"

   INSTRUCTION 2 "Operacion de cierre"

      ACTION

      CLOSE VALSAL.command

      COMMENT "TEXEC = 30 TASKLOAD = 25"

STEP 7 "Final del procedimiento"

   INSTRUCTION 1 "Finalizacion del procedimiento"

      FINISH

      COMMENT "TEXEC = 0  TASKLOAD = 0"

ENDPROCEDURE
```

PROCEDIMIENTO CIIITRT-SM-TETL2

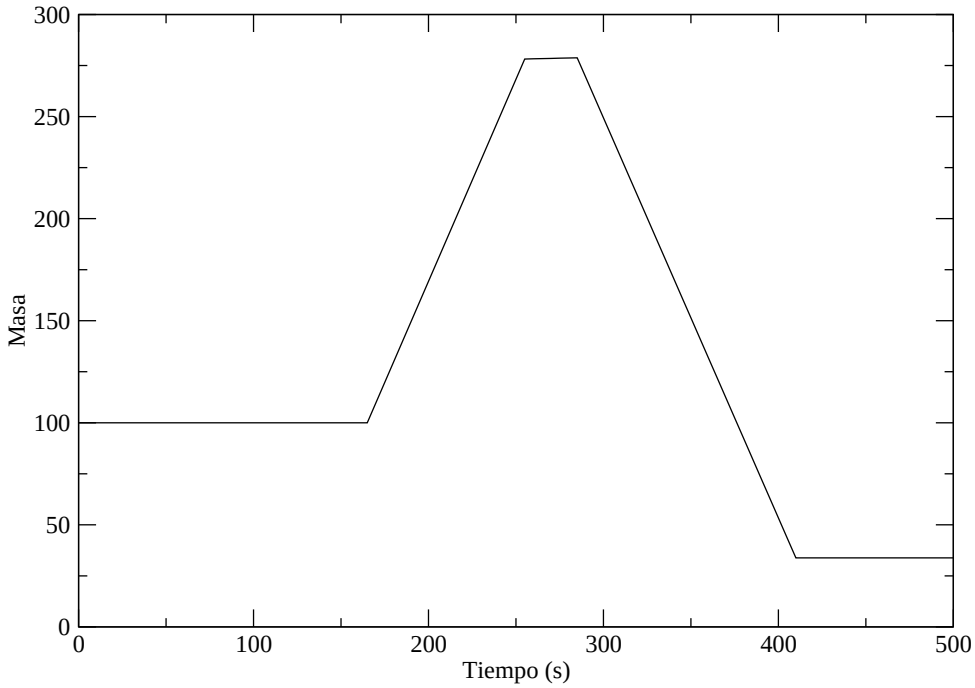
```
*******************************************************************************
ProcedureOK
*******************************************************************************

PROCEDURE CIIITRT-SM-TETL2 "Procedimiento complementario CIIITRT-SM-TETL"

STEP 1 "Se vigila que el deposito se vacia hasta los 100 kg (en 10 s)"

   INSTRUCTION 1 "Mensaje"

      MESSAGE

      "Mensaje"

      COMMENT "TEXEC = 1 TASKLOAD = 10"

   INSTRUCTION 2 "Vigilancia de vaciado del deposito"

      WAIT FOR MASA.value < 100

      COMMENT "Cuando haya 100 kg se cumple (se supone tarda 10 s)
               TEXEC = 0 TASKLOAD = 0"

STEP 2 "Apertura de la valvula de entrada para llenar el deposito"

   INSTRUCTION 1 "Apertura de la valvula de entrada"

      ACTION

      OPEN VALENT.command

      COMMENT "TEXEC = 10 TASKLOAD = 50"

STEP 3 "Se vigila que el deposito se llena hasta 200 kg (en 10 s)"

   INSTRUCTION 1 "Vigilancia de llenado del deposito"

      WAIT FOR MASA.value > 200

      COMMENT "Cuando haya 200 kg se cumple (se supone tarda 10 s)
               TEXEC = 0 TASKLOAD = 0"

STEP 4 "Actuaciones asociadas a invetario de masa maximo"

   INSTRUCTION 1 "Actuaciones asociadas a inventario masico maximo"

      MESSAGE

      "Se cierra la valvula de entrada y se abre la de salida."

      COMMENT "TEXEC = 0  TASKLOAD = 0"

   INSTRUCTION 2 "Operacion de cierre"

      ACTION

      CLOSE VALENT.command
```

```
      COMMENT "TEXEC = 30 TASKLOAD = 100"
   INSTRUCTION 3 "Apertura de la valvula de salida"
      ACTION
      OPEN VALSAL.command
      COMMENT "TEXEC = 30 TASKLOAD = 100"
   INSTRUCTION 4 "Prueba de la instruccion GOTO"
      GOTO 1 1
ENDPROCEDURE
```

5.2.2 Resultados del caso de prueba de la instrucción MONITOR

En esta prueba se ha modelado un ciclo de llenado, estando la condición de inicio del ciclo vigilada por una instrucción MONITOR. El resultado obtenido en la ejecución de la prueba se muestra en la Gráfica 5.2. Los ficheros de configuración del código TRETA y COPMA-III son iguales que los empleados en la prueba de la instrucción WAIT, cambiando solamente los procedimientos empleados.

Como se puede comprobar, el código COPMA-III simula adecuadamente el ciclo de llenado del depósito. La diferencia de los valores límite obtenidos en la simulación frente a las condiciones de control implementadas en los procedimientos se corresponden con los valores considerados de TEXEC y TASKLOAD para las actuaciones de apertura y cierre de las válvulas y con las deficiencias en la sincronización de los códigos ya comentadas en las pruebas de la instrucción WAIT.



Gráfica 5.2: Resultado de la prueba de comunicaciones de la instrucción MONITOR: masa de líquido en el depósito.

PROCEDIMIENTO CIII-TRE-MONMA

```
*******************************************************************************
ProcedureOK
*******************************************************************************

PROCEDURE CIII-TRE-MONMA "PROCEDIMIENTO PRINCIPAL"

DESCRIPTION "PROCEDIMIENTO DE LANZAMIENTO"

STEP 1 "MAIN"

   INSTRUCTION 1 "MENSAJE DE INICIO"

      MESSAGE

      "SE INICIA LA EJECUCION DEL PROCEDMIENTO"

STEP 2 "EJECUCION DEL PROCEDIMIENTO"

   INSTRUCTION 1 "VERIFICAR CONDICIONES DE EJECUCION"

      MONITOR

      IF     (     VALENT.opStatus IS CLOSED
                OR  VALSAL.opStatus IS OPEN )
         AND SIMTIME.value > 100.0
         AND MASA.value > 0.0
      INSIDE-INTERVAL
         FROM  CURRENT-TIME
         UNTIL FOREVER
      THEN
         GOTO 3 1
      ELSE
         GOTO 5 1

STEP 3 "NO FUNCIONA"

   INSTRUCTION 1 "MENSAJE DE MAL FUNCIONAMIENTO"

      MESSAGE

      "Si se llega hasta aqui es que algo no ha funcionado, el
      MONITOR o la inicializacion del nucleo de COPMA-III."

STEP 4 "FINALIZANDO MAL"

   INSTRUCTION 1 "FINALIZANDO MAL"

      FINISH

STEP 5 "MAIN FUNCIONA"

   INSTRUCTION 1 "MENSAJE DE QUE TODO VA BIEN"

      MESSAGE

      "El procedimiento se ejecuta de forma correcta"

   INSTRUCTION 2 "MENSAJE DE QUE TODO VA BIEN"
```

```
      MESSAGE
      "El procedimiento se ejecuta de forma correcta. REPETIDO."
   INSTRUCTION 3 "LANZAMIENTO DEL PROCEDIMIENTO"
      INITIATE PROCEDURE CIIITRT-SM-TETLUID
STEP 6 "FINALIZACION DEL PROCEDIMIENTO DE ARRANQUE"
   INSTRUCTION 1 "FINALIZACION DEL PROCEDIMIENTO"
      FINISH
ENDPROCEDURE
```

PROCEDIMIENTO CIIITRT-SM-TETL

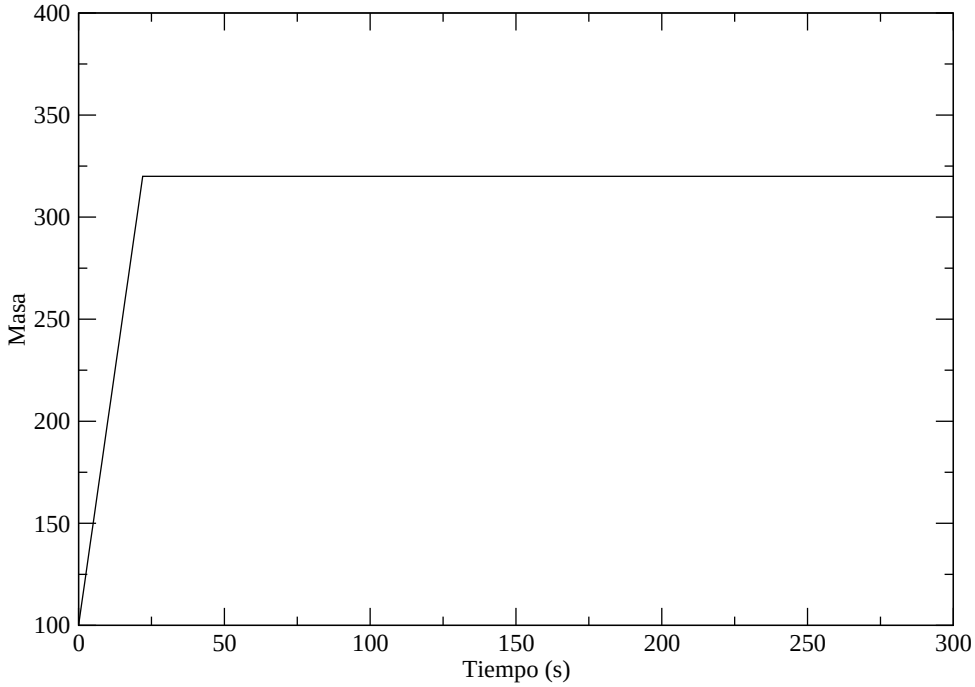
```
*******************************************************************************
ProcedureOK
*******************************************************************************

PROCEDURE CIIITRT-SM-TETL "Procedimiento prueba comunicaciones
CIII/TRETA caso 2"

STEP 1 "Mensaje"

   INSTRUCTION 1 "Mensaje"

      MESSAGE

      "mensaje"

      COMMENT "TEXEC = 1 TASKLOAD = 10"

STEP 2 "Apertura de la valvula de entrada para llenar el deposito"

   INSTRUCTION 1 "Apertura de la valvula de entrada"

      ACTION

      OPEN VALENT.command

      COMMENT "TEXEC = 10 TASKLOAD = 50"

   INSTRUCTION 2 "Apertura de la valvula de entrada"

      ACTION

      OPEN VALENT.command

      COMMENT "TEXEC = 10 TASKLOAD = 50"

STEP 3 "Se vigila que el deposito se llena hasta 200 kg (en 10 s)"

   INSTRUCTION 1 "Vigilancia de llenado del deposito"

      WAIT FOR MASA.value > 200

      COMMENT "Cuando haya 200 kg se cumple (se supone tarda 10 s)
               TEXEC = 0 TASKLOAD = 0"

STEP 4 "Actuaciones asociadas a invetario de masa maximo"

   INSTRUCTION 1 "Actuaciones asociadas a inventario masico maximo"

      MESSAGE

      "Se cierra la valvula de entrada y se abre la de salida."

      COMMENT "TEXEC = 0  TASKLOAD = 0"

   INSTRUCTION 2 "Operacion de cierre"

      ACTION
```

```
      CLOSE VALENT.command

      COMMENT "TEXEC = 30 TASKLOAD = 100"

   INSTRUCTION 3 "Apertura de la valvula de salida"

      ACTION

      OPEN VALSAL.command

      COMMENT "TEXEC = 30 TASKLOAD = 100"

STEP 5 "Se vigila que el deposito se vacia hasta los 100 kg (en 10
s)"

   INSTRUCTION 1 "Vigilancia de llenado del deposito"

      WAIT FOR MASA.value < 100

      COMMENT "Cuando haya 100 kg se cumple (se supone tarda 10 s)
               TEXEC = 0 TASKLOAD = 0"

STEP 6 "Actuaciones asociadas a invetario de masa minimo"

   INSTRUCTION 1 "Actuaciones asociadas a inventario masico minimo"

      MESSAGE

      "Se cierra la valvula de salida y se finaliza el procedimiento."

      COMMENT "TEXEC = 0 TASKLOAD = 0"

   INSTRUCTION 2 "Operacion de cierre"

      ACTION

      CLOSE VALSAL.command

      COMMENT "TEXEC = 30 TASKLOAD = 25"

STEP 7 "Final del procedimiento"

   INSTRUCTION 1 "Finalizacion del procedimiento"

      FINISH

      COMMENT "TEXEC = 0  TASKLOAD = 0"

ENDPROCEDURE
```

5.2.3 Resultados del caso de prueba del tipo de variable *generalvariable*

En esta prueba se ha modelado el llenado del depósito, estando la configuración de las válvulas en posición de llenado, VALENT abierta y VALSAL cerrada, y de vaciado, VALENT cerrada y VALSAL abierta, controlada por una variable de estado de sistema con dos modos de operación. El resultado obtenido en la ejecución de la prueba se muestra en la Gráfica 5.3. Los ficheros de configuración del código TRETA y COPMA-III, tanto como el procedimiento empleado, se muestran a continuación de la gráfica.

Como se puede comprobar, el código COPMA-III simula adecuadamente el llenado del depósito. La diferencia de los valores límite obtenidos en la simulación frente a las condiciones de control implementada en el procedimiento se corresponden se corresponden con fallos de sincronización de las comunicaciones.



Gráfica 5.3: Resultado de la prueba de comunicaciones de las estructuras *generalvariable*: masa de líquido en el depósito.

FICHERO DE ENTRADA DEL CÓDIGO TRETA

```
************************************************************
* TRETA-COPMA-III CONNECTION TEST 3
*
************************************************************
*
TRETA-COPMA-III CONNECTION
300 1.0
*
1
*----------------------
*
*---------------------------------------------------------------------
*
*   CONNECTION MODULE COPMACREW
*
*---------------------------------------------------------------------
 Copmacrew interface
 10
 0
 1007
* --
 vmware-winxp  CIIITRE-VARGENUID
*---------------------------------------------------------------------
 Simulation time
 100
 0
 27
* --
 [T]
*---------------------------------------------------------------------
 Masa entra
 120  0  2
 1010
 27
* --
 10*[1]
*---------------------------------------------------------------------
 Masa
 190 0  2
 120 200
 27
* --
 [1]+[2]
*---------------------------------------------------------------------
 Masa plus
 200 0  2
 190
 27  0  100.0
* --
 [1]
*---------------------------------------------------------------------
*
*   CONNECTION MODULE COPMA-III
*
*---------------------------------------------------------------------
 COPMA3-CONNECTION
 1000  0  2
 1010 190 100
```

```
 57   0    0.    0.
*----
 0 vmware-winxp
*     ^--------------------------------- host
 SYSTEM.mode    5
 MASA.value     0
 SIMTIME.value  0
*
 SYSTEM.command
*1000
* ^------------------ Output variable
*
*-------------------------------------------------------------------------
 Retrasa la actuacion del operador 10 s
 1010 0  2
 1000
    9
* --
 10.0
*-------------------------------------------------------------------------
ASCII output -
20645
 200
   38
* ---
FILES/MASS.dat
(F7.2,1F6.2)
(A7,1A6)
 1  1  1
Mass
*--------------
```

FICHERO DE ENTRADA DEL CÓDIGO COPMA-III

```
valvecomponent VALENT;
valvecomponent VALSAL;

VALENT.command = "CLOSE";
VALENT.opStatus = "CLOSED";

VALSAL.command = "CLOSE";
VALSAL.opStatus = "CLOSED";

VALENT.openval = "0.99";
VALENT.closeval = "0.01";

VALSAL.openval = "0.99";
VALSAL.closeval = "0.01";

physmagnitude  MASA;
physmagnitude  SIMTIME;

MASA.value = "50";

generalvariable SYSTEM;
SYSTEM.mode = "MODE1";
SYSTEM.mode1val = "0";
SYSTEM.mode2val = "1";
```

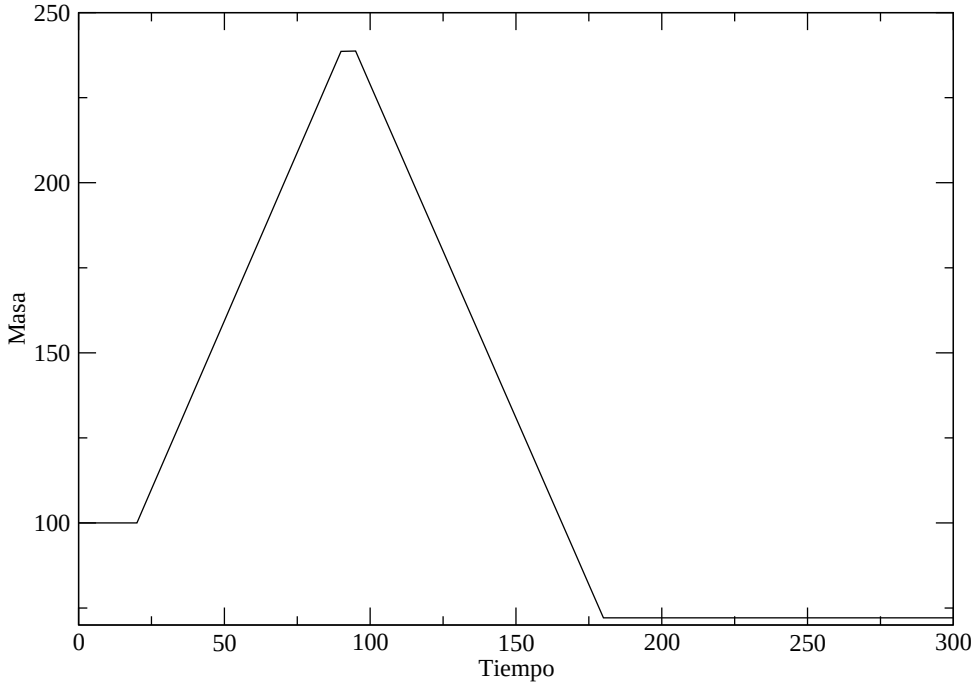
PROCEDIMIENTO CIIITRE-VARGEN

```
*******************************************************************************
ProcedureOK
*******************************************************************************

PROCEDURE CIIITRE-VARGEN "PROCEDIMIENTO PRINCIPAL"

DESCRIPTION "PROCEDIMIENTO DE LANZAMIENTO"

STEP 1 "VARGEN"

   INSTRUCTION 1 "MENSAJE DE INICIO"

      MESSAGE

      "SE INICIA LA EJECUCION DEL PROCEDMIENTO"

STEP 2 "EJECUCION DEL PROCEDIMIENTO"

   INSTRUCTION 1 "CAMBIAMOS EL VALOR DE LA VARIABLE GENERAL"

      ACTION

      MODE2 SYSTEM.command

STEP 3 "ESPERAR A QUE LA MASA SUBA"

   INSTRUCTION 1 "ESPERAR A QUE LA MASA SUBAA"

      WAIT FOR MASA.value > 300.0

STEP 4 "EJECUCION DEL PROCEDIMIENTO"

   INSTRUCTION 1 "CAMBIAMOS EL VALOR DE LA VARIABLE GENERAL"

      ACTION

      MODE1 SYSTEM.command

STEP 5 "ESPERAR A QUE LA MASA SUBA"

   INSTRUCTION 1 "ESPERAR A QUE LA MASA SUBAA"

      WAIT FOR MASA.value > 500.0

STEP 6 "FINALIZACION DEL PROCEDIMIENTO"

   INSTRUCTION 1 "FINALIZACION DEL PROCEDIMIENTO"

      FINISH

ENDPROCEDURE
```

5.2.4 Resultados del caso de prueba de la instrucción AUTOCHECK

En esta prueba se ha modelado un ciclo de llenado, estando la condición de inicio del ciclo condicionada por una instrucción AUTOCHECK. La prueba es similar a la realizada para la instrucción MONITOR. El resultado obtenido en la ejecución de la prueba se muestra en la Gráfica 5.4. Los ficheros de configuración del código TRETA y COPMA-III son iguales que para el caso de prueba de la instrucción WAIT, cambiando solamente los procedimientos empleados.

Como se puede comprobar, el código COPMA-III simula adecuadamente el ciclo de llenado del depósito. La diferencia de los valores límite obtenidos en la simulación frente a las condiciones de control implementadas en los procedimientos se corresponden con los valores considerados de TEXEC y TASKLOAD para las actuaciones de apertura y cierre de las válvulas y con los dos ciclos de computación requeridos por TRETA para recibir de COPMA-III la información del estado de las condiciones de llenado y vaciado.



Gráfica 5.4: Resultado de la prueba de de la instrucción AUTOCHECK: masa de líquido en el depósito.

PROCEDIMIENTO CIII-TRETA-MAIN

```
*****************************************************************************
ProcedureOK
*****************************************************************************

PROCEDURE CIII-TRETA-MAIN "PROCEDIMIENTO PRINCIPAL"

DESCRIPTION "PROCEDIMIENTO DE LANZAMIENTO"

STEP 1 "MAIN"

   INSTRUCTION 1 "MENSAJE DE INICIO"

      MESSAGE

      "SE INICIA LA EJECUCION DEL PROCEDMIENTO"

STEP 2 "EJECUCION DEL PROCEDIMIENTO"

   INSTRUCTION 1 "VERIFICAR CONDICIONES DE EJECUCION"

      AUTOCHECK

      IF     (     VALENT.opStatus IS CLOSED
                OR  VALSAL.opStatus IS OPEN )
         AND SIMTIME.value > 1000.0
         AND MASA.value < 0.0
      THEN
         GOTO 3 1
      ELSE
         GOTO 5 1

STEP 3 "NO FUNCIONA"

   INSTRUCTION 1 "MENSAJE DE MAL FUNCIONAMIENTO"

      MESSAGE

      "Si has llegado hasta aqui es que algo no ha funcionado, el AUTOCHECK
       o la inicializacion del nucleo de COPMA-III."

STEP 4 "FINALIZANDO MAL"

   INSTRUCTION 1 "FINALIZANDO MAL"

      FINISH

STEP 5 "MAIN FUNCIONA"

   INSTRUCTION 1 "MENSAJE DE QUE TODO VA BIEN"

      MESSAGE

      "El procedimiento se esta ejecutando de forma correcta"

   INSTRUCTION 2 "MENSAJE DE QUE TODO VA BIEN"

      MESSAGE
```

```
      "El procedimiento se esta ejecutando de forma correcta REPETIDO"
   INSTRUCTION 3 "LANZAMIENTO DEL PROCEDIMIENTO"
      INITIATE PROCEDURE CIII-TRETASINMONUID
STEP 6 "FINALIZACION DEL PROCEDIMIENTO DE ARRANQUE"
   INSTRUCTION 1 "FINALIZACION DEL PROCEDIMIENTO"
      FINISH
ENDPROCEDURE
```

PROCEDIMIENTO CIII-TRETASINMON

```
*******************************************************************************
ProcedureOK
*******************************************************************************

PROCEDURE CIII-TRETASINMON "Procedimiento prueba comunicaciones
CIII/TRETA caso 4"

STEP 1 "Mensaje"

   INSTRUCTION 1 "Mensaje"

      MESSAGE

      "mensaje"

STEP 2 "Apertura de la valvula de entrada para llenar el deposito"

   INSTRUCTION 1 "Apertura de la valvula de entrada"

      ACTION

      OPEN VALENT.command

STEP 3 "Se vigila que el deposito se llena hasta 200 kg (en 10 s)"

   INSTRUCTION 1 "Vigilancia de llenado del deposito"

      WAIT FOR MASA.value > 200

      COMMENT "Cuando haya 200 kg se cumple (se supone tarda 10 s)"

STEP 4 "Actuaciones asociadas a invetario de masa maximo"

   INSTRUCTION 1 "Actuaciones asociadas a inventario masico maximo"

      MESSAGE

      "Se cierra la valvula de entrada y se abre la de salida."

   INSTRUCTION 2 "Operacion de cierre"

      ACTION

      CLOSE VALENT.command

   INSTRUCTION 3 "Apertura de la valvula de salida"

      ACTION

      OPEN VALSAL.command

STEP 5 "Se vigila que el deposito se vacia hasta los 100 kg (en 10
s)"

   INSTRUCTION 1 "Vigilancia de llenado del deposito"

      WAIT FOR MASA.value < 100
```

```
      COMMENT "Cuando haya 100 kg se cumple (se supone tarda 10 s)"
STEP 6 "Actuaciones asociadas a invetario de masa minimo"
   INSTRUCTION 1 "Actuaciones asociadas a inventario masico minimo"
      MESSAGE
      "Se cierra la valvula de salida y se finaliza el procedimiento."
   INSTRUCTION 2 "Operacion de cierre"
      ACTION
      CLOSE VALSAL.command
STEP 7 "Final del procedimiento"
   INSTRUCTION 1 "Finalizacion del procedimiento"
      FINISH
ENDPROCEDURE
```

5.3 Conclusiones relativas a la interfase de comunicaciones de TRETA/COPMA-III

Tras la realización de un conjunto completo de pruebas para la verificación de la funcionalidad de comunicaciones y de computerización de los procedimientos se concluye:

- **Respecto a la funcionalidad de comunicaciones**, Tabla 5.6, la implementación de las funciones de llamada de COPMA-III es adecuada en todos los casos, siendo a su vez la implementación en el código TRETA tanto de la llamada como del tratamiento de la información correcta.

  El único problema detectado se corresponde con las limitaciones de sincronización procedentes del código COPMA-III, ya que la PDB y el núcleo son procesos asíncronos sin capacidad de operar de forma síncrona. Durante el trabajo realizado, el grupo del HRP implementó en el código COPMA-III cierta capacidad de sincronización de los diferentes procesos que componen el sistema y de los elementos del núcleo. En los resultados se observa que cada señal de sincronización requiere del orden de tres o cuatro segundos para ser devuelta por COPMA-III y recibir el código TRETA la información solicitada. Estos tiempos de respuesta son prohibitivos para la naturaleza de las simulaciones que se esperan llevar a cabo con el simulador integral.

  En las pruebas realizadas[7] esta limitación se manifiesta en una demora en la gestión del estado de las condiciones de instrucciones WAIT y MONITOR, lo que provoca que el código TRETA pueda presentar demoras en los tiempos de actuación sobre sistemas y componentes no estipuladas en el modelo de procedimientos, y motivadas exclusivamente por la falta de sincronización del código COPMA-III. Cabe enfatizar, que la ausencia de sincronización suele resolverse en la mayoría de los casos en pocos ciclos de simulación de TRETA, lo que conlleva normalmente demoras de décimas de segundo o un segundo, intervalo de tiempo poco significativo en la simulación de actuaciones humanas, en las que los tiempos de ejecución de las instrucciones de los procedimientos suele estimarse en minutos o varias decenas de segundos.

- En lo que respecta a la funcionalidad de la computerización de los procedimientos, Tabla 5.7, todos los resultados han sido satisfactorios. En esta tabla los casos enumerados se corresponden con las pruebas presentadas en este capítulo:

  – Caso 1: caso de prueba de la instrucción WAIT.
  – Caso 2: caso de prueba de la instrucción MONITOR.
  – Caso 3: caso de prueba del tipo de variable *generalvariable*.
  – Caso 4: caso de prueba de la instrucción AUTOCHECK.

[7] En las pruebas aquí incluidas se ha conseguido pormenorizar este problema fijando lo tiempos de espera en la sincronización en valores superiores a los cuatro segundos, tiempo requerido por la PDB de COPMA-III para sincronizar todos los procesos dependientes del núcleo.

Actualmente, en colaboración con la empresa Indizen y dentro del marco del proyecto «Investigación de sistema basado en XML de simulación de procedimientos para plantas nucleares(SIMPROC)», del programa PROFIT del Ministerio de Industria de España, se está diseñando un simulador de procedimientos mejorado, denominado SIMPROC, orientado a exclusivamente a la simulación automatizada de procedimientos de operación. Este trabajo se describe en el Capítulo 7, dentro del conjunto de líneas de trabajo consideradas a corto plazo.

Función/funcionalidad	**Caso 1**	**Caso 2**	**Caso 3**	**Caso 4**	**Estado**
INITIALIZE_SESSION	X	X	X	X	Correcto
SPWRF_WRAPPER					
Actualización variables	X	X	X	X	Correcto
Sincronización	X	X	X	X	No resuelto
OPEN_OPERATOR_SUBSCRIPTION	X	X	X	X	Correcto
PROC_VAR_UPDATES	X	X	X	X	Correcto
TERMINATE_SESSION	X	X	X	X	Correcto
SWITCH_TO_ACTIVITY	X	X	X	X	Correcto
CREATE_ACTIVITY	X	X	X	X	Correcto
GET_INSTRUCTION_DETAILS	X	X	X	X	Correcto
EXECUTE_CURRENT_INSTRUCTION	X	X	X	X	Correcto
GET_EVALUATIONS_AND_VALUE					
Gestión MONITOR		X			Correcto
Gestión WAIT	X	X	X	X	Correcto

Tabla 5.6: Resultado de las pruebas de funcionalidad de comunicaciones TRETA/COPMA-III.

Instrucción	**Caso 1**	**Caso 2**	**Caso 3**	**Caso 4**	**Estado**
INITIATE	X				Correcto
FINISH	X	X	X	X	Correcto
WAIT	X	X	X	X	Correcto
MONITOR		X			Correcto
ACTION	X	X		X	Correcto
AUTOCHECK				X	Correcto
GOTO	X				Correcto
MESSAGE	X	X	X	X	Correcto

Tabla 5.7: Resultado de las pruebas de ejecución de las instrucciones Prola.

Capítulo 6

Aplicación del simulador integral TRETA/COPMA-III

Índice

A lo largo de los capítulos anteriores se ha realizado una descripción detallada de los diferentes elementos que constituyen lo que he venido a denominar como el simulador integral TRETA/COPMA-III. Se han descrito tanto los procesos de modelado como los propios modelos de la CN PWR-W genérica, Capítulo 3, y de los EOP relativos a la gestión de emergencias en este tipo de centrales nucleares, Capítulo 4. Además, se ha explicado cual ha sido el protocolo de comunicaciones escogido entre las diferentes posibilidades y la funcionalidad del mismo, Capítulo 5.

En este capítulo se presentan los resultados obtenidos de la aplicación del simulador integral TRETA/COPMA-III a las secuencias accidentales de roturas en línea de vapor. El objetivo de dicha aplicación no es realizar un estudio de las capacidades de la herramienta, que se realizará de forma conceptual en el Capítulo 7 dedicado a las conclusiones del trabajo realizado, sino valorar la funcionalidad implementada en la herramienta respecto a las especificaciones de diseño consideradas en la Sección 2, donde se enumeraron los objetivos de este trabajo.

La estructura de este capítulo se articula en tres partes:

- Primeramente, se realiza la descripción teórica de la secuencias escogida para la prueba de la herramienta. Para la realización del modelo de procedimientos y de planta se llevó a cabo una revisión bibliográfica extensa de este tipo de secuencias. A partir de este estudio, se definieron los fenómenos físicos de relevancia en estas secuencias y el impacto de las actuaciones del operador en su modelado.

- Posteriormente, se procede a la descripción de la funciones implementadas en el modelo de planta del código TRETA y el desarrollo del modelo de EOP del código COPMA, ambos orientados de forma exclusiva al tipo de secuencias accidentales considerado, llevando a cabo la relación entre los diferentes elementos de ambos modelos y su conexión con las actuaciones del operador esperadas durante la secuencia accidental.

- Finalmente, se presentan los resultados obtenidos en la aplicación de la herramienta desarrollada a los transitorios, realizando una valoración de los mismos, tanto desde el punto de vista de los objetivos de diseño de la propia herramienta como de los resultados esperados para la secuencia accidental simulada.

6.1 Secuencias accidentales escogidas para la aplicación de la herramienta

El objetivo de la aplicación consiste en demostrar que la funcionalidad implementada en la herramienta es suficiente para realizar la simulación de actuaciones manuales del operador en transitorios que demanden cierta complejidad en la gestión de sistemas y procesos. En este sentido, la elección del conjunto de secuencias accidentales se ha realizado considerando las actuaciones demandadas al operador a lo largo de las distintas fases de las secuencias, suponiendo en todo momentos diferentes grados de fiabilidad de componentes y sistemas, lo cual

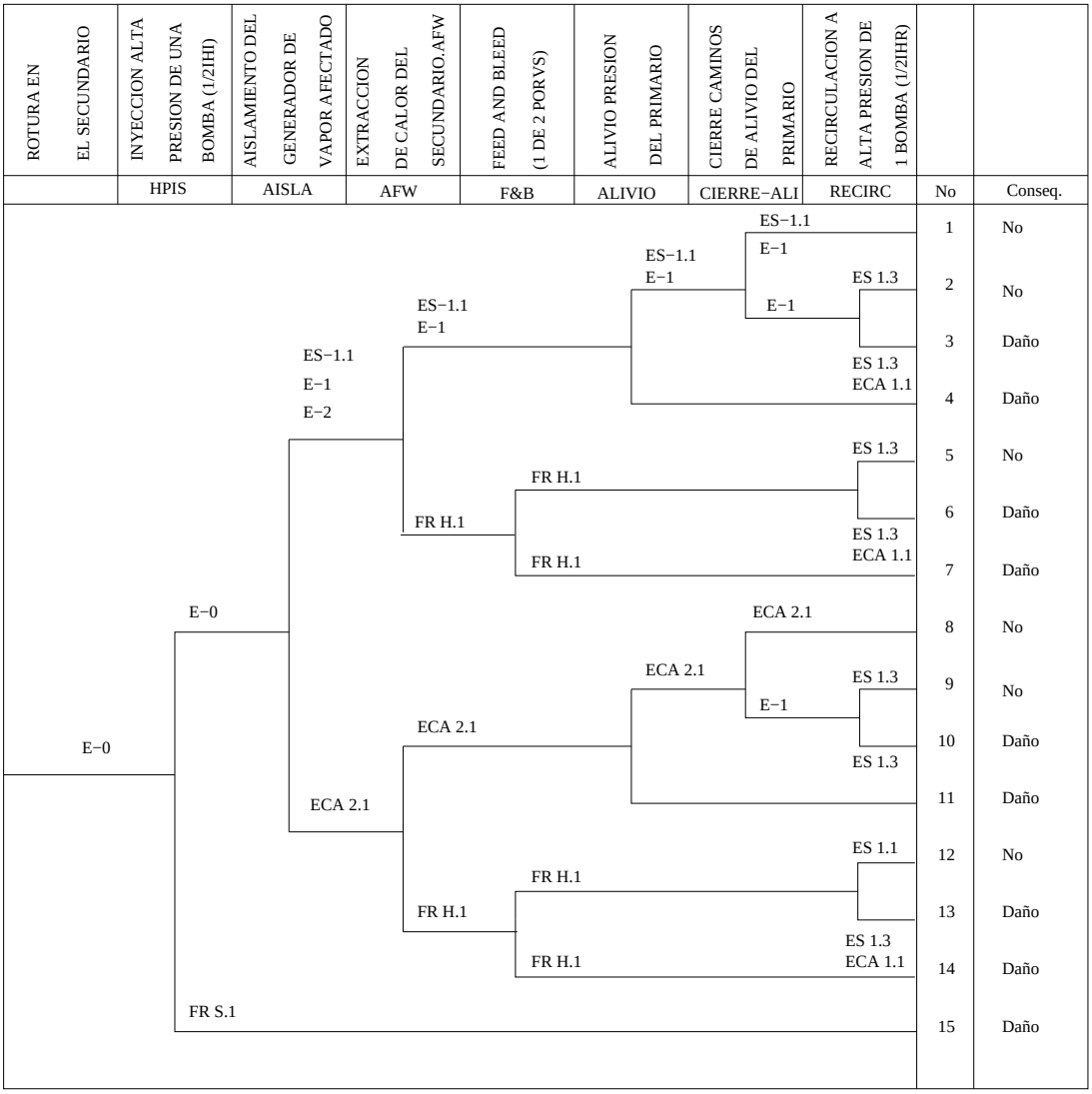


Figura 6.1: Árbol de sucesos genérico para las secuencias de roturas del secundario.

implica la posibilidad de que los fallos considerados imposibiliten la realización de las funciones de seguridad asociadas.

Las secuencias seleccionadas han sido las secuencias de roturas de secundario (*Secondary Side Breaks*, SSB), realizándose una extensa y detallada revisión bibliográfica que abarcó desde los informes de análisis de seguridad, los PSA de plantas españolas, las bases de las guías de respuesta ante emergencias (*Emergency Response Guidelines*, ERG) y los artículos y estudios relacionados, Expósito et al. (2004). Como resultado final de este estudio, se obtuvo un árbol de sucesos genérico, Figura 6.1, con la estructura completa de los EOP demandados y sus dependencias.

Dentro de estas secuencias, los transitorios se suelen clasificar en función del tamaño de la rotura como, Tecnatom (1986) y WOG (1997):

- Rotura pequeña a potencia:

  Los sistemas de control de la central son capaces de mantener la central cerca de las condiciones nominales. Así, no se requiere actuación por parte del operador, siendo la respuesta similar a la que se da a un aumento escalonado de carga. Los efectos de este tipo de transitorios es un aumento del caudal de vapor, que provoca, a su vez, aumento del caudal de agua de alimentación, y un descenso de la temperatura del primario, provocando la actuación del sistema de control de barras para mantener la temperatura del primario.

- Rotura intermedia:

  Las consecuencias de este tipo de transitorios no pueden ser compensadas por el control de barras. Por ello, bajan la presión y la temperatura del secundario y del primario. El sistema de control de barras intenta mantener la temperatura hasta que se produce disparo del reactor (alto flujo neutrónico, $OP\Delta T$ o señal de SI), siempre posterior a los cinco primeros minutos del transitorio.

- Rotura grande:

  Se consideran dentro de esta categoría todas aquellas roturas que lleven a secuencias en las cuales se inicien funciones de protección durante los cinco primeros minutos del transitorio. Generalmente, la actuación de salvaguardias y el aislamiento de la línea de vapor se da entre los cinco y los diez segundos tras la rotura. En estas secuencias se supone el disparo del reactor sin barra atascada, no considerándose la posible vuelta a criticidad del reactor a lo largo del transitorio.

En los casos de aplicación se consideraron las roturas localizadas en las líneas de vapor, el colector de las líneas de vapor y el colector del agua de alimentación principal, Figura 6.2:

- La rotura grande aislable en el colector de las líneas de vapor. La gestión de la secuencia se realiza sin fallos asociados a ningún sistema o componente.

- La rotura grande no aislable en la línea de vapor dos, asociada al lazo con presionador, fuera del edificio de contención. Considerando el modelo de planta, este lazo es el único que se puede emplear para la simulación de transitorios asimétricos. En la secuencia no se postularon fallos asociados a ningún sistema o componente.

- La pérdida total de agua de alimentación por rotura grande en el colector del agua de alimentación principal con fallo en la recuperación del suministro de agua a los generadores de vapor y, por lo tanto, implicando la pérdida del sumidero de calor, llegándose a ejecutar la operación de aporte y purga del primario (*Feed and Bleed*, F&B). Al postularse fallos múltiples, la gestión de la emergencia se deberá realizar mediante el uso de las FRG, tal como se diseña la estructura de los EOP. De hecho, la operación de F&B se considera en la FRG H.1 de *Respuesta ante la pérdida de sumidero de calor*, comprobándose durante el estudio de esta secuencia que la transferencia a dicho procedimiento es directa.

Este tipo de secuencias tienen especial importancia desde el punto de vista de la gestión del accidente por el operador debido a:

- En el caso de las roturas grandes en el secundario se puede destacar:

    1. Estos transitorios presentan dificultades en su diagnóstico ya que los síntomas asociados a los mismos durante la primera esta del transitorio son similares a los que caracterizan a las secuencias de LOCA, Kim et al. (2005). En este sentido, la fenomenología de ambos accidentes se diferencia en la recuperación del inventario del primario con la actuación de la inyección de seguridad. Este aspecto queda patente en la estructura de los EOP y se explicará en detalle en la sección dedicada al modelo de procedimientos computerizados.
    2. En el caso de las roturas no aislables, el aislamiento del generador de vapor defectuoso es una de las operaciones más críticas en la gestión de accidentes en reactores PWR debido a su complejidad, Higgins et al. (2004). Esta operación requiere de actuaciones tanto desde sala de control como locales, y las operaciones se pueden prolongar durante 30 o 40 minutos.
    3. A pesar de que son sucesos de muy baja probabilidad, tres veces menor que el SGTR por ejemplo, ciertos comportamientos durante la operación o malas políticas de mantenimiento muestran que existe cierta susceptibilidad latente de difícil estimación, Murphy (1993) y Marsden y Green (1996).

- En el caso de la pérdida total de agua de alimentación con pérdida de sumidero de calor se puede destacar respecto a la operación de F&B que:

    1. Es una de las más importantes en los estudios de PSA/HRA, considerando además el cambio a recirculación de ramas frías y la disminución de la presión de primario y secundario, Forester et al. (1996) y CSNI (1998). Todas ellas se llevan a cabo en diferentes etapas de este tipo de transitorios, siendo por lo tanto, secuencias de especial relevancia en los estudios de seguridad.
    2. El inicio del F&B es una de las decisiones más críticas y complejas que debe asumir el operador, pudiéndose destacar dos motivos. En primer lugar, implica el inicio de un LOCA en el primario en la operación de purga, hecho que los operadores tardan en decidir pues viola el criterio de gestión de accidentes relacionado con el mantenimiento del inventario del primario. En segundo lugar, las repercusiones de la purga del refrigerante a la contención, en costes de limpieza y de parada de la planta. Pruebas de esta problemática a la hora de estudiar la aplicación del F&B son:
        - Las ventanas temporales para el éxito de dicha operación consideradas en diferentes PSA a nivel internacional, que varían desde 20 a 75 minutos, llegando al caso extremo de los cinco minutos que se consideran en el PSA de la CN de Almaraz, CSNI (1998).

- De la misma forma, la probabilidad de fallo humana (HEP) de esta operación puede oscilar entre 10^{-3} a 10^{-1}, dependiendo del la secuencia en que se considere en F&B y el tipo de estudio realizado, CSNI (1998).
- La diversidad de estudios en los que se ha tratado su consideración e implementación en la gestión de emergencias, pudiendo citar por ejemplo a Bley y Stetkar (1988), Roth et al. (1994), Jakubowski y Beraha (1996) y Borgonovo et al. (2000), los estudios llevados a cabo en los Álamos tras el incidente de Davis Besse y otros tantos trabajos.
- El caso del trabajo realizado en EDF para el inicio y la ejecución del F&B mediante automatismos, Lanore et al. (1997).
- Finalmente, un ejemplo real de la reluctancia, el estrés y la carga cognitiva de este tipo de actuaciones quedó de manifiesto en el suceso de pérdida total de agua de alimentación de Davis Besse, NRC (1985) y Loomis y Cozzuol (1988).

3. A pesar de que el AFWS suele ser el segundo sistema, después del sistema de protección del reactor, con mayor fiabilidad exigida en sus especificaciones de diseño, FCFRNS (1996), los mecanismos de fallo que presenta en operación debido a factores de mantenimiento y diseño son muy variados, siendo difícil alcanzar dicho objetivo, Travis et al. (1990), Bumgardner et al. (1994) y Gertman et al. (2002). Cabe decir, que los aspectos de diseño ya han sido subsanados en su mayoría.

Por todo ello, estas secuencias son ampliamente tratadas en todo tipo de trabajos. Aquí podemos destacar los de naturaleza similar a la que se considera en este trabajo, como por ejemplo las simulaciones llevadas a cabo con la herramienta HERMES, para el estudio de procesos cognitivos con fallos de instrumentación en secuencias de SLB y TLFW, Cacciabue (1997a), o el análisis de los EOP relacionados con las secuencias de F&B mediante la herramienta EOPAS del GRS, considerando los tiempos empleados por el operador en transitorios de TLFW, Jakubowski y Beraha (1996). Estos trabajos se han considerado como referencia en la realización de la aplicación de la herramienta.

En las secciones siguientes se describe en detalle el modelo de EOP computerizado desarrollado y las modificaciones realizadas en el modelo de planta para soportarlos.

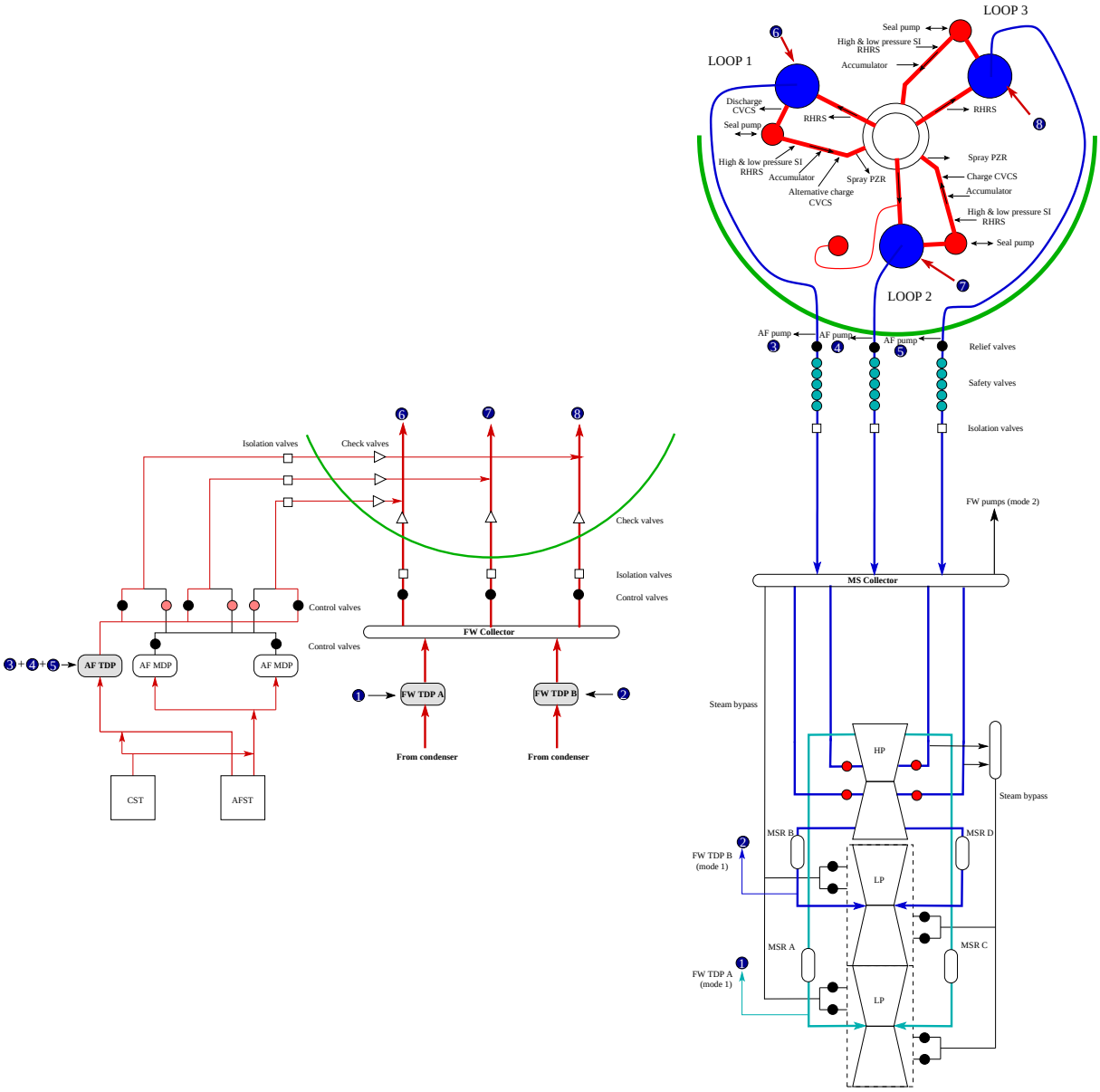


Figura 6.2: Esquema detallado de los sistemas de una planta PWR-W.

6.1.1 Modelo de procedimientos desarrollado para el código COPMA-III

Se ha considerado como objetivo prioritario la computerización de los EOP relacionados con los transitorios base seleccionados, es decir, SLB y TLFW. Los EOP que se definieron como relevantes fueron, Expósito et al. (2004), Figura 6.1:

- E-0: Procedimiento de Disparo del reactor y/o Inyección de Seguridad.
- ES-0.1: Procedimiento de recuperación del disparo del reactor.
- E-1: Procedimiento de pérdida de refrigerante del reactor o secundario.
- ES-1.1: Procedimiento de finalización de Inyección de Seguridad.
- E-2: Procedimiento de aislamiento de un Generador de Vapor defectuoso.
- FR-H.1: Respuesta ante la pérdida de sumidero de calor.
- FR-I.1: Respuesta ante alto nivel en el presionador.

A pesar de que las CSF inicialmente no fueron consideradas en el trabajo, su computerización se ha llevado a cabo mediante el análisis de los tiempos de diagnóstico del operador y de la evaluación de los tiempos de ejecución de los pasos de los procedimientos, realizándose su integración en la secuencia de seguimiento de los EOP, tal como se explicará en detalle más adelante.

En lo referente a la computerización de procedimientos, el nivel de detalle empleado ha sido reducido, Figuras 6.3 a 6.8, realizando validaciones lógicas sobre el estado de sistemas y la activación de controles manuales implementados en el modelo de planta. Estos controles simulan las actuaciones de control sobre el rango de variables físicas mediante la manipulación de componentes de ciertos sistemas de la planta. Su implementación se podría haber realizado en el simulador de procedimientos, quedando abierta la posibilidad de realizar dicha aproximación en posteriores desarrollos. Los motivos principales considerados en la elección de esta implementación en este trabajo han sido:

- Evitar complejidad innecesaria de la versión de los EOP computerizados, de forma que su seguimiento y mantenimiento fuese sencillo.
- Los modelos de sistemas implementados en el modelo de planta se corresponden con modelos matemáticos, en los cuales la inclusión de interfases que considerasen las actuaciones manuales habría supuesto una revisión de su estructura de cálculo.

Tras el estudio de la secuencia escogida, se puede concluir que los principales objetivos especificados en los EOP en lo que respecta a las roturas son:

1. Comprobar y verificar la correcta actuación de todos los sistemas de seguridad demandados. En esta categoría se encuentran englobadas las actuaciones del operador para verificar y controlar el caudal del AFW y para controlar la temperatura del RCS, EOP E-0, principalmente.

2. Aislar los SG afectados por la rotura, de forma que se garantice el sumidero de calor, EOP E-2.

3. Establecer condiciones estacionarias de planta, controlando la temperatura y la presión del RCS, el nivel de los SG operables y, reduciendo y parando la SI cuando sea necesario, EOP ES-1.1.

Para el caso de los transitorios de TLFW con pérdida de sumidero de calor:

1. Al igual que para el caso de las roturas, comprobar y verificar la correcta actuación de todos los sistemas de seguridad demandados, EOP E-0 y E-0.1.

2. Intentar mantener el sumidero de calor el máximo tiempo posible, realizando la parada de las RCP y las actuaciones necesarias para el suministro de agua a los SG. En caso de no tener éxito en las operaciones de aporte de agua a los SG, iniciar F&B en cuanto se presenten condiciones de pérdida de sumidero de calor, FRG FR-H.1.

El resto de actuaciones no se han considerado para su implementación detallada pero deben ser tomadas en cuenta a la hora de computar en la simulación el tiempos que requiere su ejecución, por ello deben ser computerizados pasos sin interacción con el simulador termohidráulico pero que incluyan la variable TEXEC con el valor adecuado. El resultado final, es un conjunto de actuaciones implementadas de forma secuencial en versiones resumidas de los procedimientos E-0, ES-0.1, ES-1.1, E-2 y FR-H.1, Figuras 6.9 a 6.14. En ningún momento se llegó a realizar la computerización del EOP E-1, *Procedimiento de pérdida de refrigerante del reactor o secundario*, ya que dicho procedimiento se considera cuando los transitorios de rotura se localizan dentro del edificio de contención y su fenomenología puede ser similar a la de una secuencia de LOCA. En las secuencias consideradas, las roturas están localizadas en el exterior del edificio de contención y los tiempos de diagnóstico son relativamente cortos, Tablas 6.1 y 6.2, debido, principalmente, a la rápida recuperación de la presión y el inventario del primario por la actuación de la inyección de seguridad, hecho inequívoco de que o el LOCA es pequeño o se trata de una SLB. Ante dicha posibilidad, el procedimiento E-0 realiza una transición al EOP ES-1.1 en el paso 23, Figura 6.3, donde reduciendo y parando la actuación de la SI de forma controlada, verifica la posible existencia de un pequeño LOCA, realizando una transición al final del paso 27 del procedimiento ES-1.1 al EOP E-1, Figura 6.5, en caso de verificarse que es necesario el aporte de inventario por parte de la SI y, por lo tanto, el transitorio no se corresponde con una SLB.

En lo que respecta a los tiempos de ejecución de los pasos, se muestra en las Tablas 6.5 a 6.9 los pasos de los procedimientos computerizados y los valores asociados a dicha variable.

Para su estimación se atendió a la bibliográfia relacionada con la simulación de transitorios con operadores, así como los estudios a nivel teórico de este tipo de secuencias.

En general, para las secuencias los tiempos se han extraído de sesiones de simulación con operadores, Tablas 6.3 y 6.4. En ambos casos se consideraron los tiempos medios, comprobando que dichos valores se corresponden con los que usualmente se empleaban en los estudios teóricos de estas secuencias, p. ej. Lanore et al. (1987), Bley y Stetkar (1988), Loomis y Cozzuol (1988), Champ y Cornille (1989), Roth-Seefrid et al. (1994), Petelin et al. (1994 1995) y Borgonovo et al. (2000). Para la secuencia TLFW con pérdida de sumidero de calor, cabe destacar el tiempo considerado para la parada de las RCP y de comprobación del sumidero de calor, pasos 3 y 8 de la FRG H.1, de 10 minutos aproximadamente. Este tiempo está condicionado por el salto a condición roja de a CSF de sumidero de calor, que como se comprobará en las simulaciones realizadas, está acorde con los tiempos considerados en el modelo de EOP. Para las secuencias de SLB la actuación más relevante es la parada de la SI para evitar el llenado excesivo del presionador, contemplada en la FRG I.1, aunque su criterio de ejecución en tiempos se ha llevado a cabo de forma condicionada a los tiempos diagnóstico del suceso de SLB, Tablas 6.1 y 6.2[1], en el paso 7.2 de la versión computerizada el EOP E-0, Figura 6.9, fijándose un valor de 390 s. desde entrada en el EOP E-0, valor aproximado al considerado en la base de diseño de los EOP de Westinghouse, WOG (1997).

Para el resto de actuaciones de ambas secuencias se han asignado tiempos considerando el verbo de acción relacionado con el paso y si su ejecución implica algún tipo de SA o DM. Cabe decir, que los valores implementados son orientativos. Una descripción de las posibles metodologías de estimación del tiempo de ejecución de instrucciones se trata en el Capítulo 7, destacando que no estaba dentro de los objetivos del trabajo su consideración.

DBA	**Tiempo EOP diagnóstico**		**Tiempo diagnóstico desde disparo**	
	Media (s)	σ (s)	Media (s)	σ (s)
LSLB	182,4	72,4	412,7	128,7
TLFW	137,2	89,8	300,8	157,8
LOCA	135,8	47,8	357,5	134,9
LOOP	106,7	39,9	271,7	79,4
SBO	101,3	55,3	251,7	78,6
SGTR	195,9	106,7	403,6	199,1

Tabla 6.1: Tiempo medio de ejecución del EOP E-0 y de diagnóstico desde disparo del reactor para las secuencias de LSLB, TLFW, LOCA, LOOP, SBO y SGTR, Park et al. (2005).

[1]En Park et al. (2005), se estima que en media el EOP E-0 tarda con un 95 % de margen de confianza 316 s., resultando en un tiempo de diagnóstico medio desde disparo del reactor de 599 s. Por otra parte, en Legaud et al. (1984) establece el tiempo de diagnóstico del SLB en 6 min. 43 s. con 1 min. 53 s. de desviación respecto al valor medio, el tiempo de localización en 7 min. 37 s. con 2 min. 16 s. de desviación y el tiempo de decisión en 10 min. 43 s. con 2 min. de desviación.

Suceso iniciador (EOP)	**Media**	σ
LOOP (I4B)	6 min 50 s	7 min 24 s
Pérdida del RHRS (IRRA2)	2 min 15 s	6 min 45 s
SGTR (A3)	12 min	1 min 24 s
LOCA (A10)	6 min 10 s	6 min
Pérdida sumidero calor (H1.1)	3 min 5 s	2 min 5 s
LFW (H2)	2 min 50 s	1 min 28 s
Media	5 min 32 s (332 s)	3 min (180 s)

Tabla 6.2: Tiempos de diagnóstico desde disparo de reactor para las secuencias de LOOP, pérdida del RHRS, SGTR, LOCA, pérdida de sumidero de calor y LNFW, Villemeur et al. (1986).

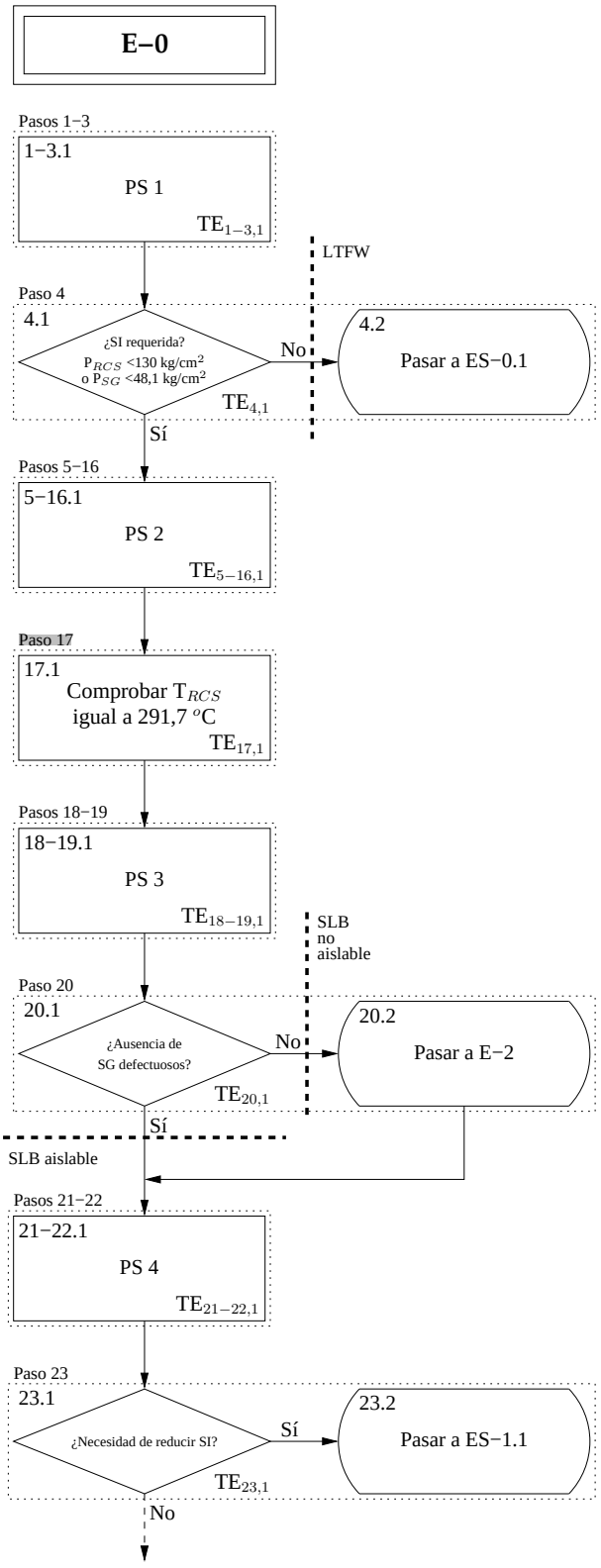


Figura 6.3: Esquema de la versión reducida del procedimiento E-0.

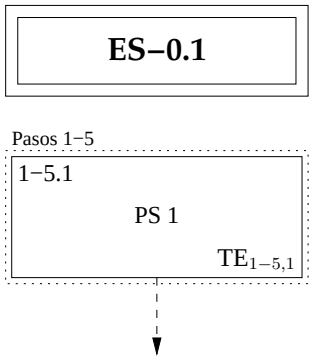


Figura 6.4: Esquema de la versión reducida del procedimiento ES-0.1.

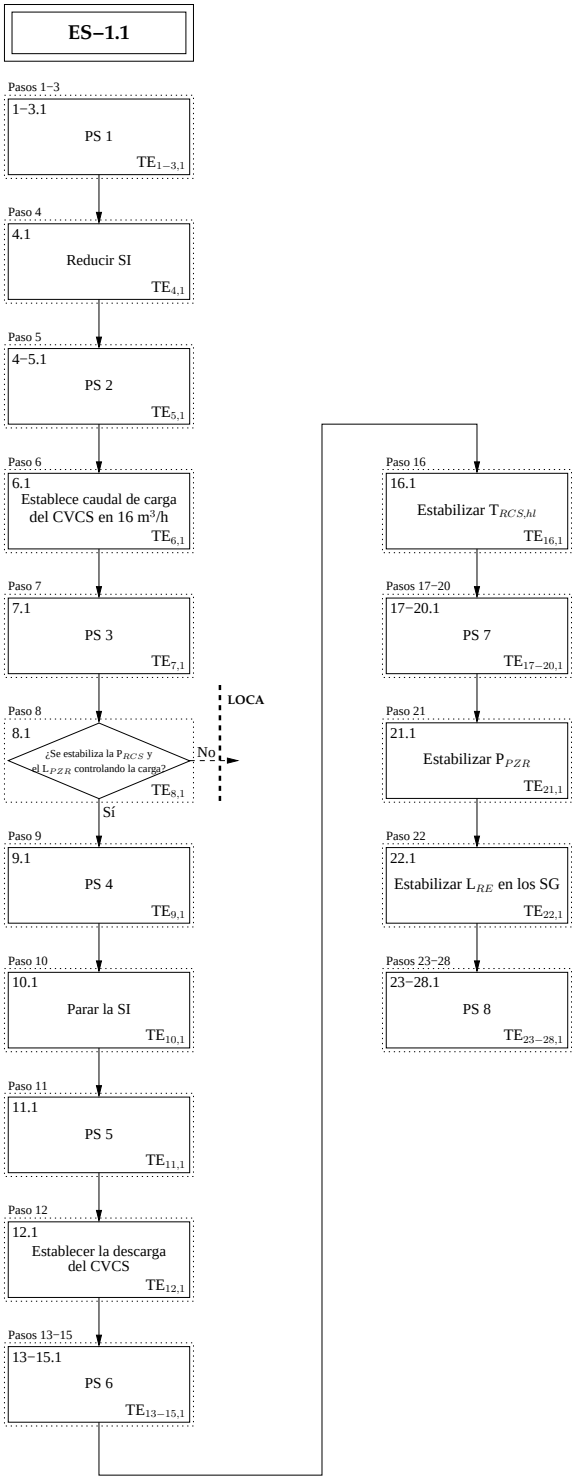


Figura 6.5: Esquema de la versión reducida del procedimiento ES-1.1.

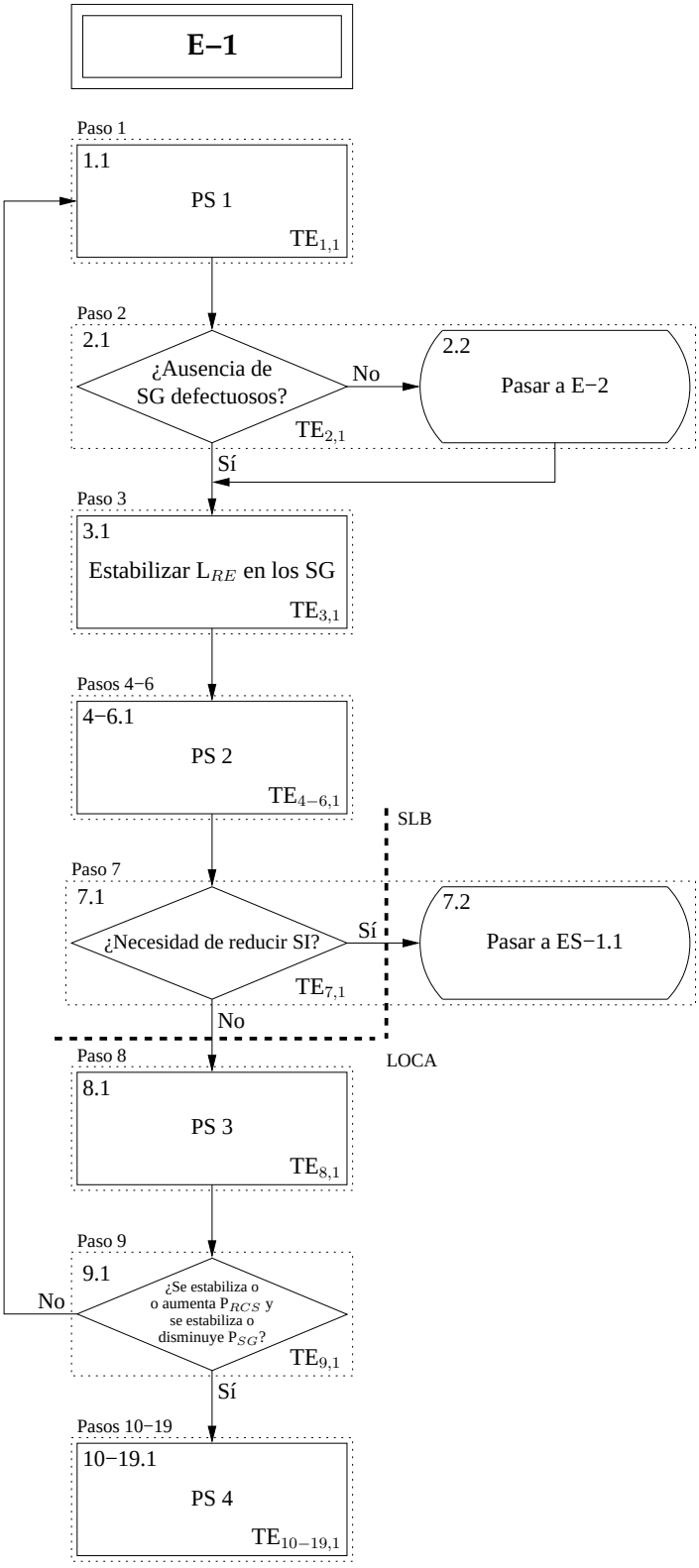


Figura 6.6: Esquema de la versión reducida del procedimiento E-1.

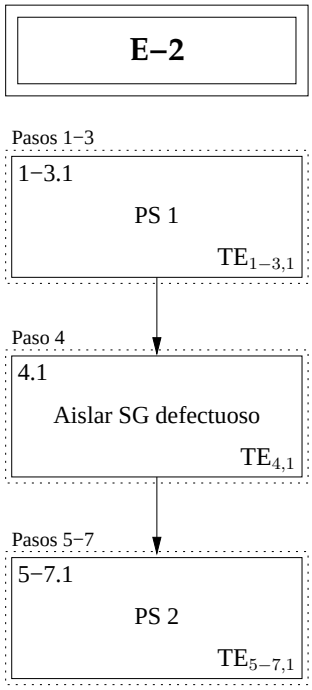


Figura 6.7: Esquema de la versión reducida del procedimiento E-2.

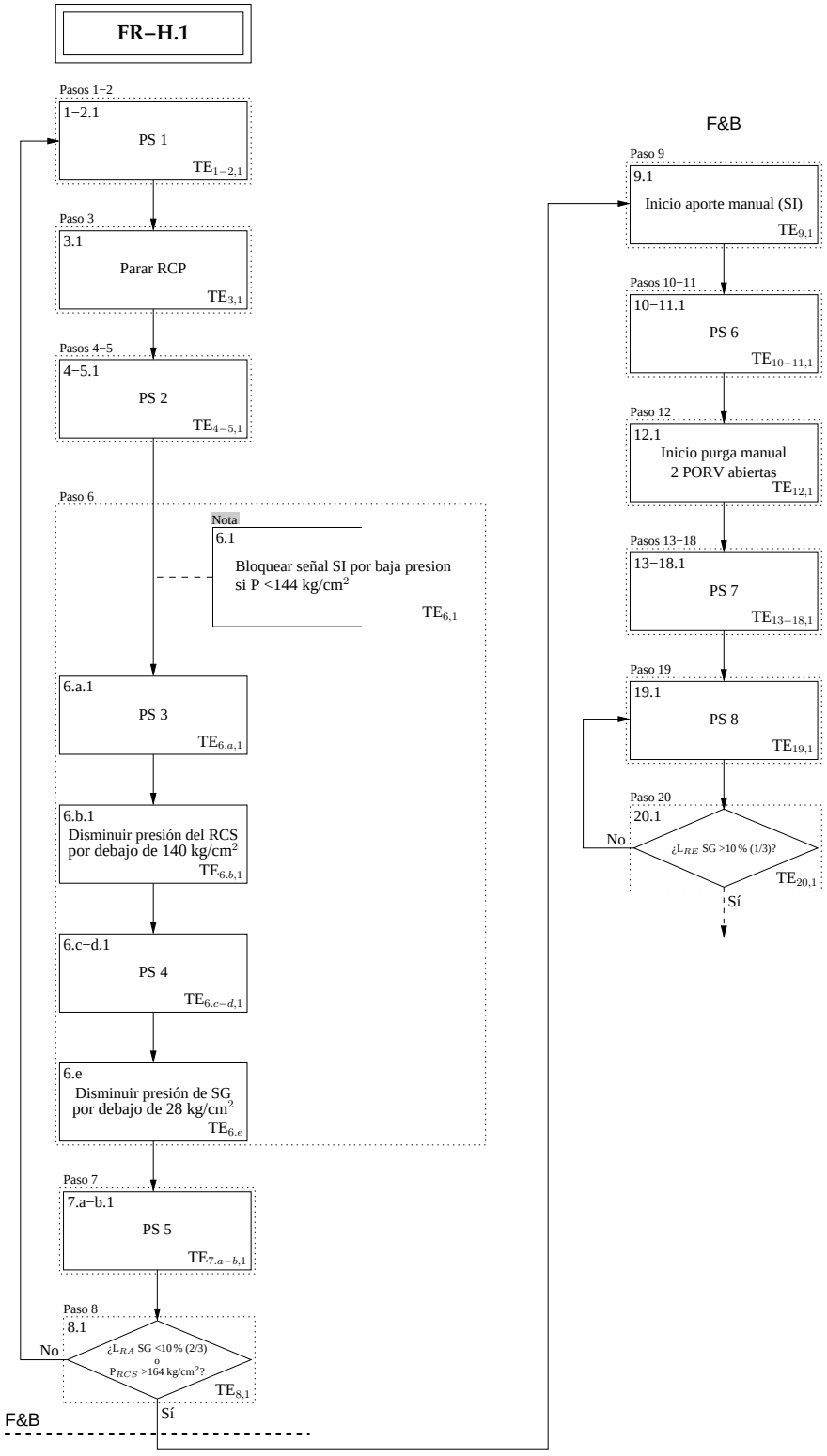


Figura 6.8: Esquema de la versión reducida del procedimiento FR-H.1.

Tarea	Tiempo medio (s)	Desviación estándar (s)
Suministro de caudal suficiente de SI	538,8	174,1
Finalización de refrigeración del RCS fuera de control	633,5	183,2
Comprobación de condiciones de parada de RCP	828,2	226,5
Estabilización de la temperatura y la presión del RCS	857,1	228,9
Comprobación de reducción o finalización de la SI	1118,6	238,3
Confirmación de la circulación natural del RCS	1571,7	192,3
Comprobación del criterio de rearranque de las RCP	1730,0	153,1

Tabla 6.3: Tiempos de realización de tareas en los transitorios de SLB, Park et al. (2005).

Tarea	Tiempo medio (s)	Desviación estándar (s)
Parada de las RCP	415,4	246,3
Mantenimiento del inventario de agua de los SG	556,9	137,6
Comprobación del criterio para F&B	565,6	286,4
Verificación de circulación natural en el RCS	791,6	161,8

Tabla 6.4: Tiempos de realización de tareas en los transitorios de TLFW, Park et al. (2005).

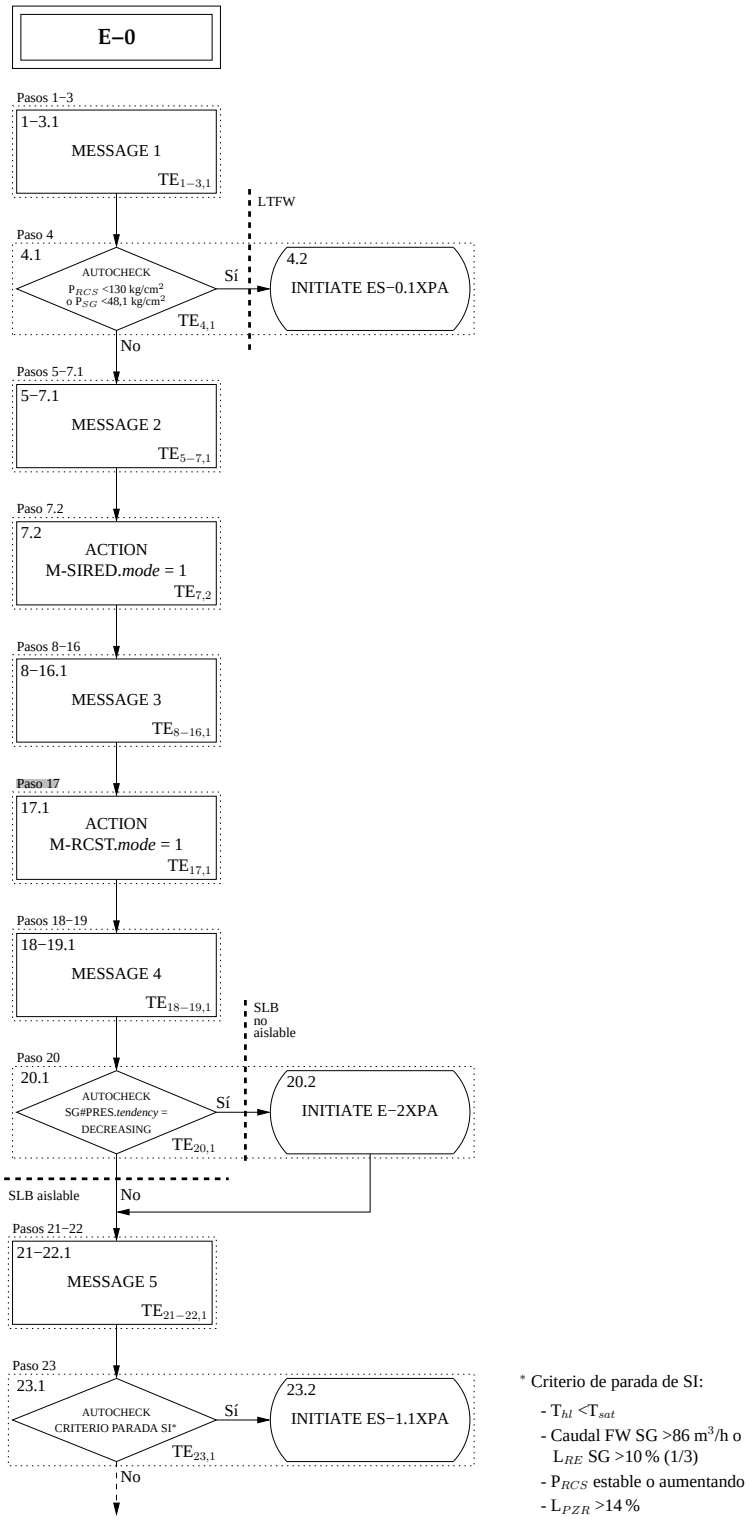


Figura 6.9: Esquema del procedimiento E-0 computerizado (versión reducida).

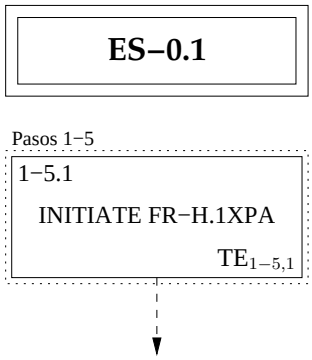


Figura 6.10: Esquema del procedimiento ES-0.1 computerizado (versión reducida).

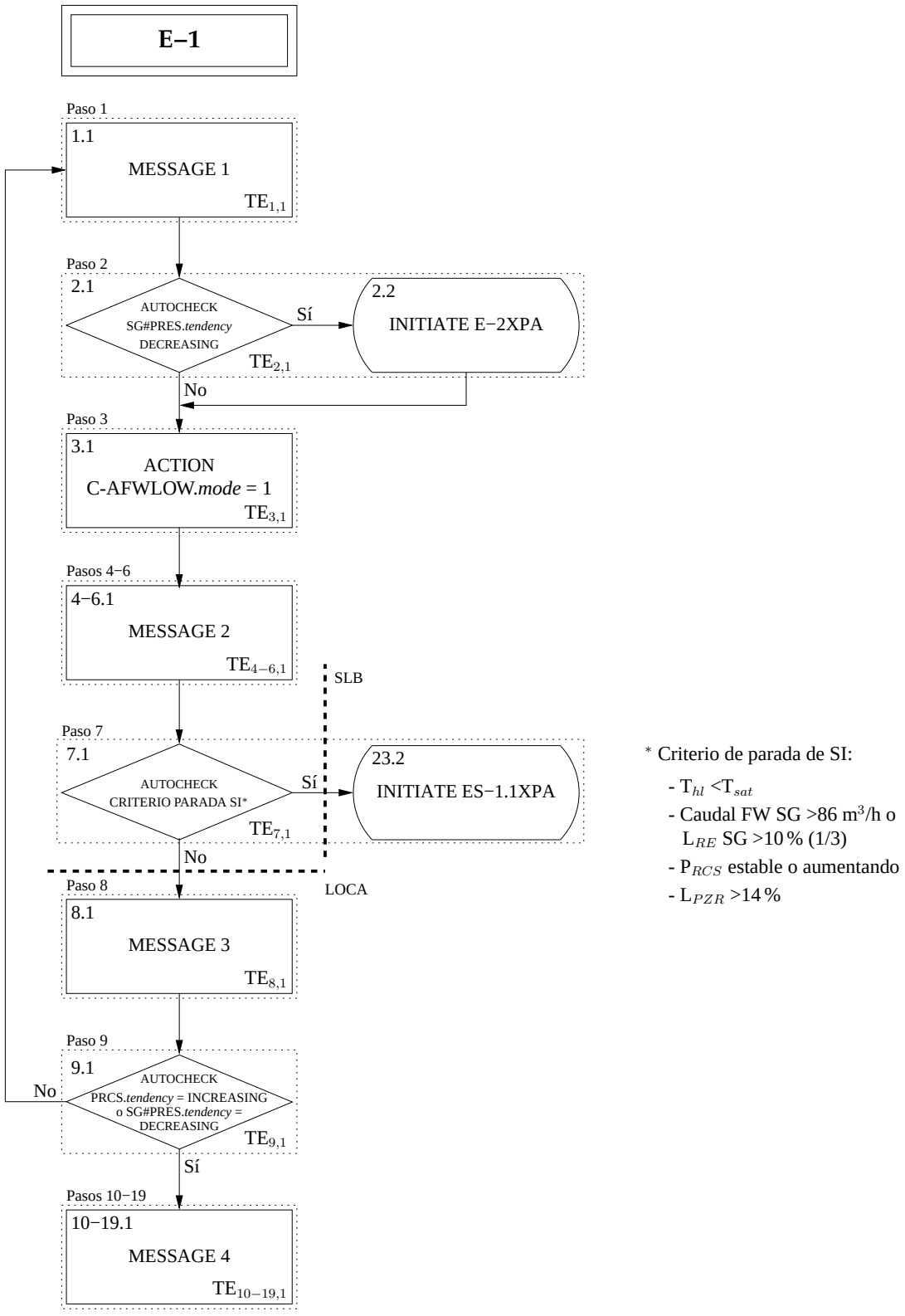


Figura 6.11: Esquema del procedimiento E-1 computerizado (versión reducida).

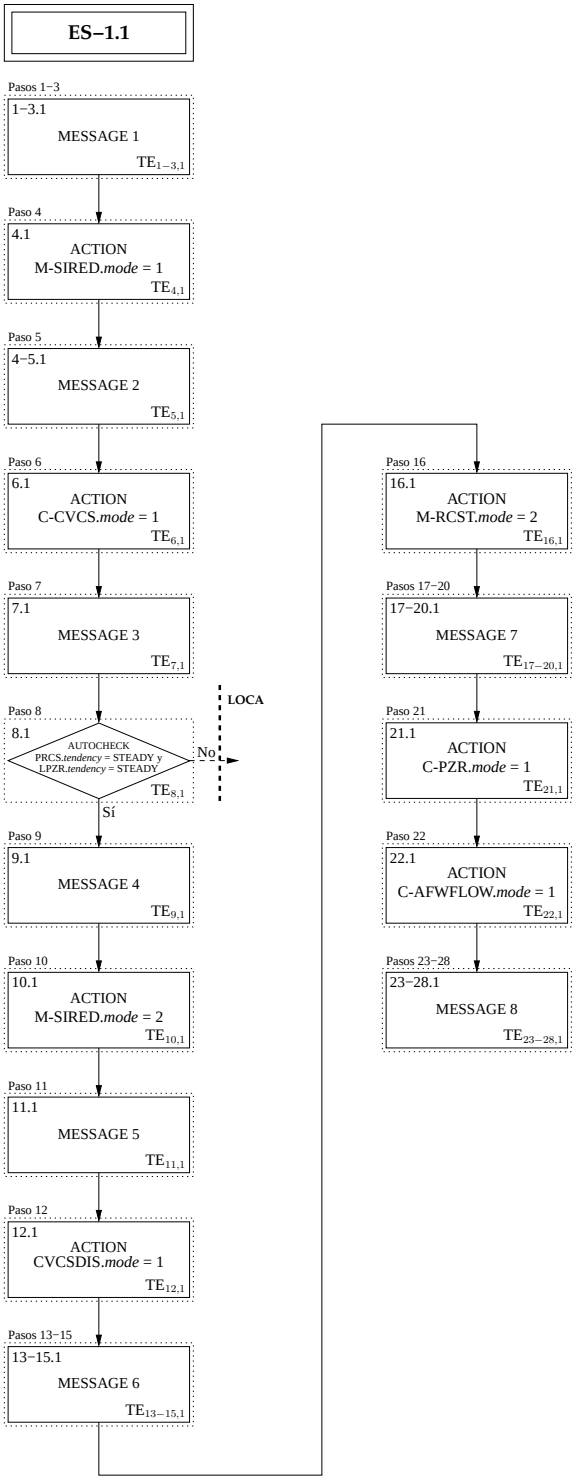


Figura 6.12: Esquema del procedimiento ES-1.1 computerizado (versión reducida).

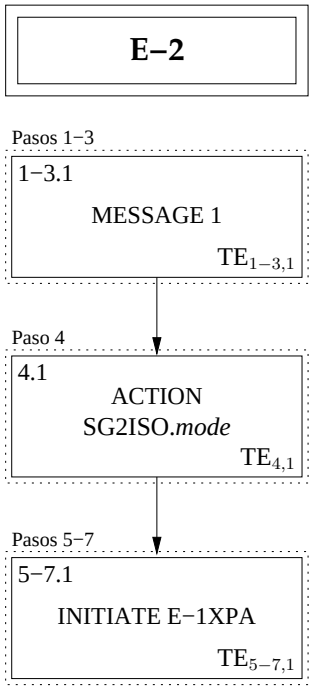


Figura 6.13: Esquema del procedimiento E-2 computerizado (versión reducida).

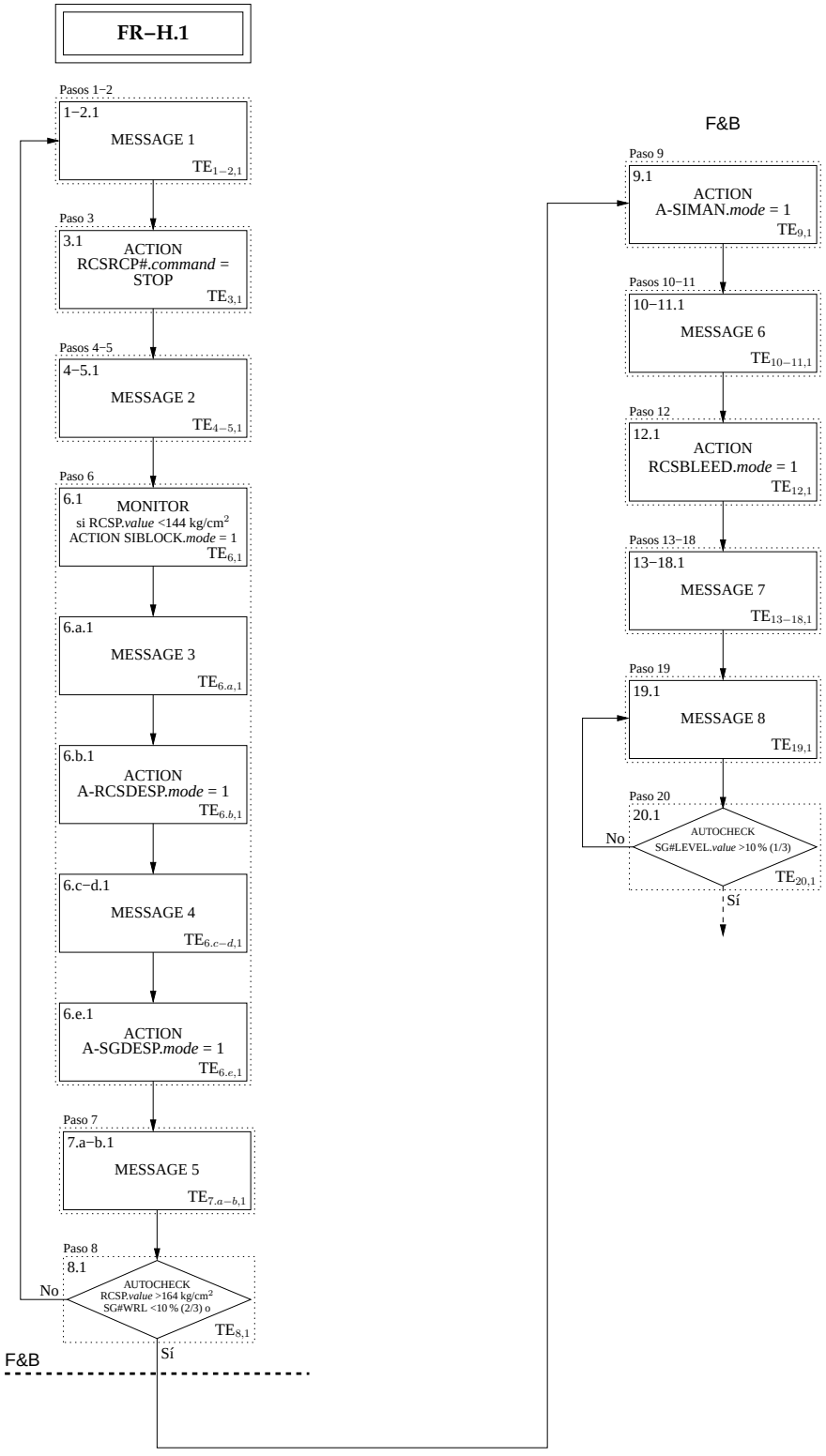


Figura 6.14: Esquema del procedimiento FR-H.1 computerizado (versión reducida).

Subtarea	TE (s)
Entrada	180
1-3.1	80
4.1	30
5-7.1	70
7.2	30
8-16.1	355
17.1	50
18-19.1	40
20.1	20
21-22.1	50
23.1	40

Tabla 6.5: Tiempos asignados a las subtareas del EOP E-0.

Subtarea	TE (s)
Entrada	20
1-5.1	40

Tabla 6.6: Tiempos asignados a las subtareas del EOP ES-0.1.

Subtarea	TE (s)
Entrada	60
1-3.1	60
4.1	30
5.1	30
6.1	50
7.1	30
8.1	30
9.1	10
10.1	20
11.1	20
12.1	30
13-15.1	60
16.1	30
17-20.1	100
21.1	30
22.1	20
23-28.1	200

Tabla 6.7: Tiempos asignados a las subtareas del EOP ES-1.1.

Subtarea	TE (s)
Entrada	10
1-3.1	20
4.1	10
5-7.1	20

Tabla 6.8: Tiempos asignados a las subtareas del EOP E-2.

Subtarea	TE (s)
Entrada	60
1-2.1	120
3.1	75
4-5.1	30
6.1	10
6.a.1	20
6.b.1	30
6.c-d.1	20
6.e.1	30
7.a-b.1	50
8.1	60
9.1	95
10-11.1	30
12.1	30
13-18.1	300
19.1	30
20.1	30

Tabla 6.9: Tiempos asignados a las subtareas del EOP FR-H.1.

6.1.2 Configuración del modelo de planta y del código TRETA

Para poder gestionar las actuaciones manuales demandadas consideradas en el modelo de EOP computerizados, se han implementado en el modelo de planta, entre otros elementos, las interfases necesarias para gestionarlas, Tabla 6.11. El objetivo principal de las interfases implementadas es modelar las actuaciones manuales puntuales y de control, o continuas, sobre los componentes o sistemas incluidos en el modelo. En este sentido, las especificaciones de estas interfases son:

- C-AFWFLOW: controlar el caudal del AFW, garantizando la función del sumidero de calor y controlando el nivel de los SG entre el 20 y el 50 %. Este control es competitivo con el control de temperatura del RCS, M-RCST, y la gestión del caudal del AFWS debe hacerse considerando la posibilidad de su anulación por enfriamiento excesivo del primario.

- M-RCST: controlar la temperatura del RCS empleando como referencia el valor de cero carga en caliente.

- M-SIRED: reducir el caudal de SI, e incluso anularlo, cuando las condiciones consideradas en los EOP lo requieran.

- A-CHDCHMAN: restitución de la carga y descarga del CVCS, tras su anulación automática por señal de SI.

- C-PZR: controlar la presión empleando los calentadores, la ducha y las PORV, y el nivel del presionador mediante el ajuste de la carga del CVCS, de forma que se ajusten a los valores de consigna o deseados.

- A-SG2ISO: aislamiento del generador de vapor afectado por la rotura.

- A-RCPSTOP: parar las RCP para permitir un mejor aprovechamiento del inventario de los SG en secuencias de pérdida de sumidero de calor.

- A-RCSBLOW: bajar la presión del RCS por debajo de 140 kg/cm^2, para preparar las condiciones óptimas para iniciar el aporte al RCS.

- A-SGBLOW: bajar la presión del secundario por debajo de 28 kg/cm^2 para posibilitar el aporte de agua de alimentación a los SG mediante las bombas de condensado.

- A-RCSFEED: iniciar el aporte al RCS mediante las dos bombas de carga de alta del CVCS.

- A-RCSBLEED: iniciar la purga del RCS mediante la apertura total de las dos PORV del presionador.

En general, los controles implementados se corresponden con las actuaciones del operador relacionadas con la estabilización de la planta, Tabla 6.10; control de temperatura del RCS, de las SRV, y de la presión y el nivel del presionador. El control del AFWS se corresponde con la necesidad de mantener dentro del rango estrecho el nivel de los SG, y conjuntamente con el control de las SRV, se encuentra supeditado a la demanda del control de la temperatura del RCS, tal como ya se ha comentado previamente. Las actuaciones que simplemente implican una acción sobre un componente o sistema, denominadas **A**, no requieren más que la implementación del bloque de interfase contemplado en la Tabla 6.11. Sin embargo, las acciones tipo **M** o **C**, de vigilancia o control respectivamente, requieren de un control asociado en el modelo de planta:

- C-AFWFLOW: control manual AFWS, Figura 6.15.
- M-RCST: control manual de la temperatura del RCS, Figura 6.16. De este control dependen a su vez el control manual del AFWS y el control de apertura manual del alivio al condensador, Figuras 6.17, y de apertura de las válvulas de alivio de los SG, Figura 6.18
- C-PZR: control manual de la presión y del nivel del presionador, Figuras 6.19 y 6.20.

La implementación de estos controles es de bajo, basándose principalmente en elementos proporcionales, e incluyendo la posibilidad de modelar retrasos de actuación, efectos integrales, pesados de señales de entrada y la modificación, tanto dinámica por el modelo de procedimientos como por modelo del control en el fichero del modelo de planta, del rango del control de la magnitud física asociada.

Variable controlada	**Rango**	**Objetivo**	**Componentes actuados***
SG#LNR	±SG#LNR	Mantener el nivel de rango estrecho del SG	HV-1672/3/4 (TDP) HV-1675/6/7 (MDP)
AFWF	[86 m^3/h, 408.825 m^3/h]	Recuperar el nivel de rango estrecho de los SG	HV-1672/3/4 (TDP) HV-1675/6/7 (MDP)
RCSCLTAVG	[291 °C,292 °C]	Control manual de la temperatura del RCS con RCP paradas	HV-450(0-7) (CD) PCV-4794/5/6 (AT)
RCSAVGT	[291 °C,292 °C]	Control manual de la temperatura del RCS con RCP funcionando	HV-450(0-7) (CD) PCV-4794/5/6 (AT)
PZRPR	±PZRPR	Estabilizar la presión del RCS	PCV-444B/C
SG#LNR	[30 %,50 %]	Mantener el nivel de rango estrecho del SG	HV-1672/3/4 (TDP) HV-1675/6/7 (MDP)

*Referencia de componente de planta

Tabla 6.10: Controles manuales implementados en los EOP computerizados.

Acción del operador	Referencia	Bloques asociados
Comprobación de caudal de AFW	C-AFWFLOW	19999
Comprobación de las temperaturas del RCS	M-RCST (modo 1)	20160 y 20100/20105
Comprobación de necesidad de reducción del caudal de SI o parada de la SI	M-SIRED	2281/2282
Comprobación de los niveles de los SG	C-AFWFLOW	19999
Comprobación de las temperaturas de ramas calientes del RCS	M-RCST (modo 2)	20160 y 20100/20105
Restitución de la carga y descarga del CVCS	A-CHDCHMAN	7750
Control de presión y nivel del presionador	C-PZR	20300 y 7698
Aislar generador de vapor defectuoso	A-SG2ISO	20025
Parar todas las Bombas del Refrigerante del Reactor	A-RCPSTOP	3692 y 4692
Bajar la presión del primario por debajo de 140 kg/cm^2	A-RCSBLOW	7105
Bajar la presión del secundario por debajo de 28 kg/cm^2	A-SGBLOW	485
Operación de aporte del F&B	A-RCSFEED	9001
Operación de purga del F&B	A-RCSBLEED	7105

Tabla 6.11: Actuaciones manuales implementadas en el modelo de planta relacionadas con el casos de aplicación.

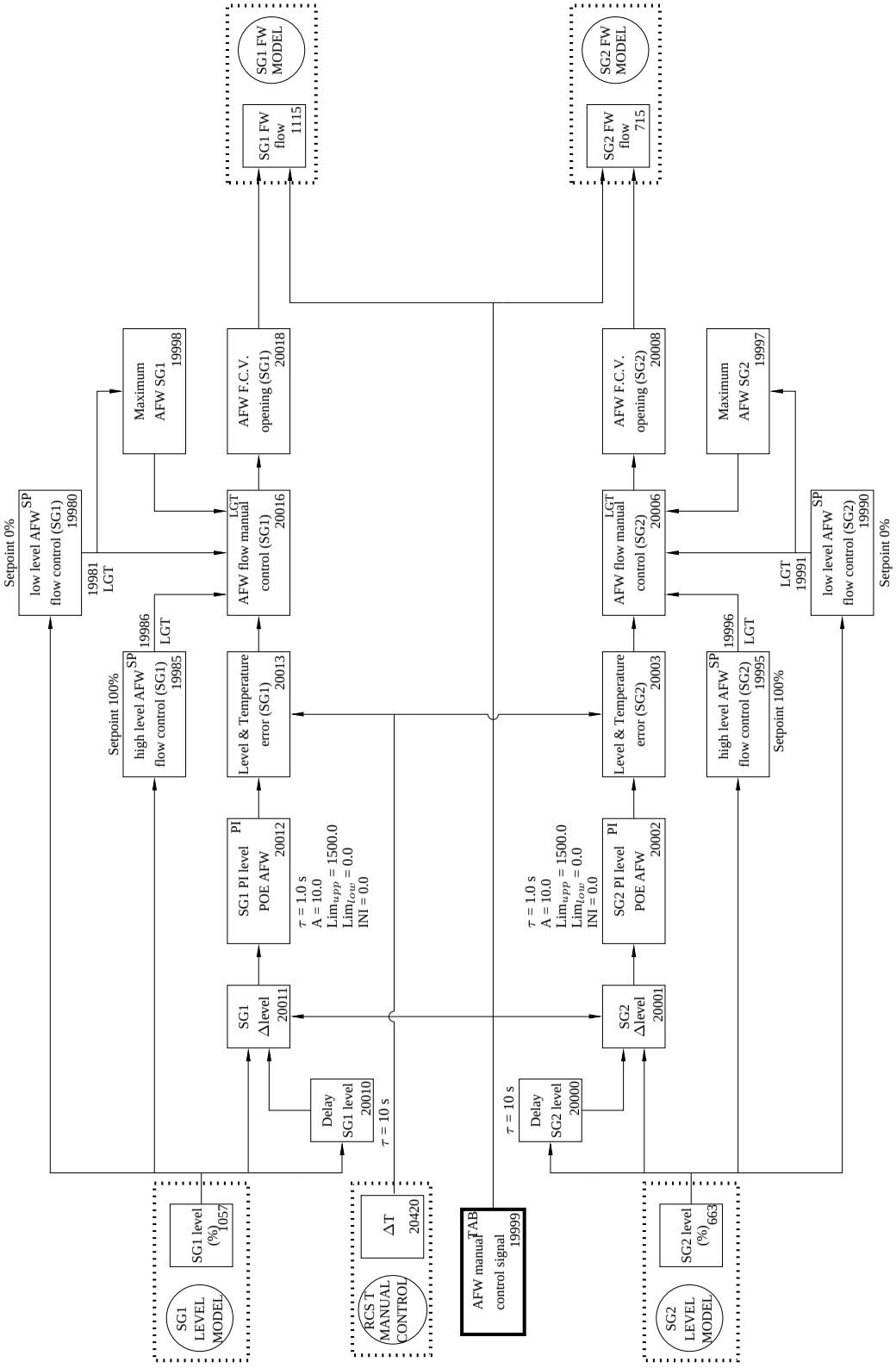


Figura 6.15: Modelo del control manual del caudal del AFW.

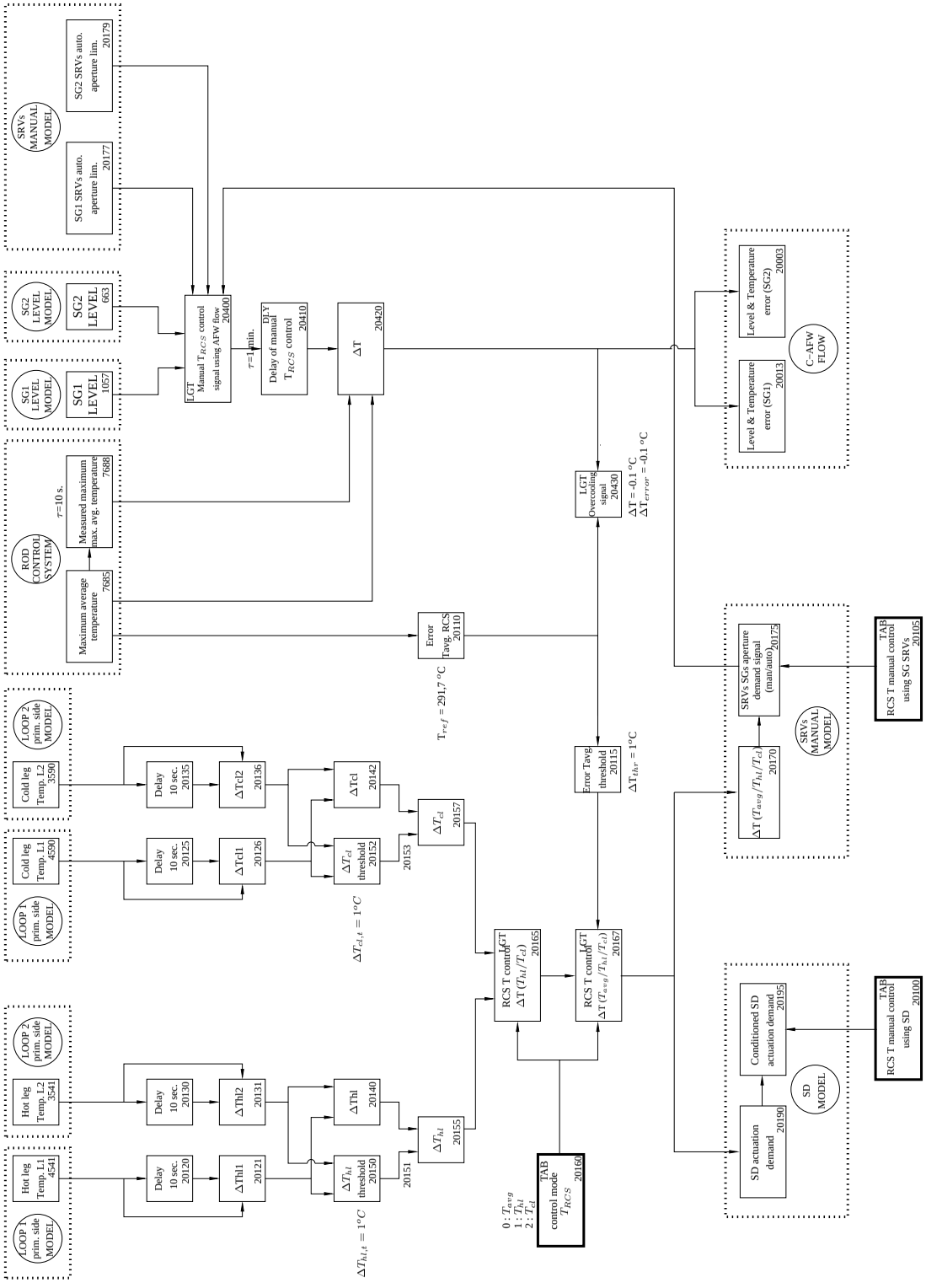


Figura 6.16: Modelo del control manual de la temperatura del RCS.

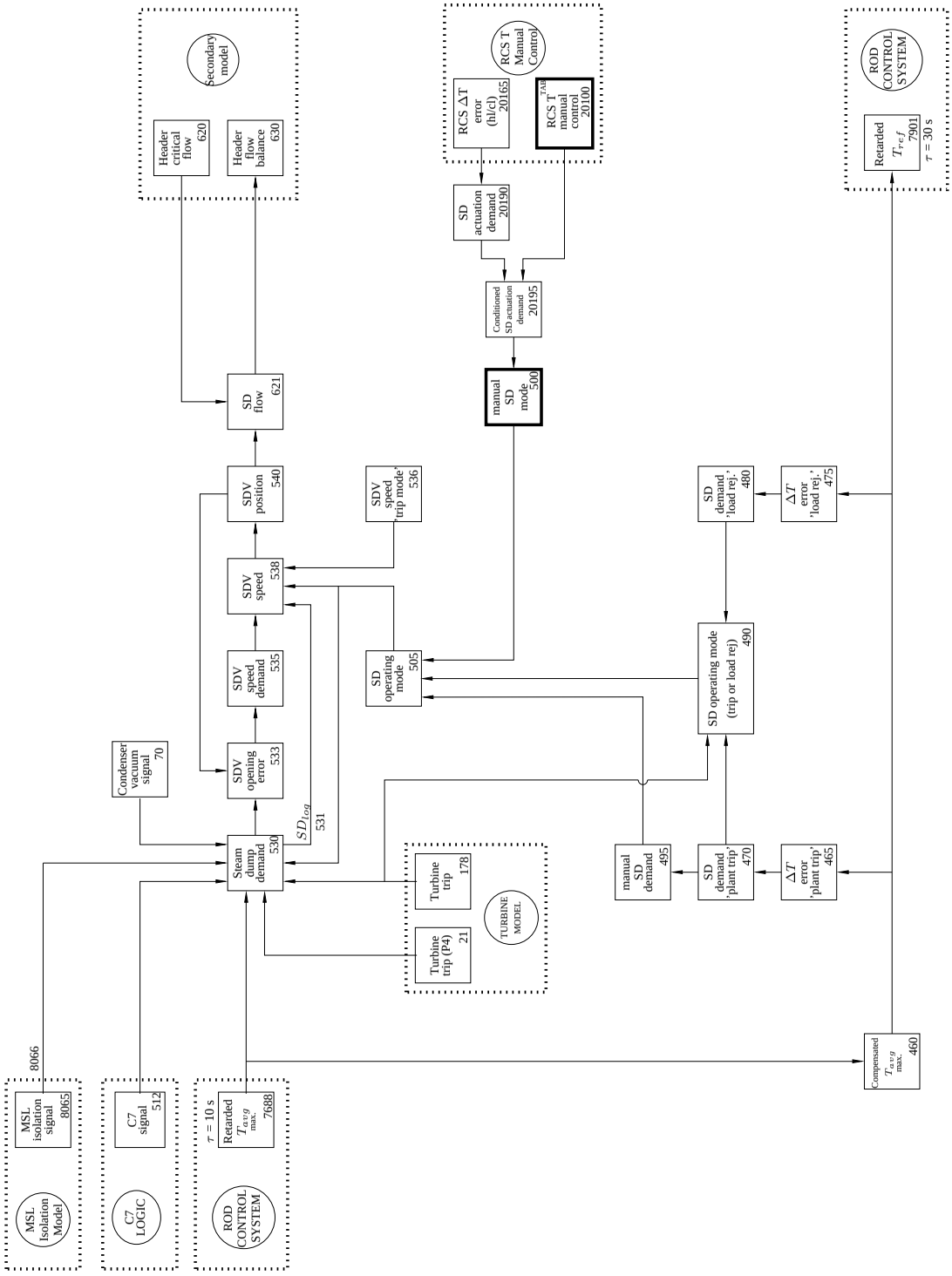


Figura 6.17: Modelo de control manual del alivio de vapor al condensador.

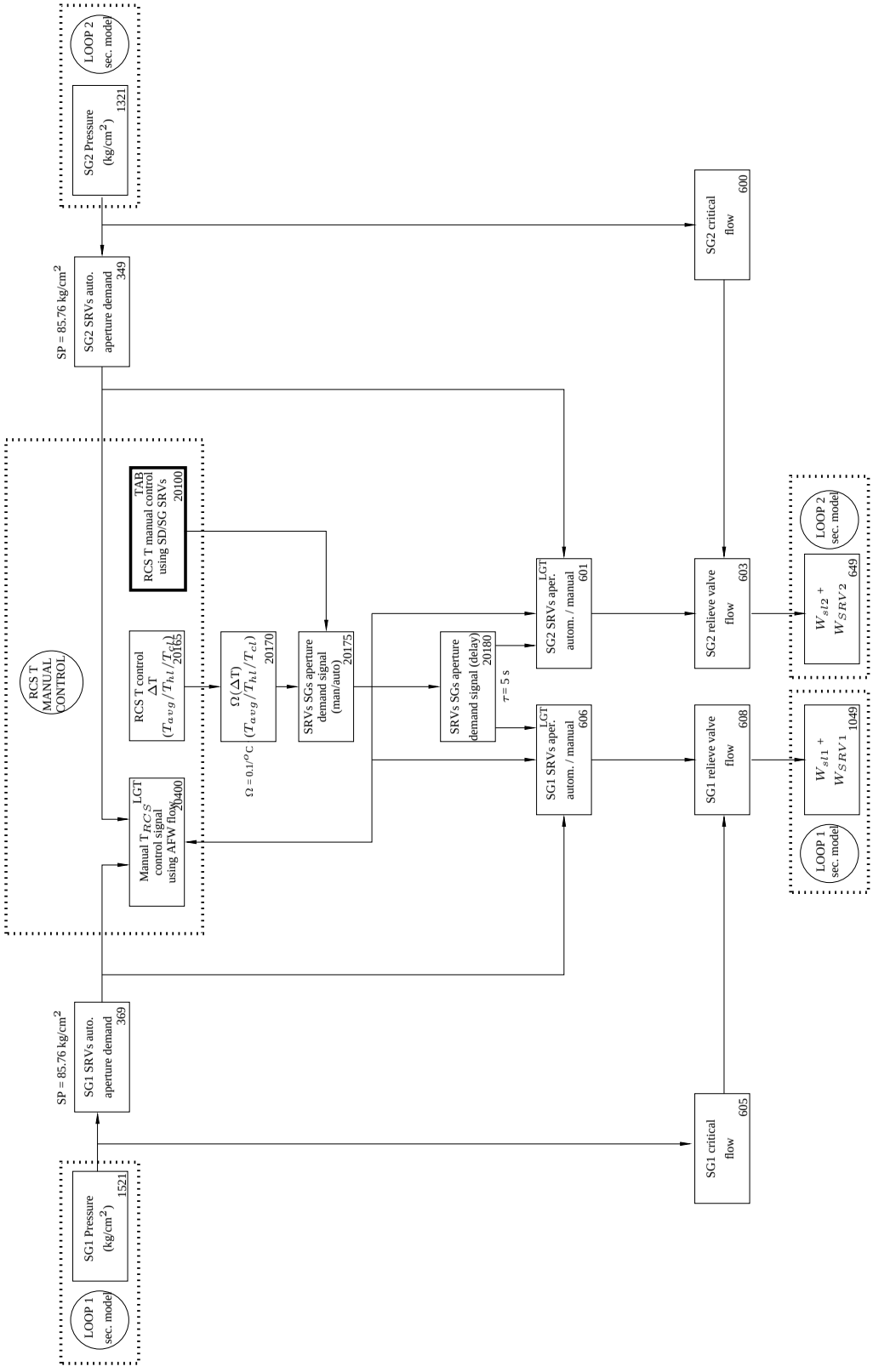


Figura 6.18: Modelo del control manual y automático de las SRV.

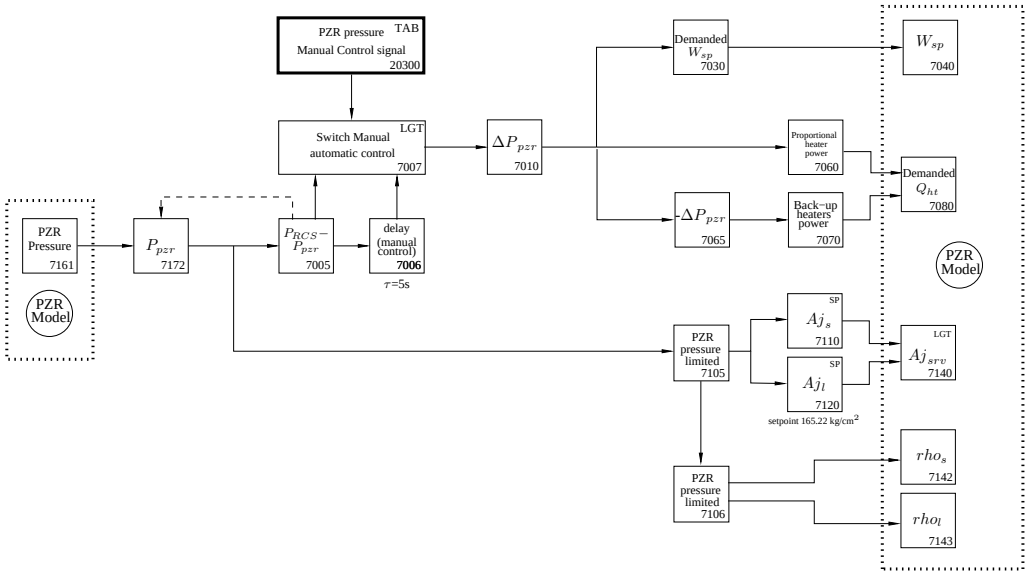


Figura 6.19: Modelo del control manual de presión presionador.

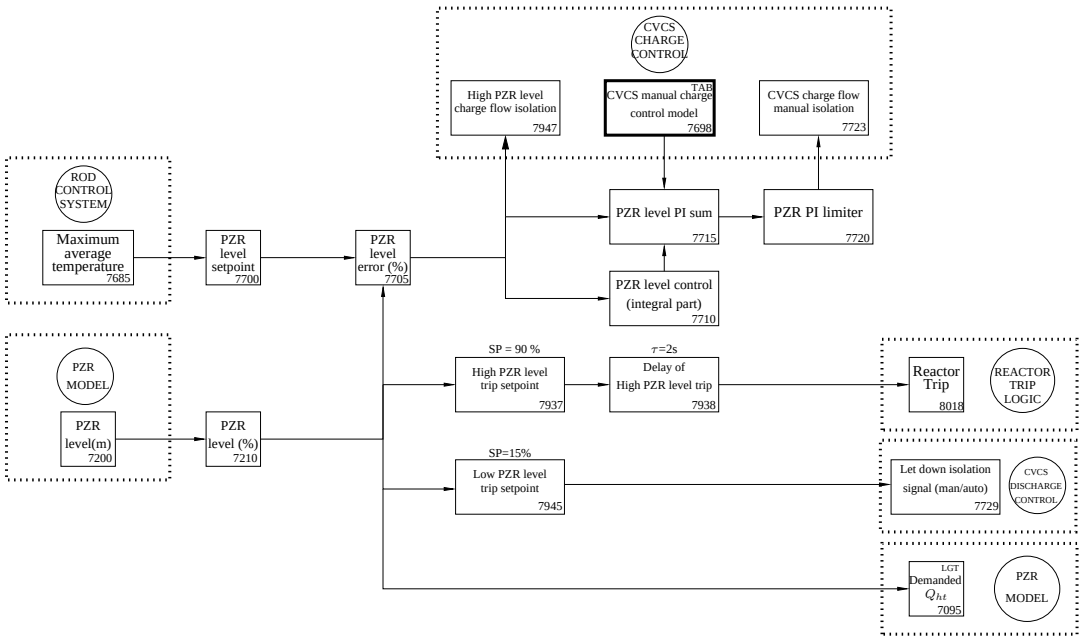


Figura 6.20: Modelo del control de nivel del presionador.

6.2 Roturas aislable y no aislable en el secundario

Los dos primeros casos que se utilizaron para la aplicación de la herramienta consistieron en las roturas aislable en el colector y no aislable en una línea de vapor del generador de vapor del lazo dos (*Steam Line Break*, SLB), sin postular fallos asociados a ningún sistema o componente, Figura 6.21. Estas secuencias, especialmente el caso no aislable, son similares a la evaluada en la base de los EOP, WOG (1997). En ambos casos se considera una rotura de 0,046 m^2 (aprox. 1/3 del área de un restrictor de un SG, $0{,}13\,m^2$), correspondiéndose con una rotura grande de acuerdo con la clasificación de roturas de los PSA y la base de los EOP. Para el caso aislable, la rotura está localizada en el colector de las líneas de vapor, mientras que la rotura no aislable en la línea de vapor asociada al lazo de refrigeración dos está localizada entre la salida de la línea de la contención y su válvula de aislamiento[2], Figura 6.22.

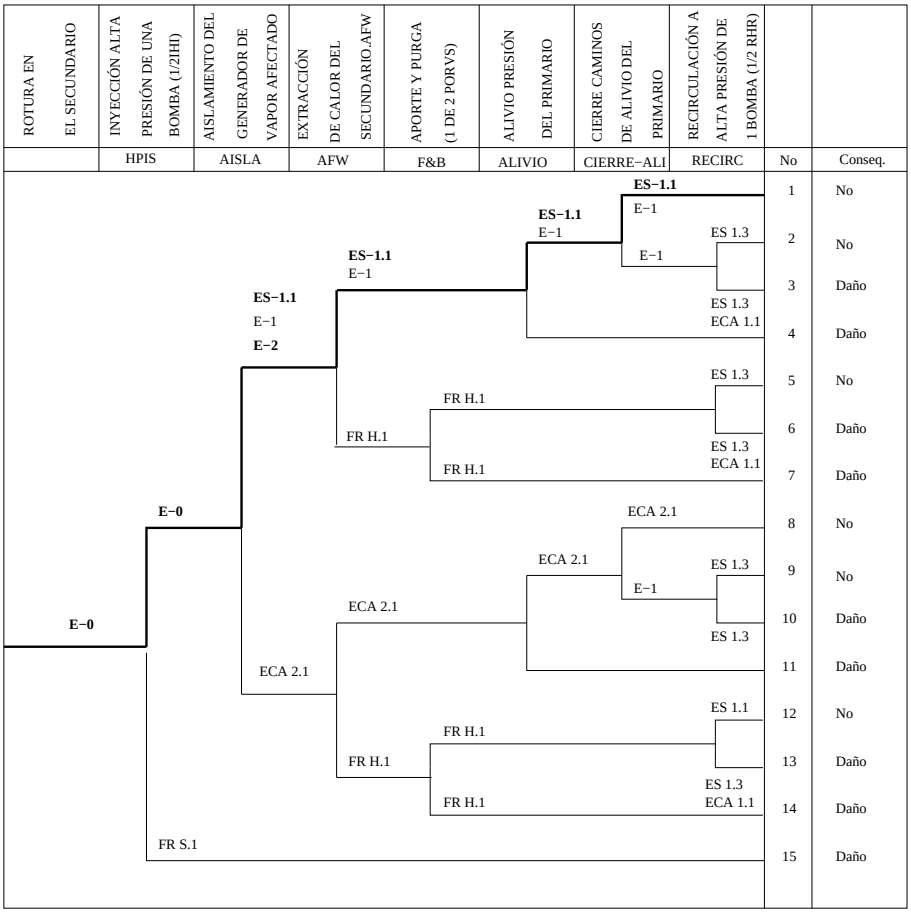


Figura 6.21: Árbol de sucesos de las secuencias de rotura del secundario escogidas.

[2]Aunque pueda parecer que la verosimilitud de este tipo de roturas pueda ser reducida, en realidad son secuencias cuyo riesgo asociado es relevante, considerándose en la realización del PSA de las plantas, tal como es el caso de las CN de Ascó y Vandellós.

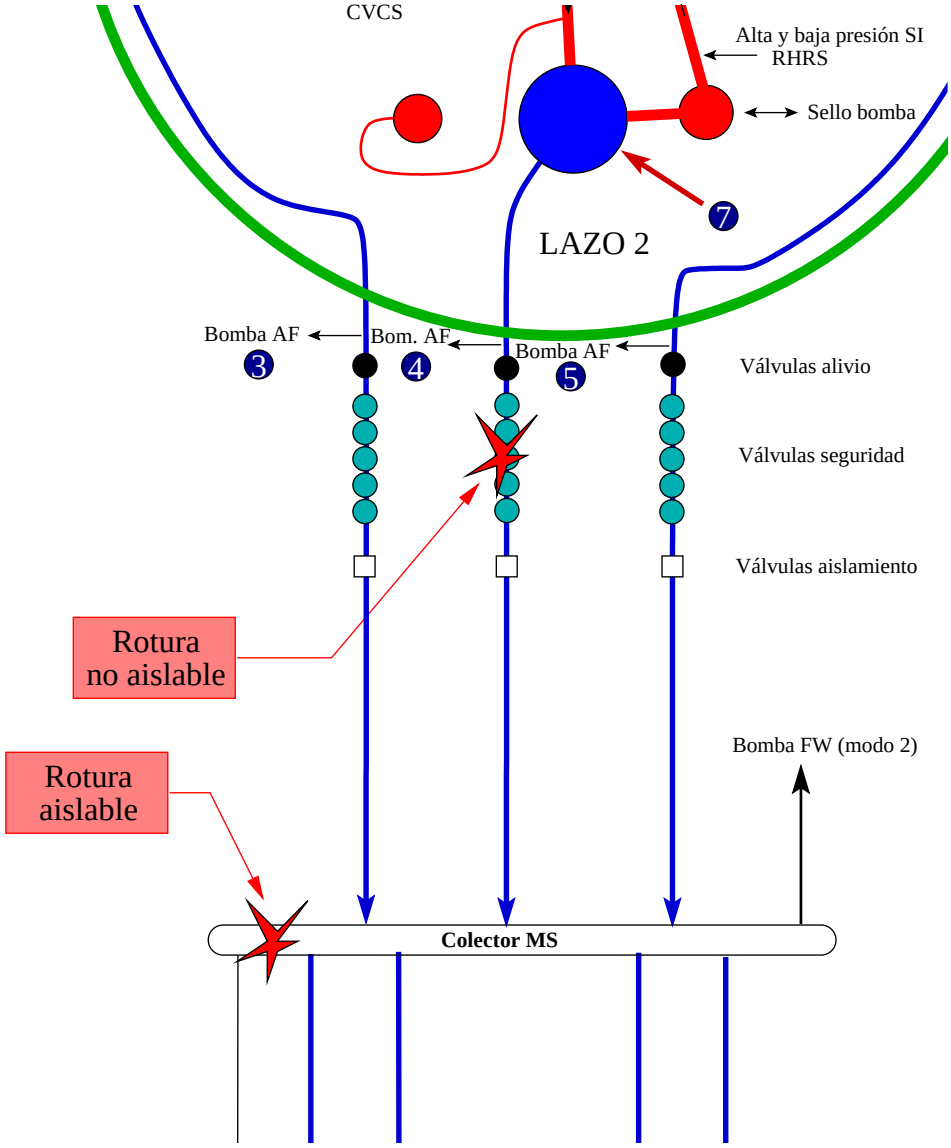


Figura 6.22: Localización de las roturas para las secuencias de SLB.

6.2.1 Actuaciones del operador contempladas en los procedimientos para las secuencias de SLB

Como transitorio de referencia para validar los resultados obtenidos, se empleará la simulación que se considera en la base de diseño de los EOP, WOG (1997). En este transitorio, se simula una rotura de 0.056 m^2 (0.6 ft^2) con la potencia inicial del 100 % para una central típica de tres lazos. La secuencia temporal de los sucesos relevantes se muestra en la Tabla 6.12 y Figuras 6.1 a 6.7.

Cuando se produce la rotura en la línea de vapor, se observa una disminución de la presión en el lazo o lazos del secundario según sea la rotura aguas arriba o aguas abajo del colector de las líneas de vapor, Figura 6.1. Esta categoría de rotura implica que la actuación de los sistemas de control no pueden compensar la despresurización, por lo que se observará una disminución del nivel de los generadores de vapor afectados, Figura 6.2, y un descenso de la temperatura media del primario, Figuras 6.3 y 6.4. Al diferir la temperatura media del primario de su valor programado, se iniciaría la extracción de barras de control para recuperar el valor programado, Tecnatom (1986) y WOG (1997).

La disminución de presión y temperatura media en el primario, Figuras 6.5 y 6.6, continua hasta que se producen las señales automáticas de scram por $OP\Delta T$, a los 23 segundos del transitorio, y del SIS por baja presión en el PZR o baja presión en una de las líneas de vapor, Figura 6.7, ésta última es la que provoca la actuación de la SI en la secuencia simulada a los 55 s. El disparo del reactor provoca el disparo de la turbina, también se produce aislamiento del FWS por baja temperatura media del primario y/o señal S1 con permisivo P4, el aislamiento de las líneas de vapor por baja presión en la línea de vapor, a los 56 s, Figura 6.1, y el inicio de la actuación del sistema de alimentación de agua auxiliar por señal S y/o disparo de las bombas del FWS.

A partir de este punto, finaliza la parte de actuaciones correspondientes al control automático, sistema de protección del reactor y salvaguardias tecnológicas, para dar paso a la parte correspondiente a las actuaciones manuales que se describe en detalle en el apartado siguiente.

Si la rotura estuviese localizada aguas arriba de las MSIV, el SG afectado se despresurizaría

Tiempo	Suceso
23 s	Disparo por $OP\Delta T$
55 s	Iniciación de SI por baja presión del PZR
56 s	Señal de aislamiento de líneas de vapor por baja presión de línea de vapor
5 min	PZR vacío
10 min	AFW finalizada por actuación manual
14 min	SI finalizada por actuación manual
15 min	Apertura de las PORV por alta presión en el RCS
39 min	PZR sólido
56 min	Apertura de las válvulas de seguridad de las SL por alta presión

Tabla 6.12: Secuencia temporal de la rotura de tamaño intermedio en una línea de vapor analizada en la base de los EOP.

hasta la presión del recinto de contención, Figura 6.1. Sin embargo, si la rotura se produce aguas abajo, el transitorio quedaría finalizado con la actuación de las señal de aislamiento de las líneas de vapor.

Para determinar el SG afectado, en el caso de rotura aguas arriba del colector de vapor, bastaría con identificar la SL que experimentó el descenso de presión de forma descontrolada o el SG que finaliza el transitorio completamente despresurizado. En el caso de no ser suficiente con estas observaciones se podrían considerar otros síntomas, como el aumento de caudal de la línea del FWS del SG afectado y un descenso de su nivel más o menos acusado según el tamaño de la rotura.

La finalización de la SI y de la actuación del AFWS son parte de las acciones de recuperación del transitorio registradas en los EOP. Por ello, a partir de este punto de la secuencia el transitorio pasará a estar dominado por el efecto que provocan en la planta las actuaciones del operador, que se muestran de forma resumida en la Tabla 6.13.

Las acciones del operador están centradas, principalmente, en el control del caudal del AFW y la finalización de la SI. Para la secuencia ejemplo, Figura 6.1, se puede comprobar como una vez realizado el aislamiento de las SL y la finalización del aporte de caudal de AFW, WOG (1997), se alcanzan las condiciones óptimas de nivel de los SG establecidas en el EOP E-1, paso 3, CNA (2000). Sin embargo, el SG afectado experimenta una disminución acusada de presión, que hará que se quede sin inventario en los diez minutos posteriores, quedando despresurizado a presión de contención.

Los niveles de los SG no afectados siguen subiendo hasta que se establece el control del AFWS, a los diez minutos aproximadamente, Figura 6.2. Debido al enfriamiento provocado por el caudal del AFW, la presión en los lazos intactos baja hasta un valor aproximado de $16{,}5\,kp/cm^2\ (220\,psig)$, Figura 6.1. Cuando el operador finaliza el aporte de AFW, según criterios de nivel de los SG del EOP E-1, la presión del vapor aumenta paulatinamente hasta alcanzar el punto de tarado de las válvulas de seguridad del SG[3], Figura 6.1. Este aumento de la presión se produce por el calentamiento del sistema primario por el calor residual, WOG (1997) y Tecnatom (1986).

Una vez se interrumpe el AFW, el calor residual empieza a provocar la recuperación del nivel del PZR, la temperatura y la presión del RCS nominales, Figuras 6.5, 6.6 y 6.7. Como además sigue en funcionamiento el SIS, se alcanza el tarado de presión de las PORV del PZR, abriéndose a los 15 segundos. A pesar de ello, el PZR se hace sólido a los 40 segundos.

Con un subenfriamiento adecuado, y siempre que los niveles de los SG no afectados estén en el rango estrecho, se producirá un aumento de la presión del RCS y del nivel del PZR, quedando en condición estable dentro de los criterios que posibilitan la disminución del caudal del SIS, pudiéndose finalizar la misma siguiendo la guía ES-1.1, FINALIZACIÓN DE LA SI. A los catorce minutos, se paran las bombas del SIS, se establecen la carga y la descarga normales y se

[3]El estudio de transitorios que se realiza en la base de los EOP se basa en el empleo del código LOFTRAN y el uso de modelos de análisis determinista de seguridad. Debido a ello, las válvulas de alivio de las líneas de vapor no están incluidas en el modelo, suponiéndose falladas.

inicia el alivio de vapor al condensador[4], que se demanda en los pasos 15 y 16 del EOP ES-1.1 de la CNA.

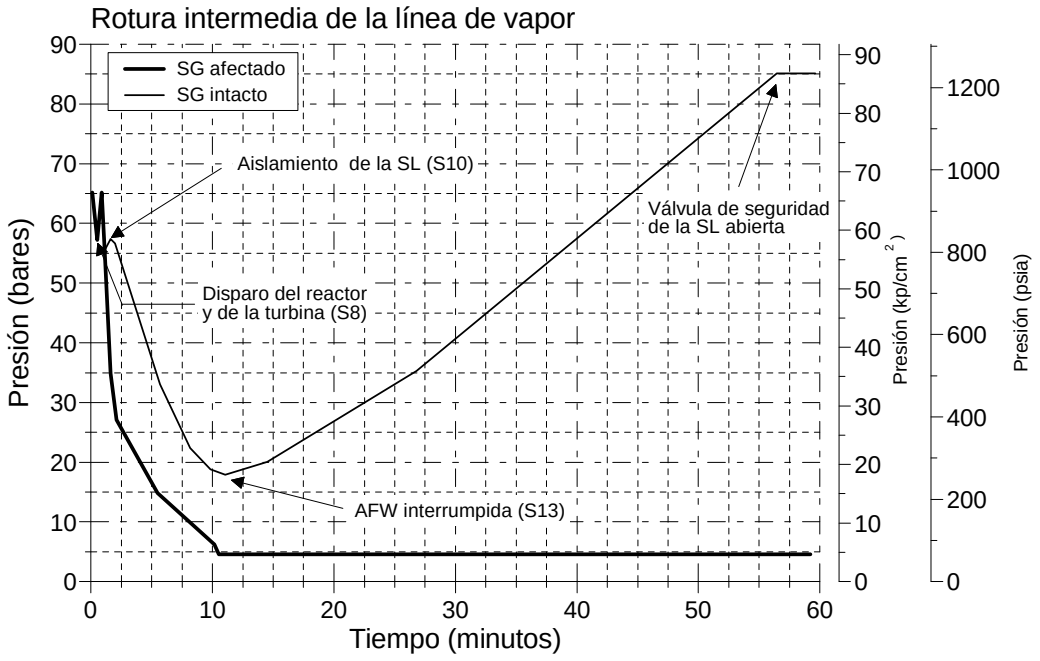
Debido al alto nivel del PZR, es posible que se inicie la guía FR-I.1, RESPUESTA ANTE ALTO NIVEL EN EL PZR, tras la finalización de la actuación del SIS, al presentarse una condición amarilla para el árbol de estado de inventario del primario. Esta guía también establece la carga y descarga y dirige al operador de nuevo al procedimiento ES-1.1. A continuación se realizaría el enfriamiento de la central mediante los procedimientos normales y específicos de cada planta, WOG (1997).

El conjunto de procedimientos requerido para la simulación de estas secuencias de accidente se muestra en la Figura 6.23, donde se incluyen de forma esquemática las actuaciones más relevantes y las transiciones entre los distintos EOP.

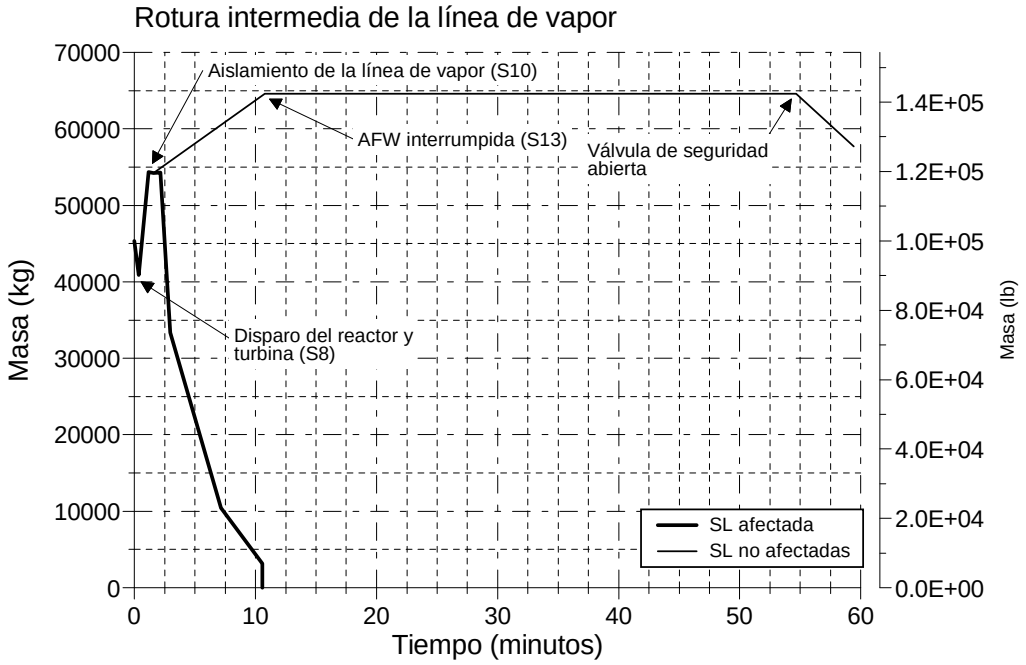
[4]El alivio de vapor al condensador no está considerado en la simulación de la secuencia.

Nº	Descripción del suceso	Acción del operador
S1	Rotura de tamaño intermedio en una línea de vapor.	
S2	Despresurización en la(s) línea(s) afectada(s).	**Inicio del EOP E-0** si se presenta necesidad de actuación de SCRAM o del SIS
S3	Despresurización presión y temperatura media del primario por exceso de refrigeración	**Inicio del EOP E-0** si se presenta necesidad de actuación de SCRAM o del SIS. El control de la temperatura del primario se realiza en el **paso 17 E-0**, una vez asegurado el sumidero de calor (condición de G_{min} del AFWS).
S4	El control de barras inicia la extracción de barras, en un intento de corregir la desviación de la temperatura media respecto al valor programado.	El control de la temperatura del primario se realiza en el **paso 17 del EOP E-0**, una vez asegurado el sumidero de calor (condición de G_{min} del AFWS).
S5	Aumento del caudal de vapor en lazo(s) afectado(s).	
S6	Aumento del caudal del FWS al SG afectado siguiendo el programa de nivel.	
S7	Descenso del nivel en el pozo caliente por exceso de descarga del FWS.	
S8	Disparo del reactor manual por OPΔT o por señal automática de SI por baja presión en una de las líneas de vapor o en el PZR ($\sim$ 1 min.)	Se inicia la ejecución del **EOP E-0** en el caso de señal automática. Podría haberse dado actuación manual del disparo del reactor por parte del operador al verificarse necesidad de SCRAM. (**Paso 1. E-0**)
S9	Disparo de turbina por señal de disparo de reactor.	1) **E-0, paso 2**: Verificación y, en su defecto, actuación manual del disparo de turbina. 2) **E-0, paso 4**: Se verifica necesidad de SI. Si se requiere, y no ha actuado de forma automática, se actúa manualmente. En el caso de que actuase de forma espúrea, se cede control al **EOP ES-0.1**.
S10	Señales de aislamiento del FWS, aislamiento de líneas de vapor e iniciación del AFWS. ($\sim$ 1 min.)	1) **E-0, pasos 5-14**: Se verifica la correcta actuación en la totalidad de los componentes asociados de las señales y se realizan las actuaciones manuales necesarias. 2) **E-0, paso 15**: Se garantiza eficiencia del sumidero de calor. En caso contrario el transitorio pasa a ser un transitorio de pérdida de sumidero de calor, dando paso al **EOP FR-H.1**. 3) **E-0, paso de acción continua 17**: Se inicia el control de la temperatura del refrigerante del primario.
S11	Si la rotura está localizada aguas arriba de las válvulas de aislamiento de la SL, el SG afectado se despresuriza hasta la presión del RC. Si está localizada aguas abajo de las válvulas de aislamiento, la despresurización del secundario finaliza con el aislamiento.	**E-0, paso 20**: Es necesario verificar el aislamiento del SG defectuoso al no estar presurizado, o de aquellos SG que presenten anomalía en sus parámetros de operación. Se cede el control al **EOP E-2**.
S12	Si la rotura está localizada dentro del recinto de contención se produce un aumento de la presión y la temperatura en su interior.	**E-0, paso de acción continua 12**: Si la presión o la temperatura del recinto de contención exceden los criterios de seguridad, se actúa de forma manual el sistema de rociado de contención.
S13	Control (finalización) del caudal de AFW para mantener el nivel de los SG dentro de rango ($\sim$ 10 min.)	**E-1, paso de acción continua 3**: Se controla el caudal del AFWS para mantener los niveles de los SG dentro de rango. En caso de no ser posible se cede el control al **EOP E-3**.
S14	Finalización de la SI ($\sim$ 14 min.)	**E-1, paso de acción continua 7**: Cuando se cumplen condiciones apropiadas para la finalización de la SI se cede el control al **EOP ES-1.1**, donde se lleva a la planta a parada segura.
S15	Apertura de las PORV del PZR ($\sim$ 15 min.)	**E-1, paso de acción continua 5**: Cuando se produzca la apertura de alguna de las válvulas PORV del PZR, el operador debe verificar que cierren correctamente, una vez la presión haya disminuido por debajo del punto de tarado.

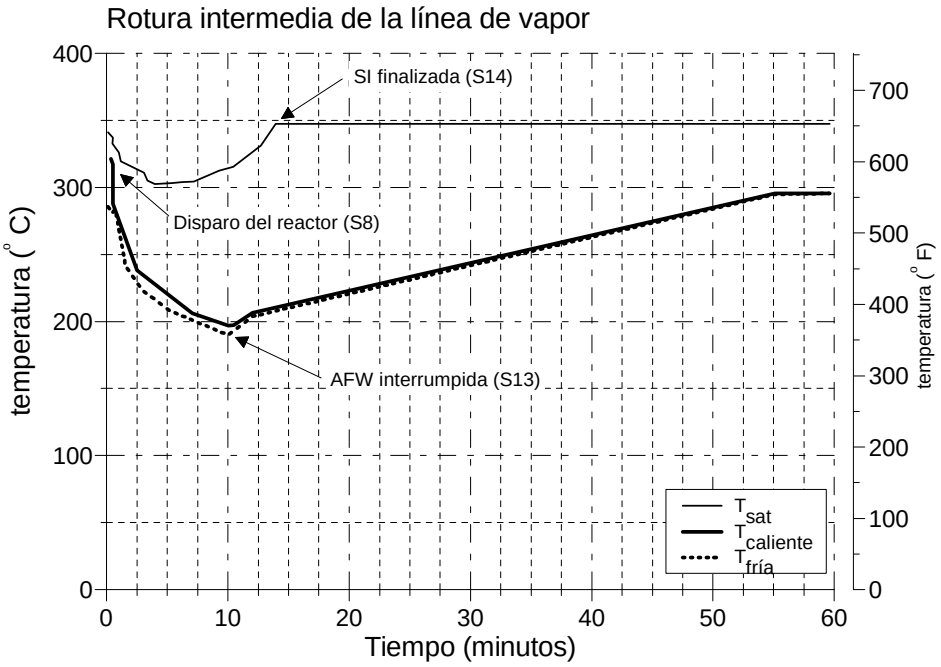
Tabla 6.13: Actuaciones del operador consideradas en la secuencias de SLB en la base de diseño de los EOP.



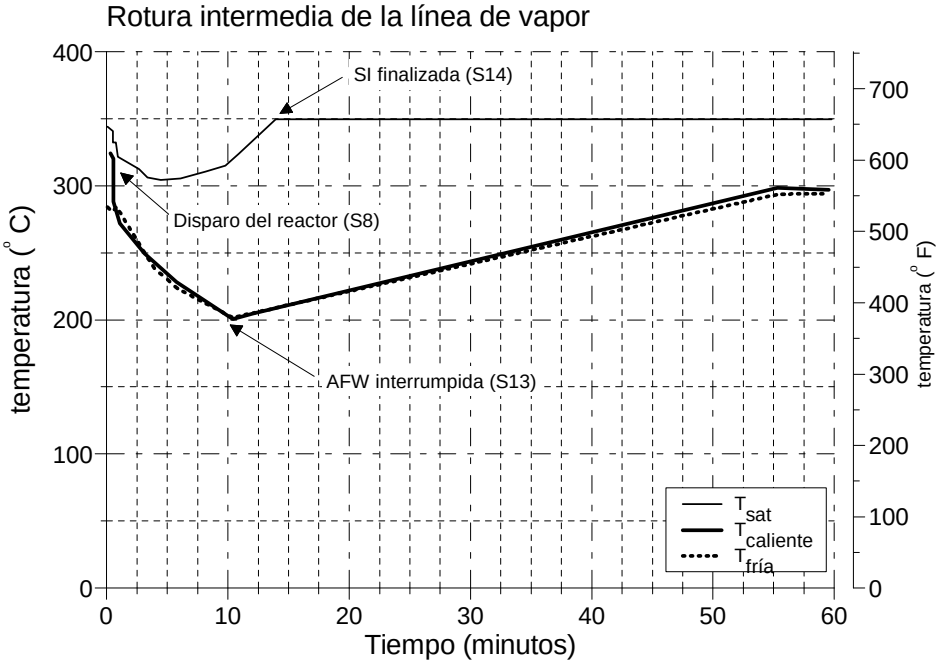
Gráfica 6.1: SLB: rotura intermedia en la SL. Presión en los SG.



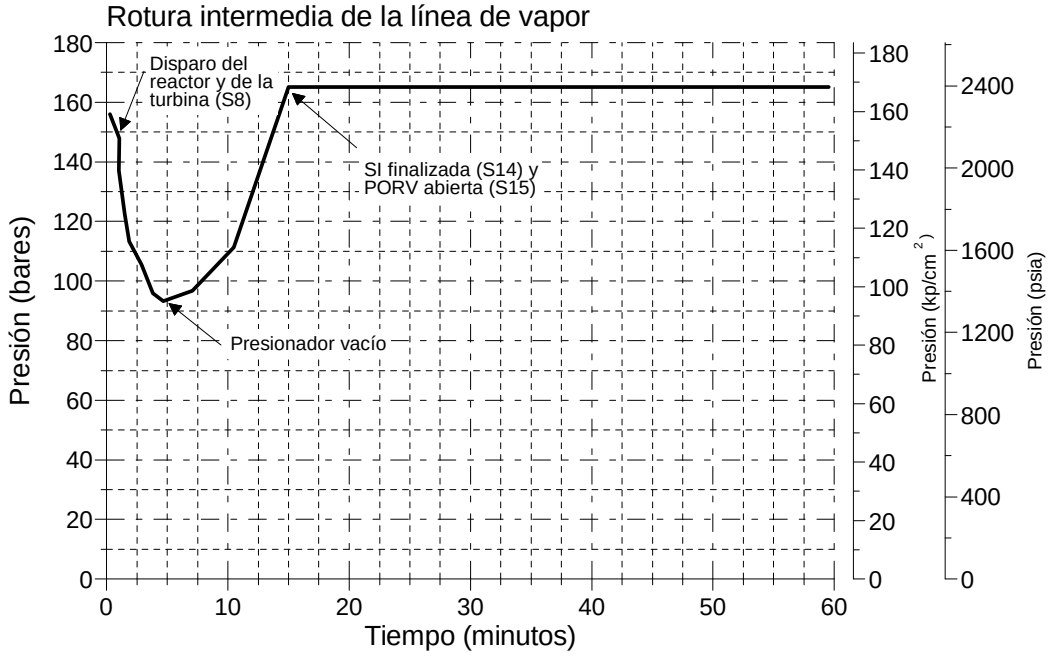
Gráfica 6.2: SLB: rotura intermedia en la SL. Inventariado de masa de los SG.



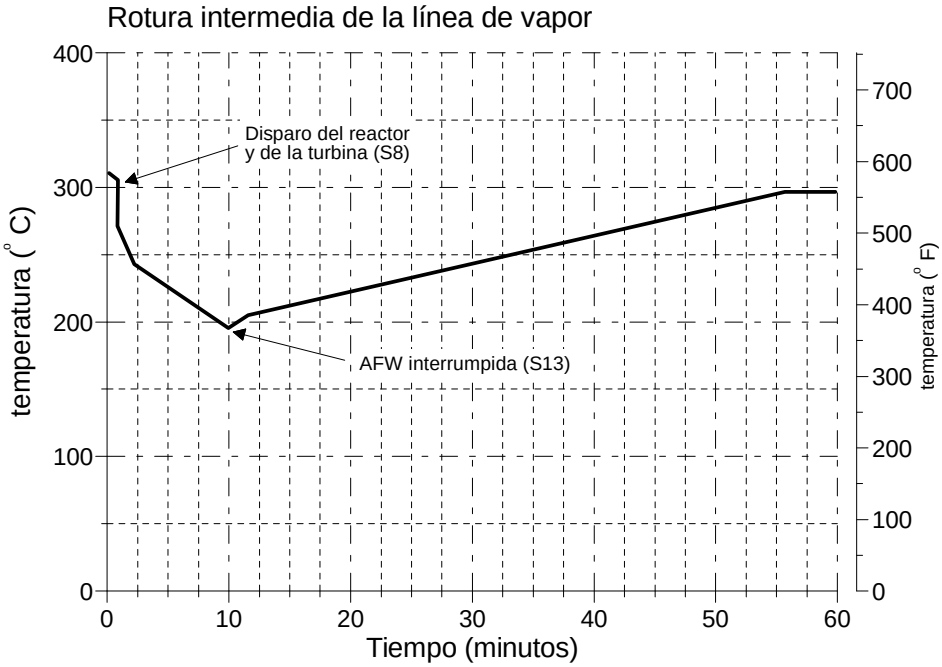
Gráfica 6.3: SLB: rotura intermedia en la SL. Temperatura del lazo afectado.



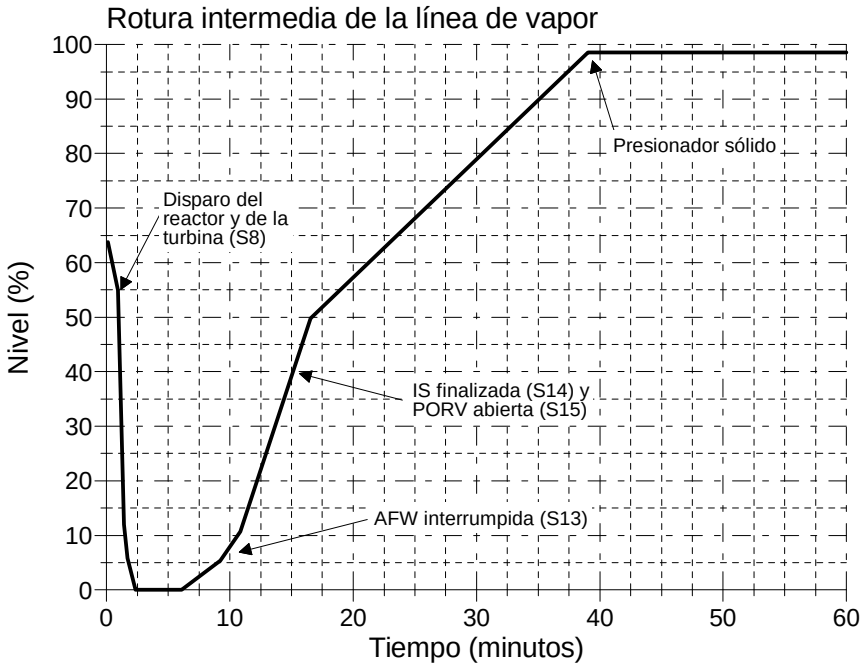
Gráfica 6.4: SLB: rotura intermedia en la SL. Temperatura del lazo no afectado.



Gráfica 6.5: SLB: rotura intermedia en la SL. Presión del RCS.



Gráfica 6.6: SLB: rotura intermedia en la SL. Temperatura media en el núcleo.



Gráfica 6.7: SLB: rotura intermedia en la SL. Nivel del presionador.

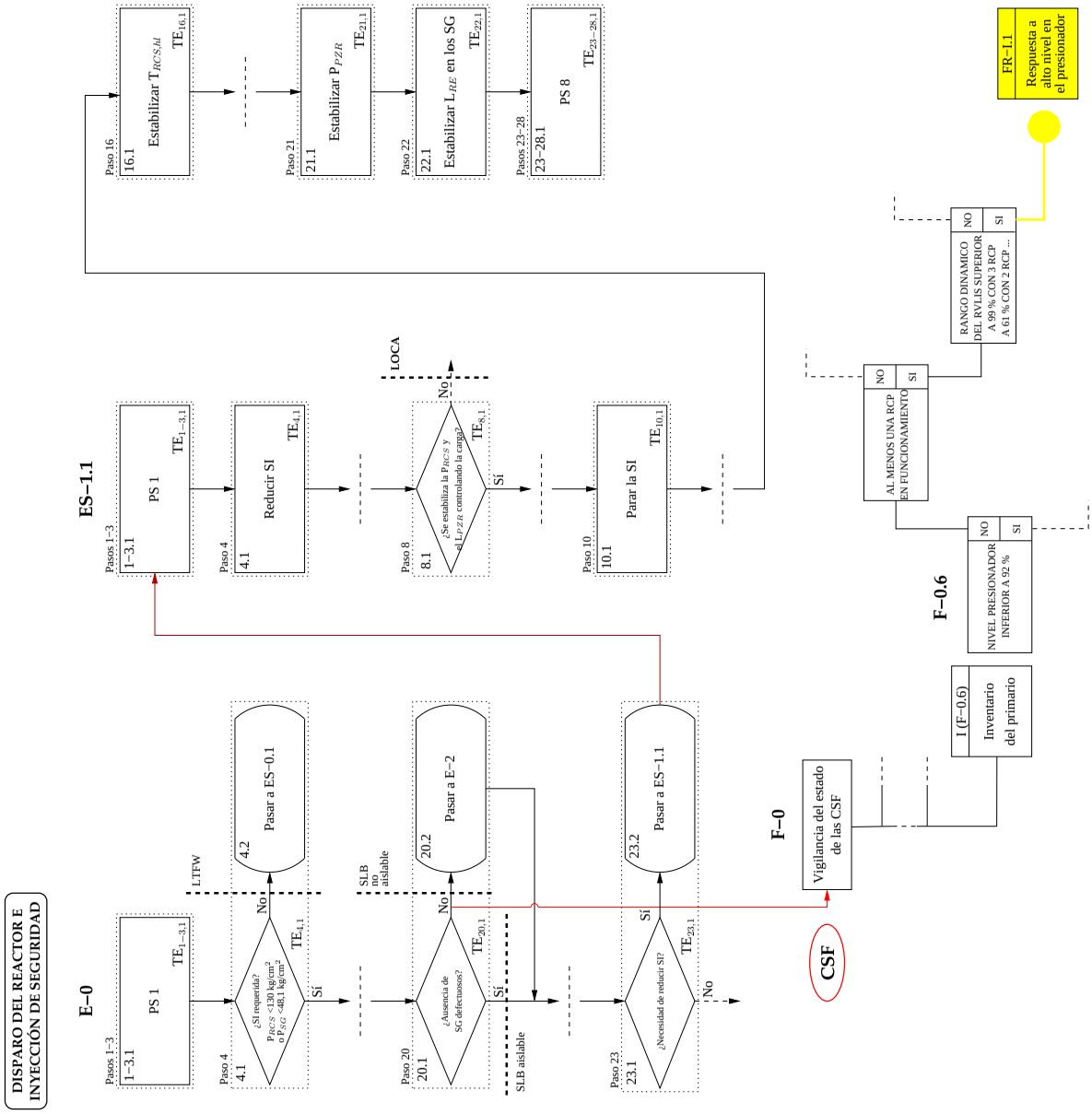


Figura 6.23: Esquema de la secuencia de accidente de SLB con los EOP asociados.

Actuación	Acción del operador	EOP-PASO	Subtarea
1	Comprobar si el caudal de la SI debe ser reducido	E0-23, ES1.1-4	E0-7.2, ES1.1-4.1
2	Comprobación de la temperatura media del RCS	E0-17	E0-17.1
	Comprobar niveles de los SG	E0-25, ES1.1-21	E-0-17.1, ES1.1-21.1
	Comprobar temperaturas de ramas calientes del RCS	ES1.1-16	ES1.1-16.1
3	Controlar nivel del presionador	ES1.1-16	ES1.1-16.1
4	Controlar presión del presionador	ES1.1-21	ES1.1-21.1

Tabla 6.14: Tareas significativas de los EOP considerados en las secuencias de roturas aislable y no aislable.

6.2.2 Resultados obtenidos con la herramienta TRETA/COPMA-III para el caso de SLB aislable

Se supone la rotura grande en el colector de las líneas de vapor, Figura 6.22, con un tamaño de 0,046 m^2, a los 120 s. Durante los primeros 24 s., se produciría la actuación de los sistemas de control para compensar la bajada de presión, por lo que se observa una disminución del nivel de los generadores de vapor afectados y un descenso de la temperatura media del primario, Figuras Figura 6.15 y 6.11, terminando esta primera etapa de inicio del transitorio con el disparo del reactor por alto flujo neutrónico debido al enfriamiento del primario a los 144,9 s., momento en el cual los operadores determinarían la entrada en estado de operación de emergencia. En este caso, la entrada al EOP E-0 de diagnóstico tras disparo de reactor / inyección de seguridad se ha demorado hasta los 300 segundos de simulación, considerado el tiempo de entrada en 155 s., valor comprendido en la orquilla de tiempo medio de inicio para su seguimiento, que puede oscilar entre 130 a 170 segundos, Park et al. (2005).

Mientras que los operadores inician el seguimiento del EOP E-0, se produce la actuación de los sistemas automáticos de seguridad, Tabla 6.15. Por un lado, tiene lugar el disparo de turbina a los 145,2 s., derivando en señal de actuación del AFWS, que inyecta transcurridos los 26 s. de retraso considerados para dicho sistema, relacionados con el arranque de las turbobombas de alimentación, Figura 6.17. La actuación del alivio de vapor al condensador y la pérdida de inventario de vapor por la rotura del colector, Figura 6.16, hacen que tanto la presión de los SG, Figura 6.14, como el inventario de agua de los mismos, Figura 6.16, disminuyan de forma drástica hasta el momento en que se produce el aislamiento de las líneas de vapor, a los 249,3 s. por baja presión en ambos SG. A partir de ese momento, el caudal de inyección del AFWS comienza a recuperar el nivel de los SG, aumentando la presión del secundario al quedar aislada la rotura, Figura 6.14. En lo que respecta al primario, y debido a la señal de baja presión en el presionador, se da señal S a los 179,7 s., inyectando el SIS a los 182,7 s., Figura 6.12. Cabe destacar, que este la inyección de inventario por parte de este sistema no es capaz de recuperar el nivel y la presión del RCS hasta que se produce el aislamiento de las líneas de vapor,a los 257,8 s., momento en el cual se inicia la recuperación de la presión y el nivel en el primario, Figuras 6.8 y 6.9.

Hasta este momento, la fenomenología del transitorio ha estado dominada por la actuación de los controles automáticos. Sin embargo, a los 300 s. se inicia la ejecución del EOP E-0, *Procedimiento de Disparo del reactor y/o Inyección de Seguridad*, por parte del personal de la sala de control. Tras verificar la actuación adecuada del sistema de disparo del reactor y que el núcleo se encuentra subcrítico, pasos 1 a 3 del procedimiento E-0, a los 410 s. se considera necesaria la actuación de la SI por baja presión en el RCS, Figura 6.8, paso 4 del procedimiento. Este tipo de transitorios, debido a la similitud de los síntomas, suele confundirse con los transitorios tipo LOCA. Por ello, y a partir del paso 4, el operador considera dos parámetros clave para su diagnóstico: el subenfrimiento a la salida del núcleo y la recuperación del inventario del primario. Transcurridos 500 s., y considerando la evolución de dichos parámetros, se da por diagnosticado el suceso como un LSLB, Tabla 6.1. Para evitar el llenado excesivo del presionador, suceso que tiene lugar si no se lleva a cabo la parada preventiva de la SI, se supone que los operadores deciden realizar la parada de la SI a los 510 s., diagnóstico que se realizaría si no se implementarse a

priori en el paso 23 del procedimiento, aproximadamente a los 1065 s, dándose una transición al EOP ES-1.1 y finalizándose la SI por cumplimiento de los criterios de reducción y parada de los pasos 4 y 10 del EOP ES-1.1. Además, esta actuación podría darse en cualquier momento del transitorio por condición amarilla del árbol F-0-6 tras subir el nivel del presionador por encima del 92 % en el terminal asociado a la FR-I.1, *Respuesta ante alto nivel en el presionador*, Figura 6.23. La implementación a priori de su realización se corresponde a la intención de simular que pasaría si se adelanta la secuencia de actuaciones de los pasos cuando se dispone de un juicio de situación adecuado, comportamiento habitual de los operadores, Theureau et al. (2000).

Tras la parada de la SI, se inicia el control de la temperatura media del RCS a los 915 s., considerada en el paso 17 del EOP E-0, iniciándose el control implementado en el modelo de TRETA al efecto, Figura 6.16. Cabe constatar, que el control de temperatura del RCS y el de nivel de los SG está interrelacionado por el impacto que tiene en ambos el caudal del AFWS. Debido a que el nivel de los SG se ha recuperado en esos momentos, Figura 6.15, y el enfriamiento del primario es excesivo respecto a la temperatura de referencia de 291.7 ^{o}C, Figura 6.11, el operador anularía el caudal del AFWS, actuación que simula el control del caudal del AFWS cerrando las válvulas de control de caudal, Figura 6.17.

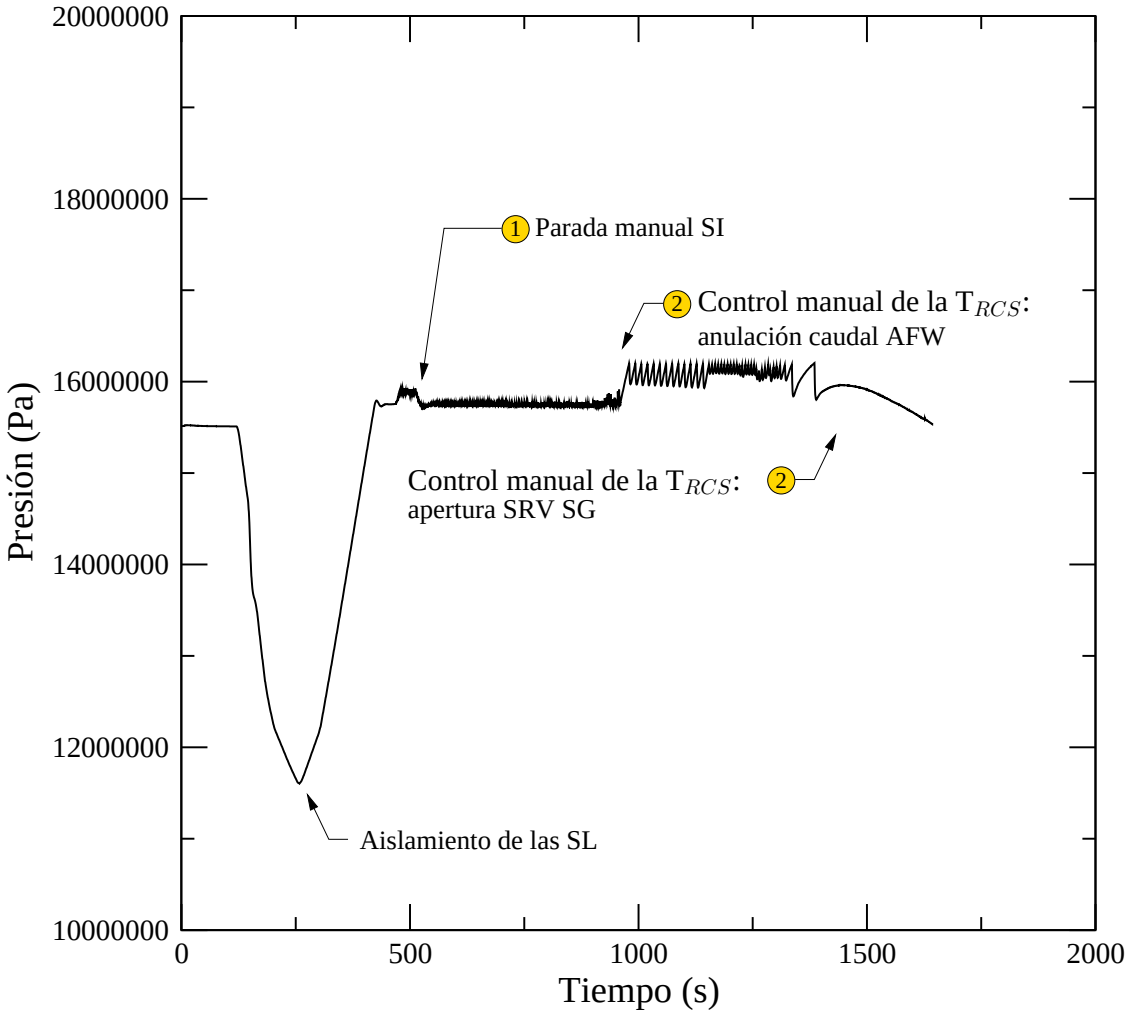
Debido al aislamiento de las líneas de vapor, y al estar localizada la rotura aguas abajo de las válvulas de aislamiento, la presurización del secundario es un hecho desde dicho instante, pudiéndose comprobar en la Figura 6.14, lo que hace que se concluya a los 975 s. que ningún generador de vapor se encuentra afectado por la rotura una vez cerradas las MSIV, dándose a los 1065 s. la transición al EOP ES.1.1, tras constatarse en el paso 23 que la reducción y parada de la SI ha sido una actuación correcta, al mantenerse las condiciones de subenfriamiento a la salida del núcleo, caudal de agua de alimentación o nivel de los SG, presión del RCS y nivel del presionador, Figura 6.9.

Debido a que el diagnóstico se ha verificado, se iniciará en el EOP ES-1.1, *Procedimiento de finalización de Inyección de Seguridad*, las actuaciones relacionadas con la estabilización de la planta en condiciones seguras. En este sentido, inicia el control manual del nivel del presionador en el paso 6 del procedimiento a los 1295 s., restableciendo la carga y la descarga del CVCS e iniciando el control manual de nivel del modelo de TRETA, Figura 6.20. En el tiempo transcurrido desde el inicio del control manual de la temperatura media, a los 915 s., la temperatura del primario ha ido aumentando, superando el valor de referencia, Figura 6.11. Este hecho provoca que se realice la apertura de las SRV de los SG para enfriar el RCS, Figura 6.10, y para compensar la pérdida de inventario de los SG, Figura 6.16, se vuelva a inyectar agua de alimentación a los SG mediante el AFWS, Figura 6.17. A los 1525 s., las operaciones de control de temperatura del RCS comienzan a realizarse tomando como referencia la temperatura en las ramas calientes del RCS, tal como se registra en el paso 16 del procedimiento ES-1.1.

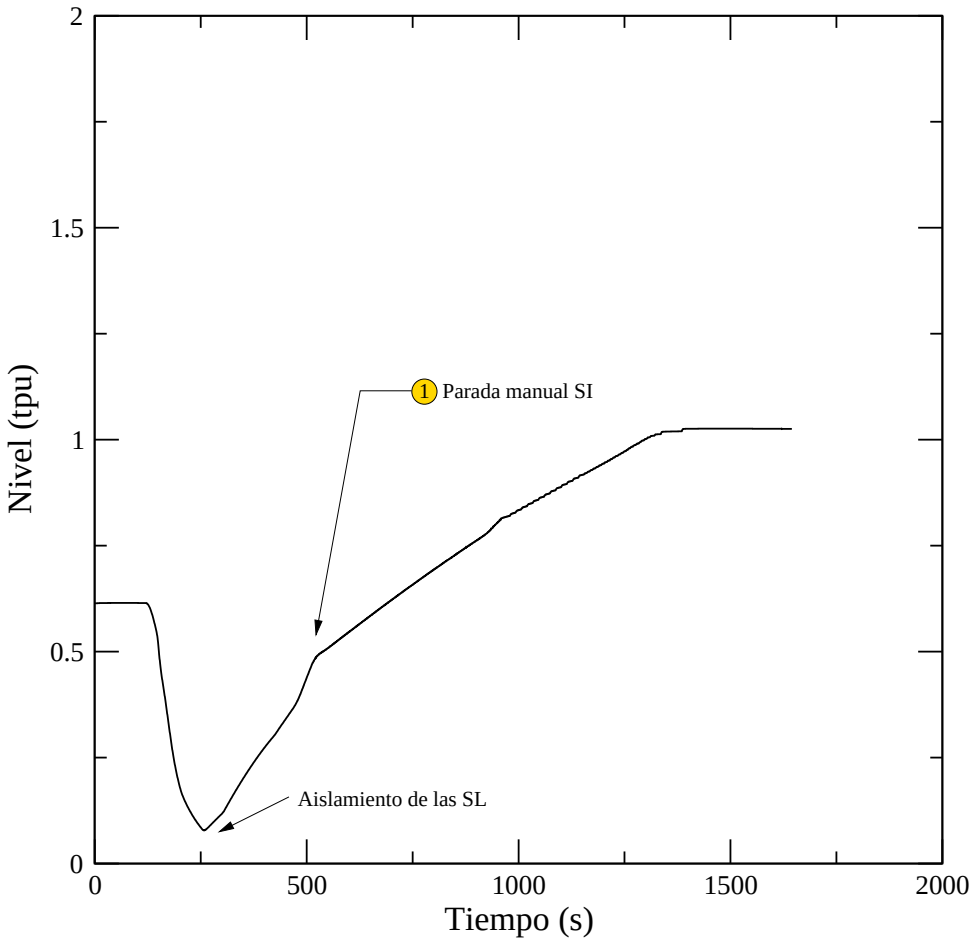
Debido a problemas de cálculo del caudal de la línea de compensación del presionador, cálculo ligado a la distribución de caudales de los lazos de refrigeración, a los 1645,8 s. la simulación finaliza, quedando la simulación de los procedimientos abandonada en los pasos 17 a 20 del ES-1.1, quedándose sin ejecutar el paso 22 relacionado con el control manual de los niveles de los SG, Figura 6.15, que se realizaba de forma indirecta desde el paso 17 del EOP E-0, relacionado con el control de la temperatura del RCS.

ACTUACIONES AUTOMÁTICAS	
Tiempo (s.)	**Descripción**
120	Rotura de 0,046 m^2 en el colector de las líneas de vapor
144,9	Disparo del reactor por alto flujo neutrónico. Apertura del alivio de vapor al condensador
145,2	Disparo de turbina
147,3	Disparo de las bombas del FWS
147,6	Señal de actuación del AFWS (Señal W)
173,6	Inyección del AFWS (26 s. de retraso respecto a la señal W)
179,7	Señal de inyección de seguridad (Señal S). Señal de aislamiento del FWS
182,7	Inyección del SIS (3 s. de retraso respecto a la señal S)
249,3	Señal de aislamiento de las SL
257,8	MSIV cerradas
1296,8	Llenado del presionador
ACTUACIONES MANUALES / GESTIÓN DEL OPERADOR	
Tiempo (s.)	**Descripción**
300	**Entrada en EOP (EOP E-0)**
410	Se considera necesaria la SI debido a baja presión en el RCS. Subtarea 4.1
500	Se supone diagnóstico del suceso como una LSLB
510	Parada de la SI. Subtarea 7.1. Implementada por SA/DM del operador
915	Inicio del control manual de la temperatura media del RCS. Subtarea 17.1
	Finalización de la inyección del AFWS por baja temperatura media del RCS y nivel controlado de los SG. Subtarea 17.1
975	Comprobación del estado de los SG. Subtarea 20.1
1065	**Transferencia al EOP ES-1.1**. Subtarea 23.1
1295	Restablecimiento de la carga y de la descarga para el control del nivel del presionador. Subtarea 6.1
1299,6	Apertura de las SRV de los SG para el control de la temperatura media del RCS. Control derivado de la subtarea 17.1 EOP E-0
1525	Cambio del control de temperatura del RCS a temperatura en ramas calientes. Subtarea 16.1
1645,8	Finalización de la simulación por fallo en el cálculo del caudal de la línea de compensación del presionador

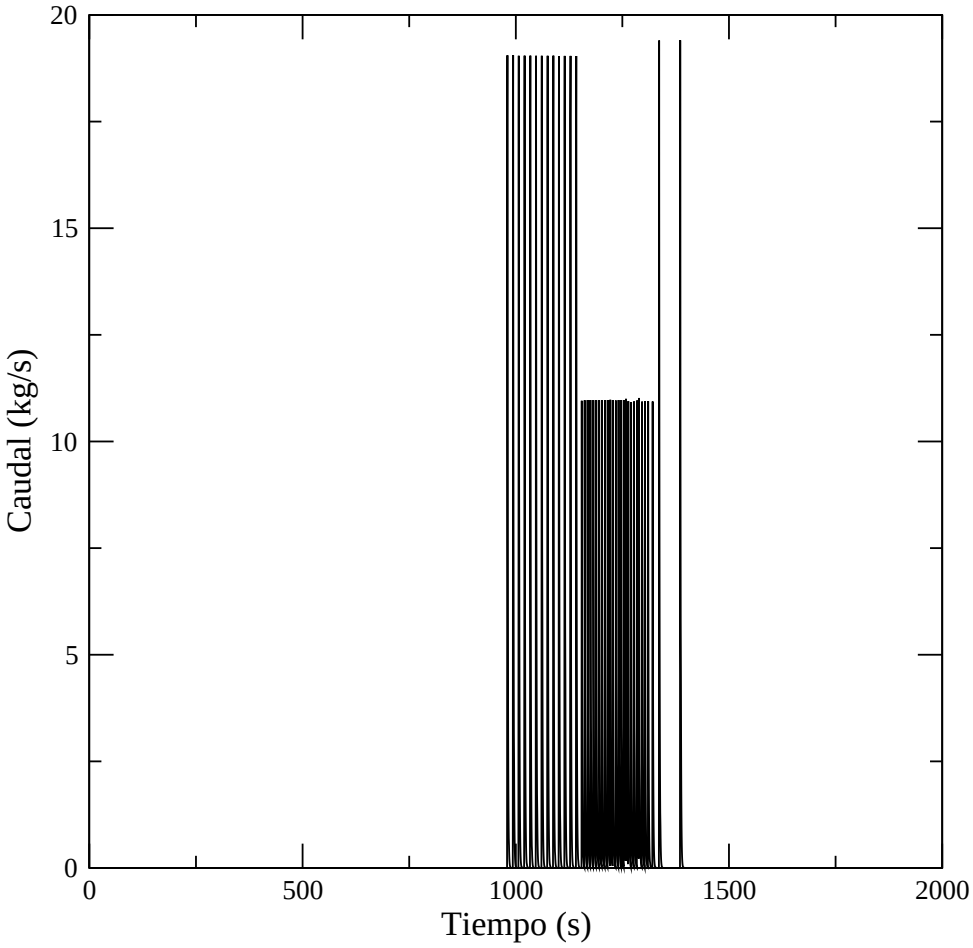
Tabla 6.15: SLB aislable: secuencia de actuaciones automáticas y manuales.



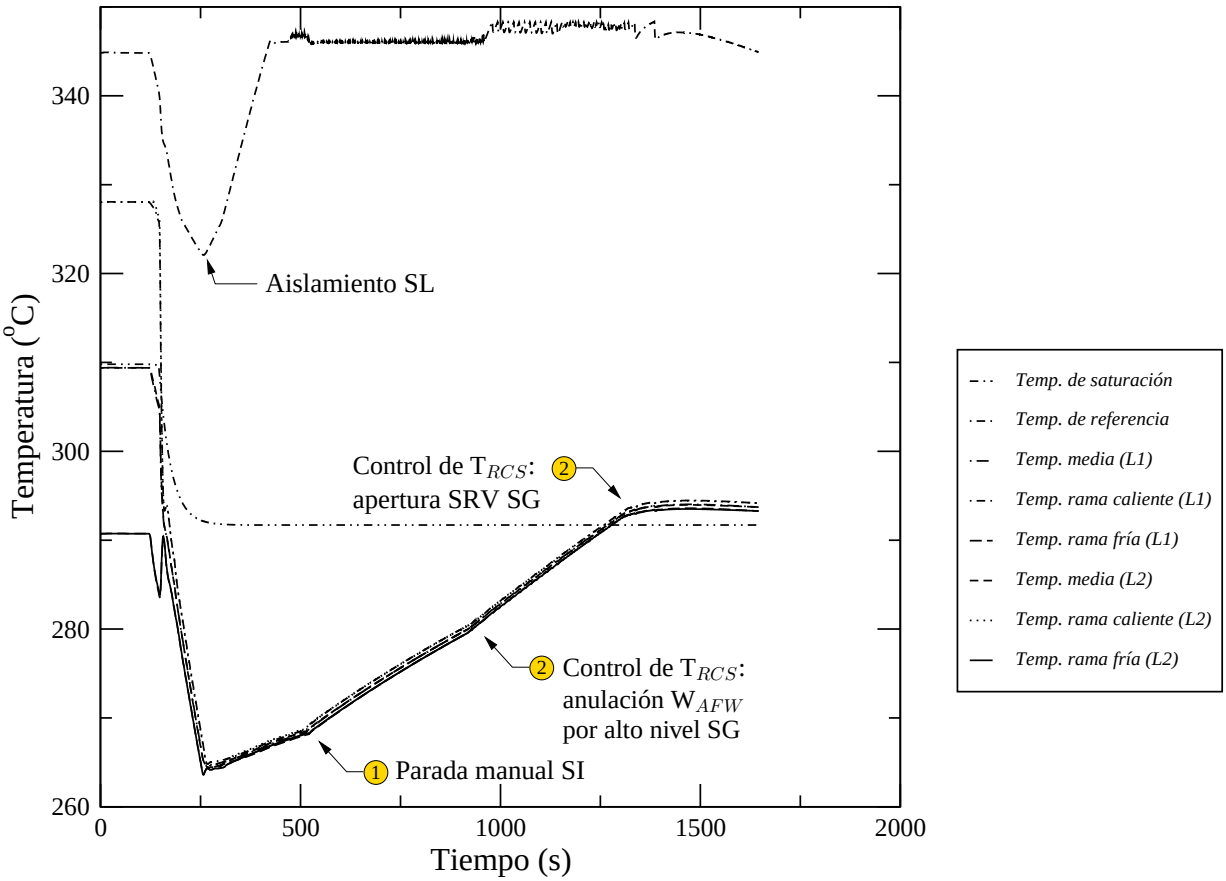
Gráfica 6.8: SLB aislable: presión en el primario.



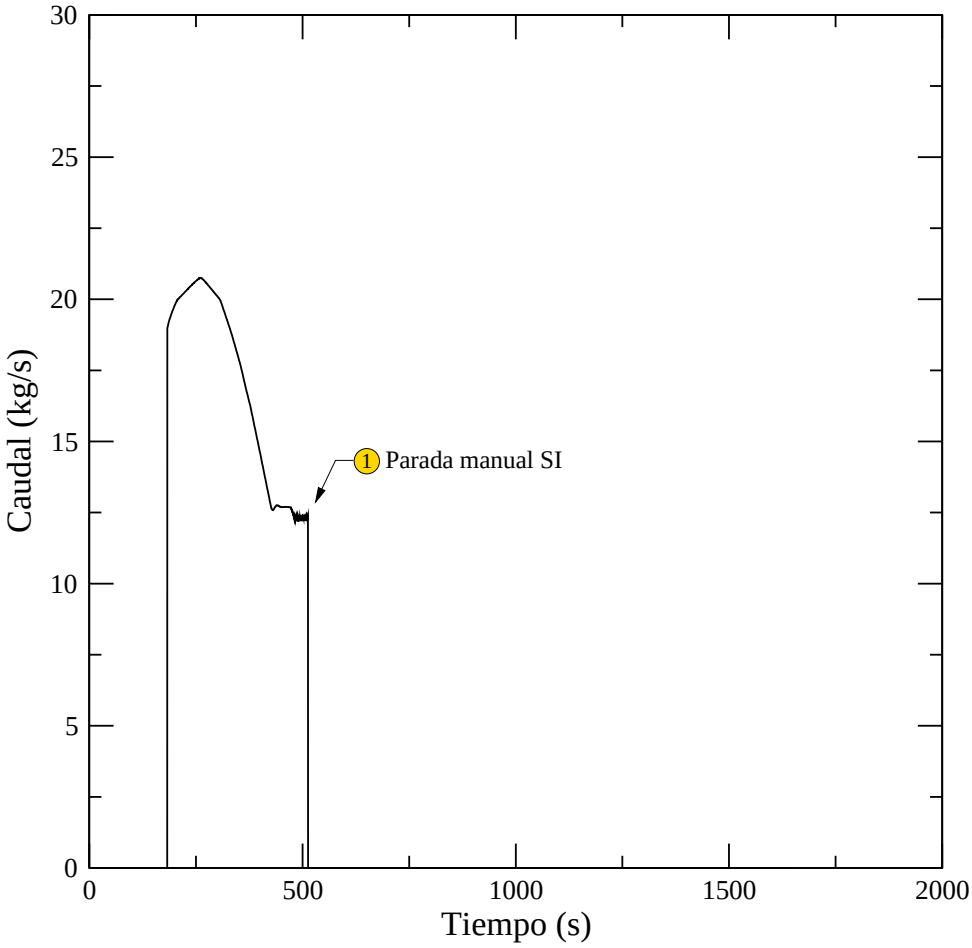
Gráfica 6.9: SLB aislable: nivel en el presionador.



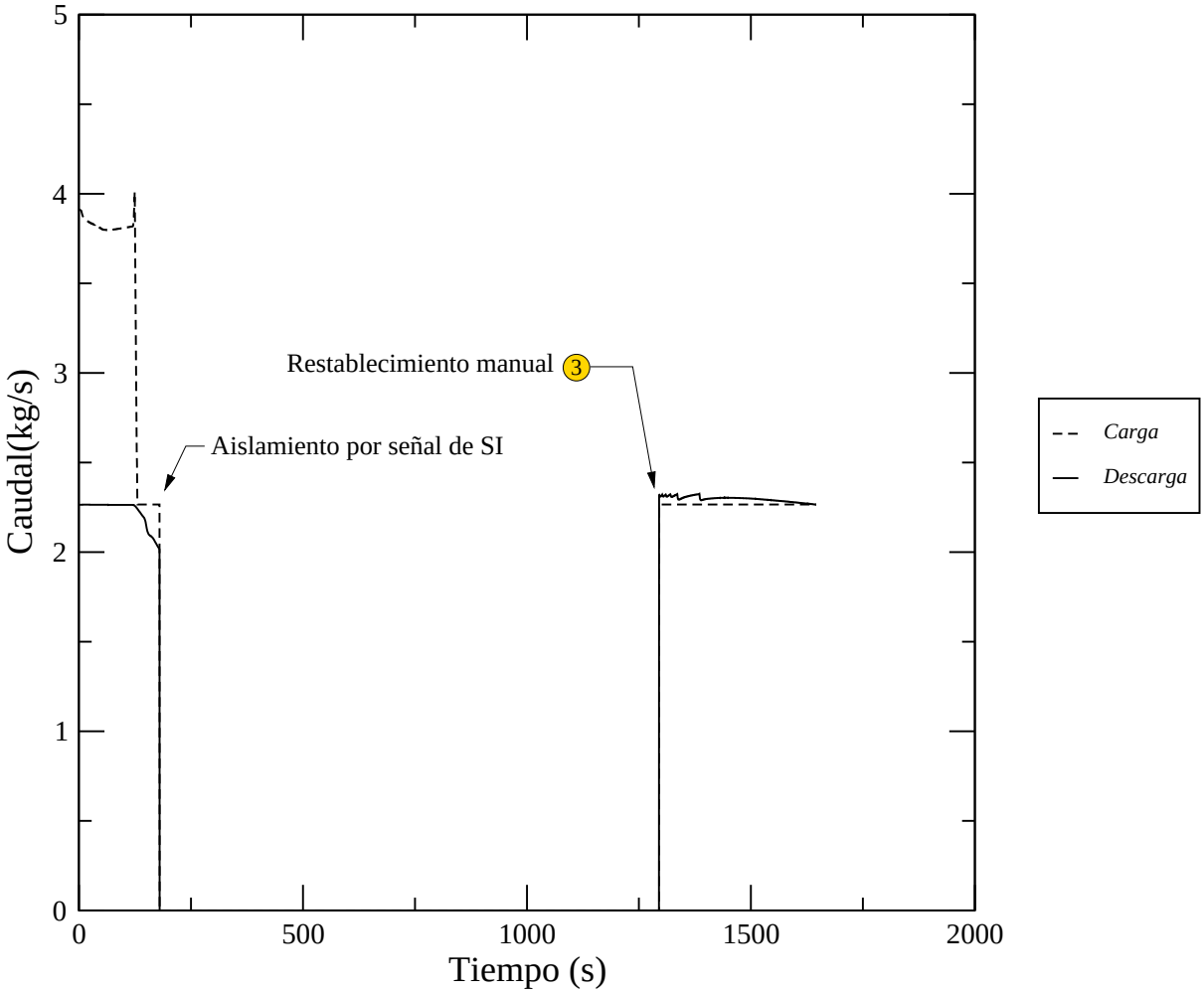
Gráfica 6.10: SLB aislable: caudal por las válvulas de alivio del presionador.



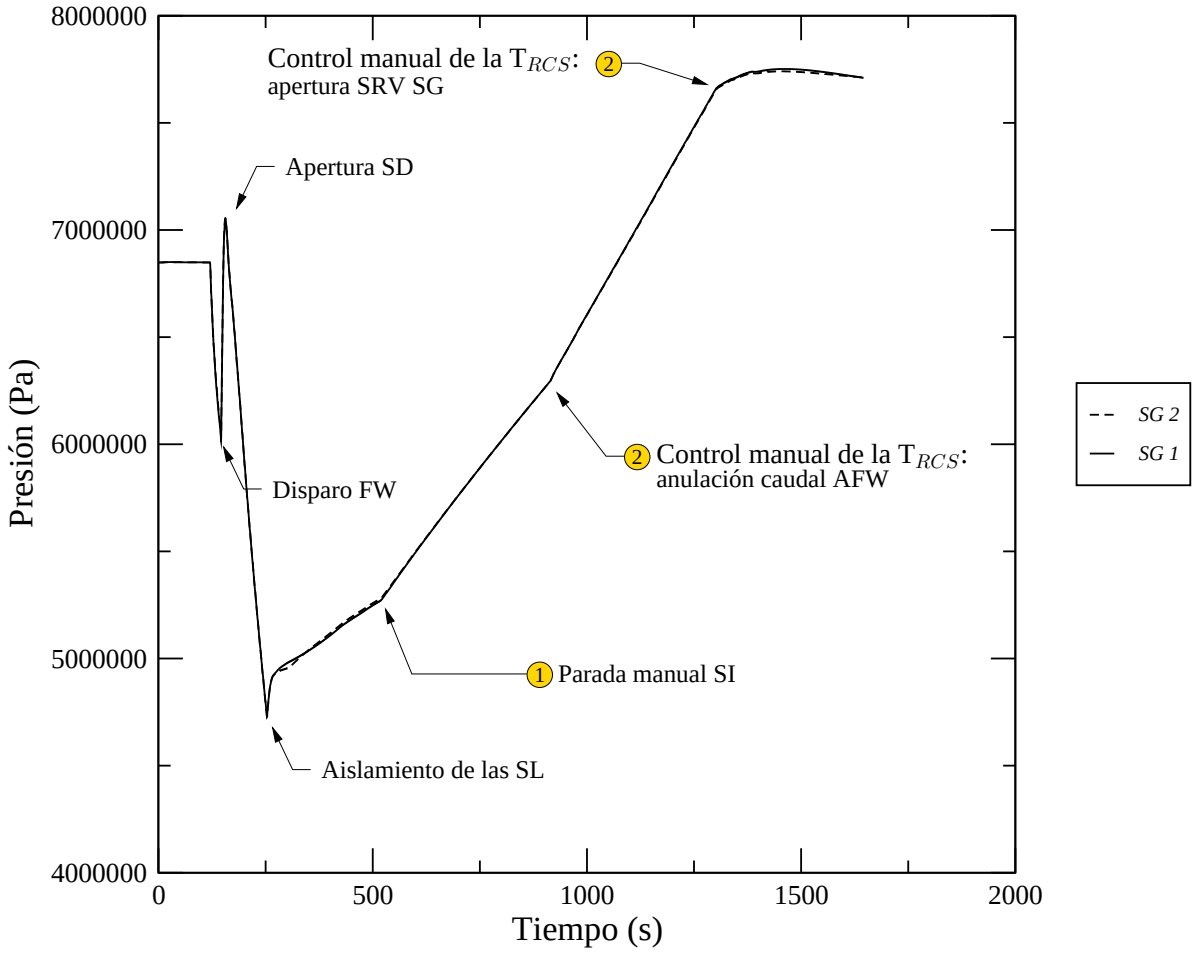
Gráfica 6.11: SLB aislable: temperatura media, de referencia y en los lazos del primario.



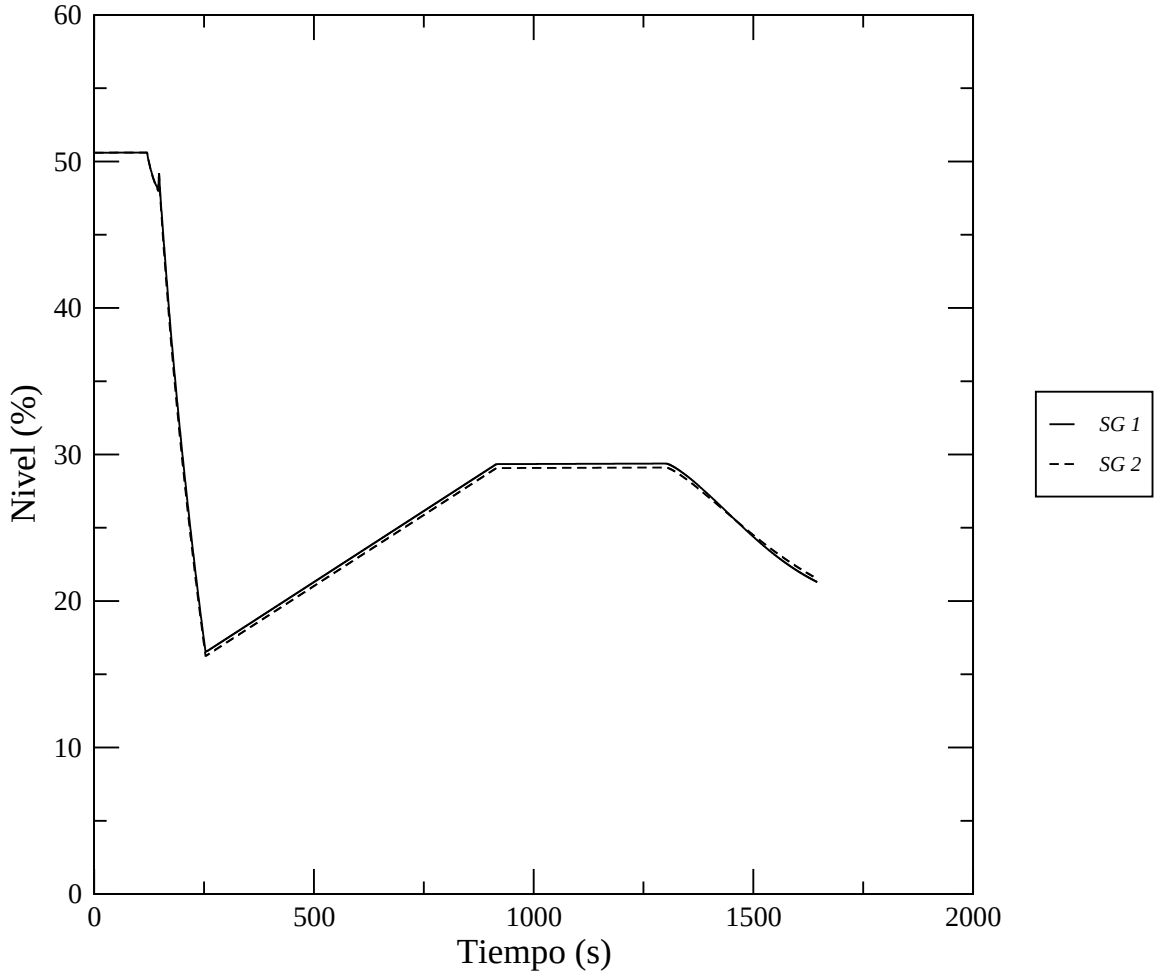
Gráfica 6.12: SLB aislable: caudal de inyección de seguridad.



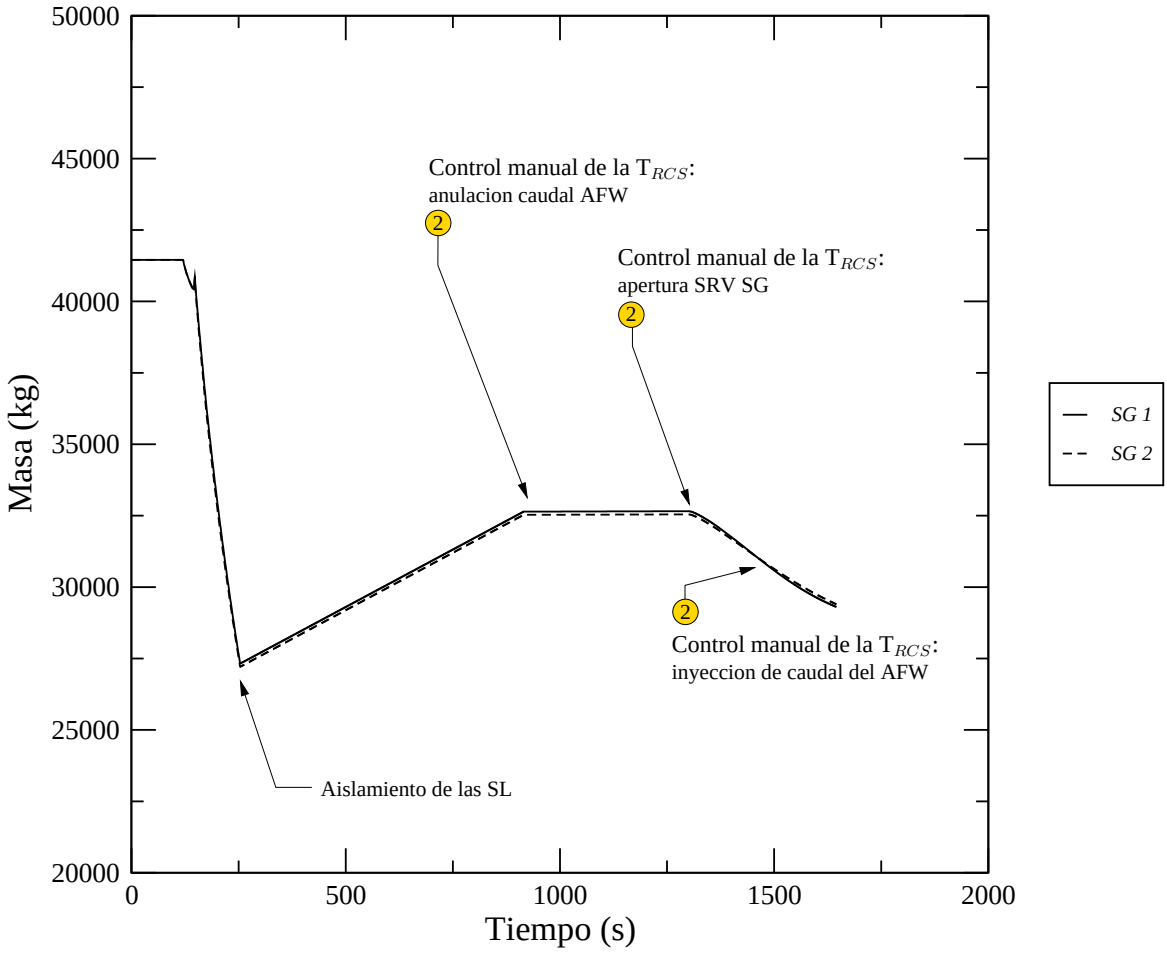
Gráfica 6.13: SLB aislable: caudales de carga y descarga del CVCS.



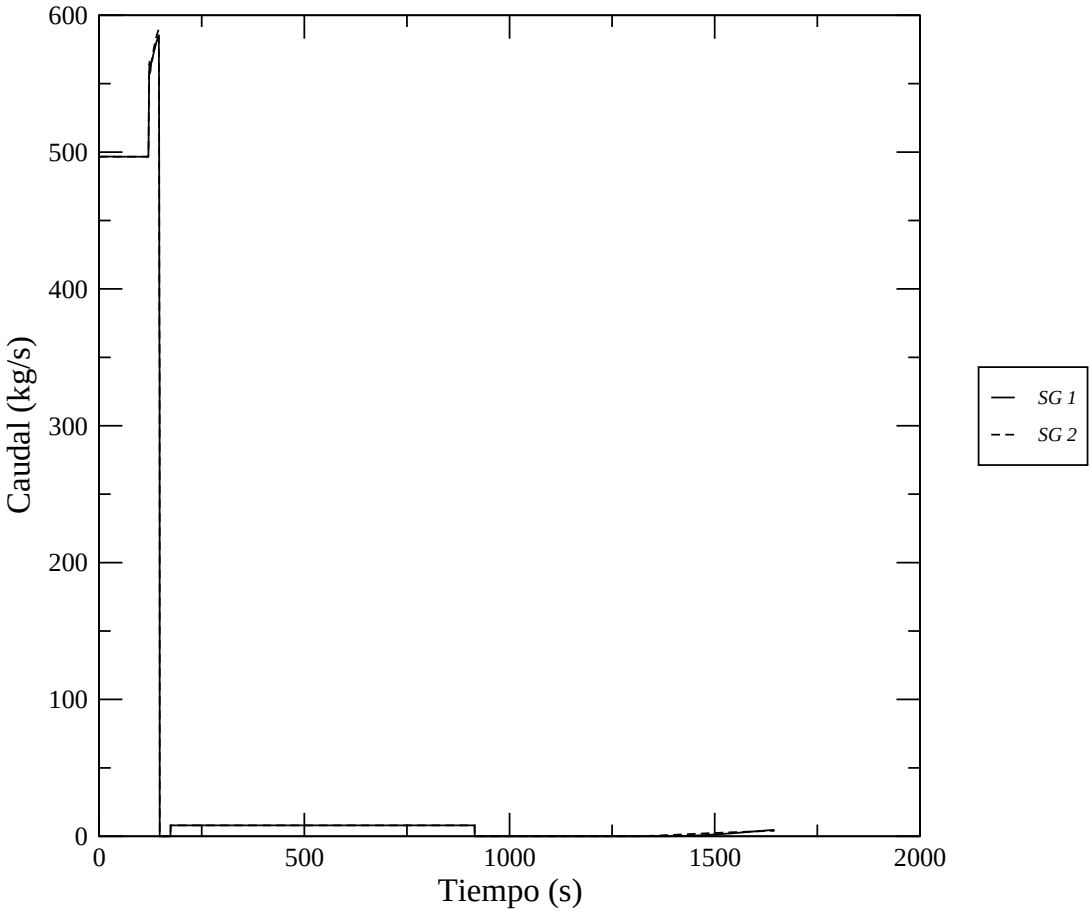
Gráfica 6.14: SLB aislable: presión en los generadores de vapor.



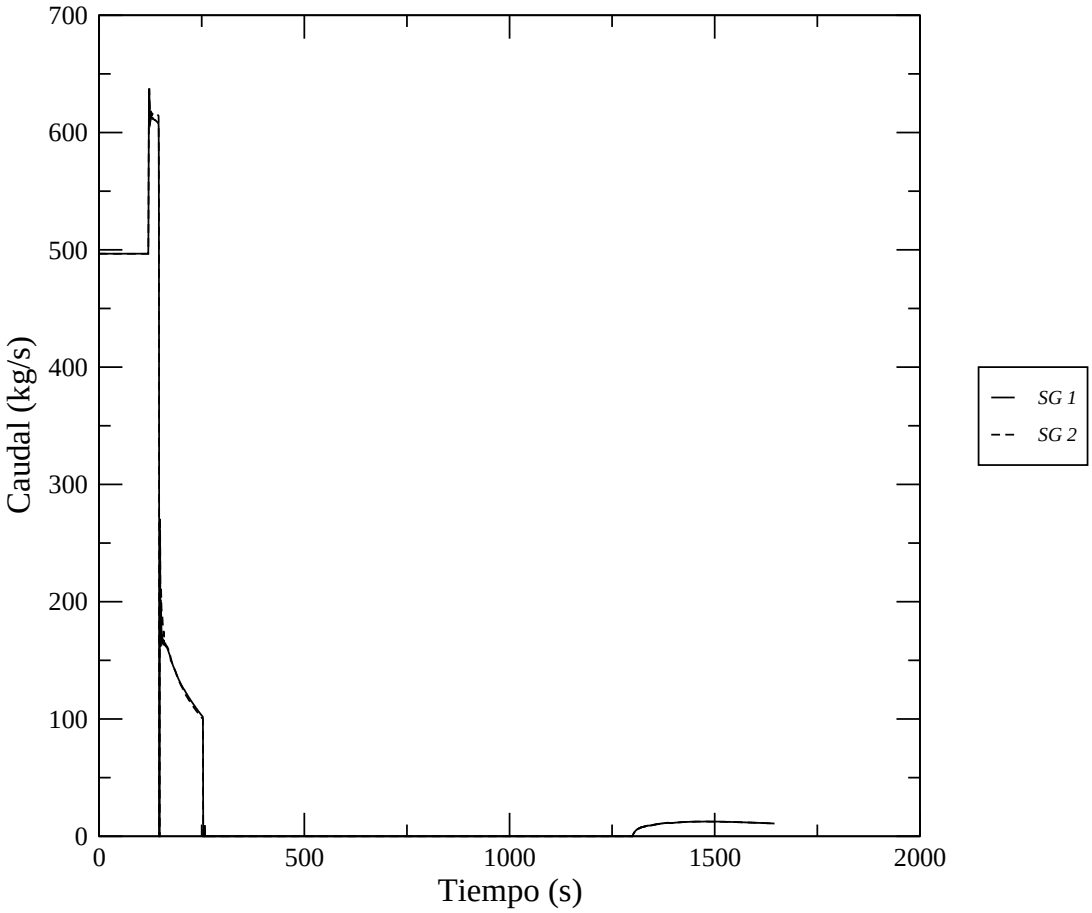
Gráfica 6.15: SLB aislable: nivel de rango estrecho de los generadores de vapor.



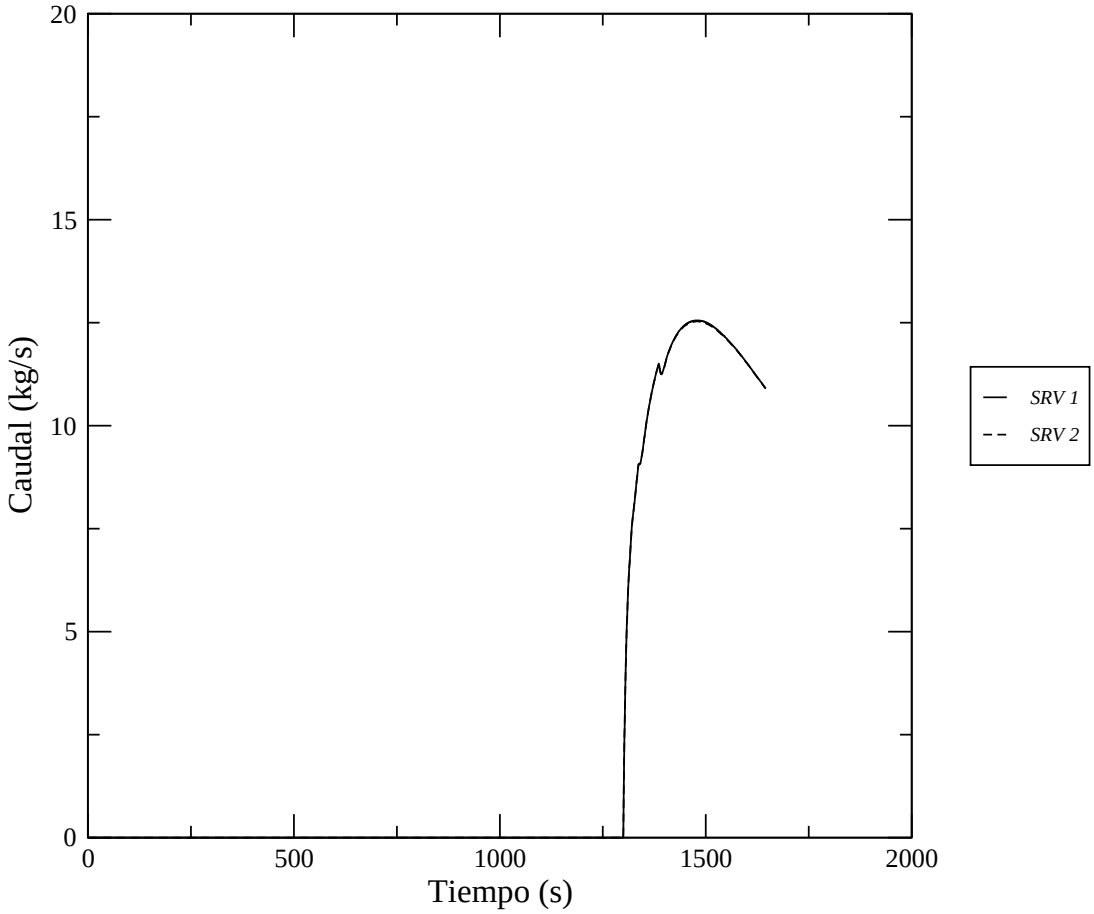
Gráfica 6.16: SLB aislable: inventario en los generadores de vapor.



Gráfica 6.17: SLB aislable: caudal de agua de alimentación de los generadores de vapor.



Gráfica 6.18: SLB aislable: caudal de vapor de los generadores de vapor.



Gráfica 6.19: SLB aislable: caudal por las válvulas de alivio de los generadores de vapor.

6.2.3 Resultados obtenidos con la herramienta TRETA/COPMA-III para el caso SLB no aislable

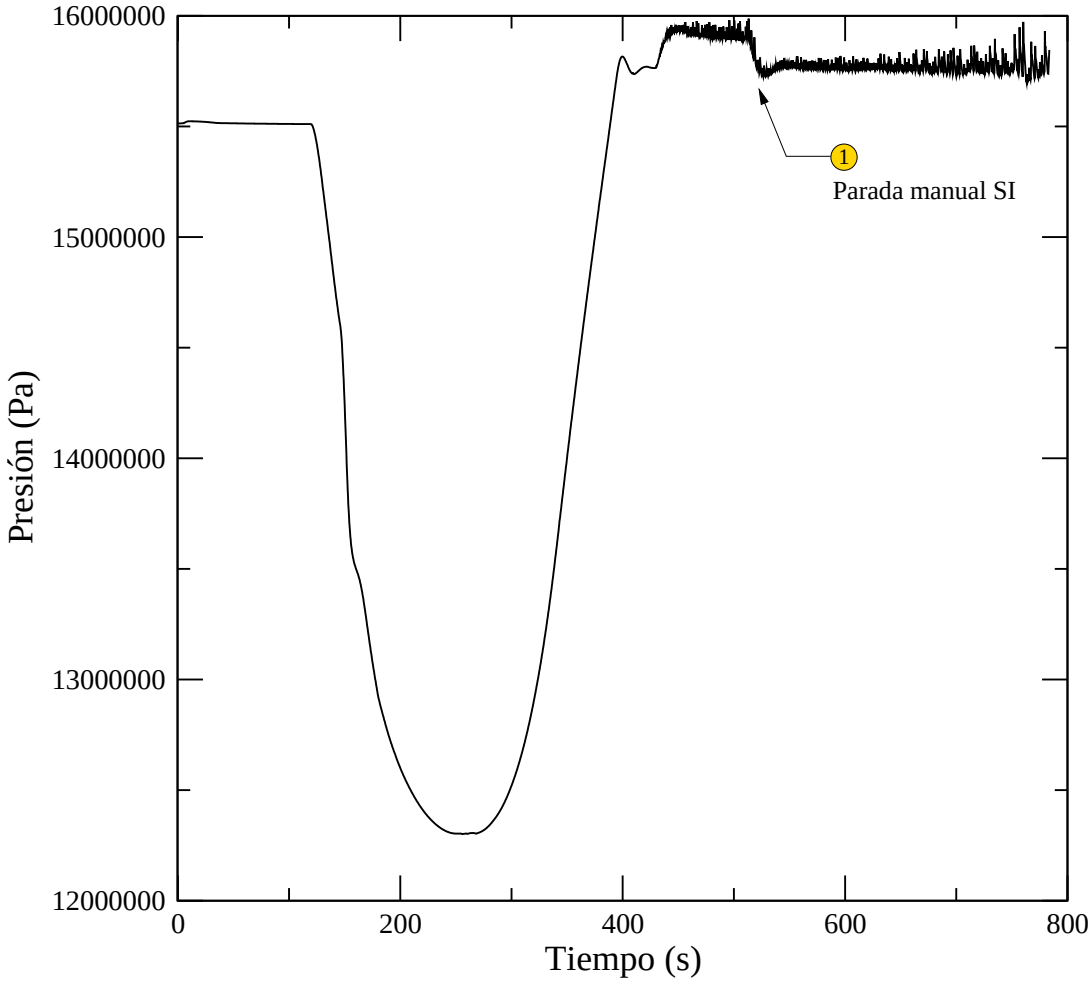
En este caso, se ha simulado la rotura grande en la línea de vapor correspondiente al lazo con presionador, Figura 6.22, que al igual que la simulación anterior, presenta un tamaño de 0,046 m^2, ocurriendo a los 120 s. La evolución de la planta, considerando la presión y el nivel del RCS, Figuras 6.20 y 6.21, no presenta grandes diferencias hasta que se produce el aislamiento de las líneas de vapor a los 185,4 s. Las diferencias más significativas se presentan en la evolución de las temperaturas de los ramas del primario, Figura 6.22. Para este caso, y en comparación con el transitorio de rotura grande en el colector, la bajada de presión y pérdida de inventario en el generador de vapor de la línea afectada son más acusados, Figuras 6.14 y 6.16, lo que provoca un enfriamiento mayor en el lazo de refrigeración correspondiente, lazo 2. Este hecho se refleja en los flujos caloríficos que se dan en cada uno de los SG, Figura 6.29, donde se comprueba como el generador de vapor afectado no solo refrigera el primario, si no que también refrigera los generadores de vapor intactos, llegándose a producir flujos de calor inversos, del lado secundario al primario, Figuras 6.30 y 6.31. Para modelar fielmente el fenómeno de refrigeración asimétrica de los lazos del RCS, el código TRETA dispone, en el módulo correspondiente a la simulación del mezclado a la entrada de la vasija (MIXRVI), de un parámetro de ajuste del mezclado que simula la mezcla del refrigerante proveniente de las ramas frías al atravesar la bajante y el plenum inferior de la vasija. Variando dicho parámetro se podría ajustar de forma realista la refrigeración asimétrica de los sectores azimutales del núcleo refrigerados por cada lazo, minimizando el efecto de flujo inverso en los lazos no afectados por la rotura.

La secuencia temporal difiere ligeramente de la obtenida para la rotura aislable del colector de las líneas de vapor, Tabla 6.16. Pudiéndose destacar el hecho de que el generador de vapor afectado se seca a los 341,7 s., poco después de la entrada en el procedimiento E-0 por parte del personal de la sala de control. A partir de ese momento, una vez aislados los generadores de vapor no afectados, su presión comienza a recuperarse, Figura 6.14, siendo el transitorio de comportamiento termohidráulico similar al correspondiente a la roturas aislable.

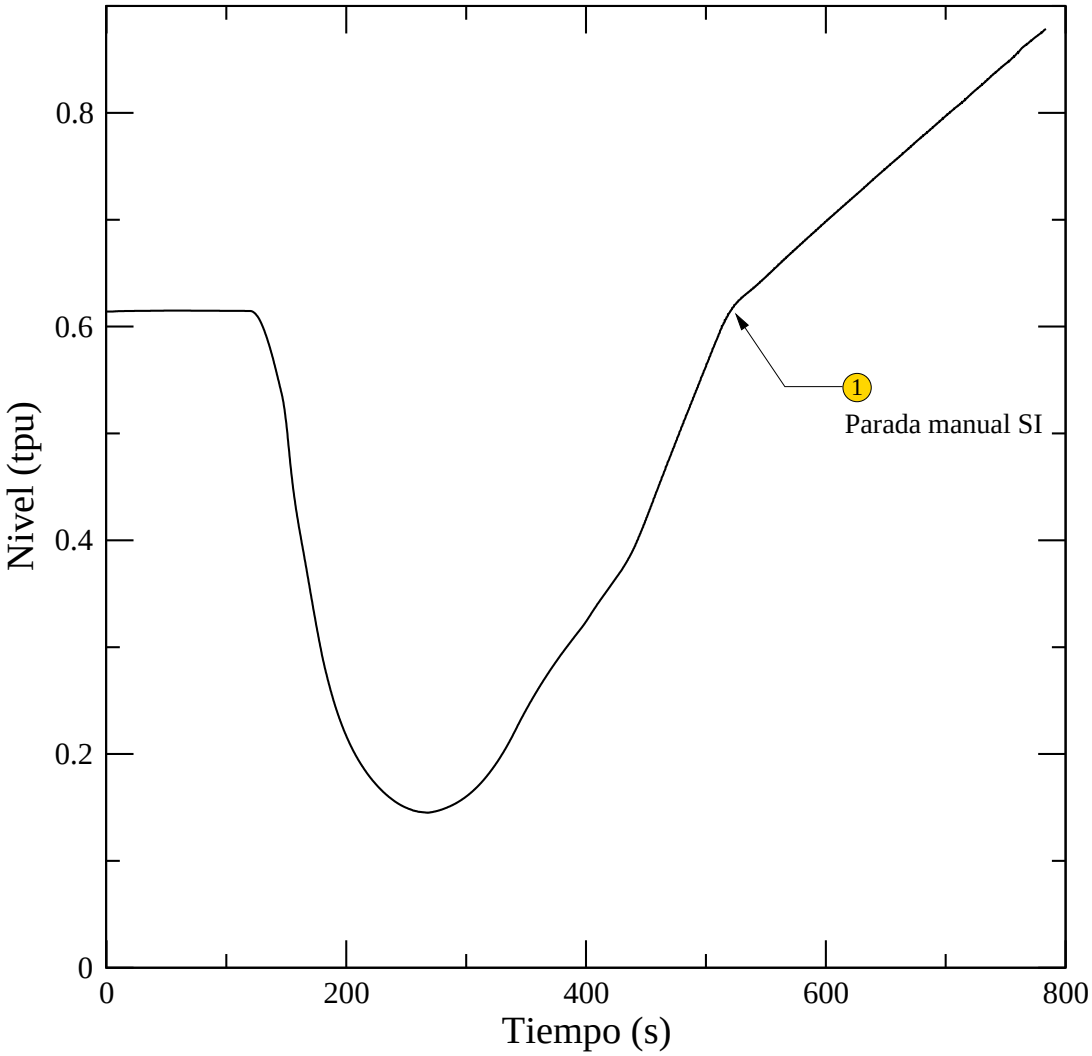
Las actuaciones humanas consideradas para este transitorio son las mismas que para el transitorio de rotura aislable, exceptuando el hecho de que la realización de las mismas presentaría, a partir del la transferencia al EOP E-2, *Procedimiento de aislamiento de un Generador de Vapor defectuoso*, un retraso de 70 s., tiempo considerado para la ejecución del procedimiento E-2. Cabe comentar, que ese tiempo no es el tiempo considerado para la realización del aislamiento del generador de vapor defectuoso, operación asignada al operador de turbina y que suele conllevar actuaciones tanto locales como en sala de control que se prolongan durante unos 20 minutos de media, sino el que requiere su exclusivamente su lectura por parte del operador supervisor del reactor y la asignación de las tareas en el registradas. Sin embargo, y debido a problemas de la simulación por fallo en el cálculo del punto de operación de la RCP del lazo afectado por la rotura, la simulación finaliza a los 783,6 s., momento hasta el cual el operador solo ha realizado la parada manual de la SI a los 510 s., actuación registrada en la subtarea 7.1 del procedimiento E-0., tal como se explica en la sección anterior, correspondiente a la simulación del transitorio de rotura aislable en el colector de las líneas de vapor.

ACTUACIONES AUTOMÁTICAS	
Tiempo (s.)	**Descripción**
120	Rotura de 0,046 m^2 en la línea de vapor asociada al lazo 2
145,8	Disparo del reactor por alto flujo neutrónico. Apertura del alivio de vapor al condensador
146,1	Disparo de turbina
148,2	Disparo de las bombas del FWS
148,5	Señal de actuación del AFWS (Señal W)
174,5	Inyección del AFWS (26 s. de retraso respecto a la señal W)
176,7	Señal de aislamiento de las SL
177	Señal de inyección de seguridad (Señal S). Señal de aislamiento del FWS
180	Inyección del SIS (3 s. de retraso respecto a la señal S)
185,4	MSIV cerradas
341,7	Secado del SG defectuoso
ACTUACIONES MANUALES / GESTIÓN DEL OPERADOR	
Tiempo (s.)	**Descripción**
300	**Entrada en EOP (EOP E-0)**
410	Se considera necesaria la SI debido a baja presión en el RCS. Subtarea 4.1
500	Se supone diagnóstico del suceso como una LSLB, margen conservador Park et al. (2005)
510	Parada de la SI. Subtarea 7.1. Implementada por SA/DM del operador
783,6	Finalización de la simulación por fallo en el cálculo del punto de operación de la RCP del lazo afectado por la rotura. Flujo inverso en el lazo 2.

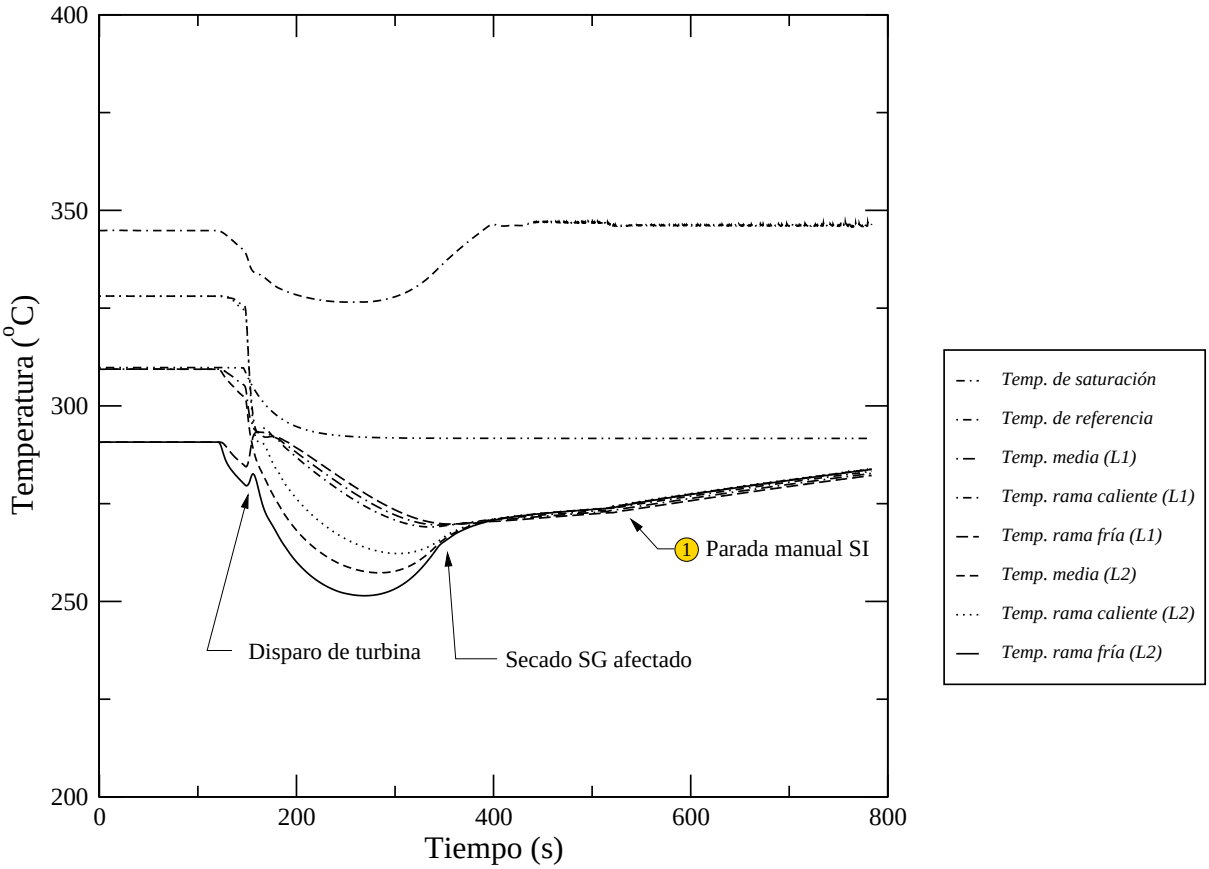
Tabla 6.16: SLB no aislable: secuencia de actuaciones automáticas y manuales.



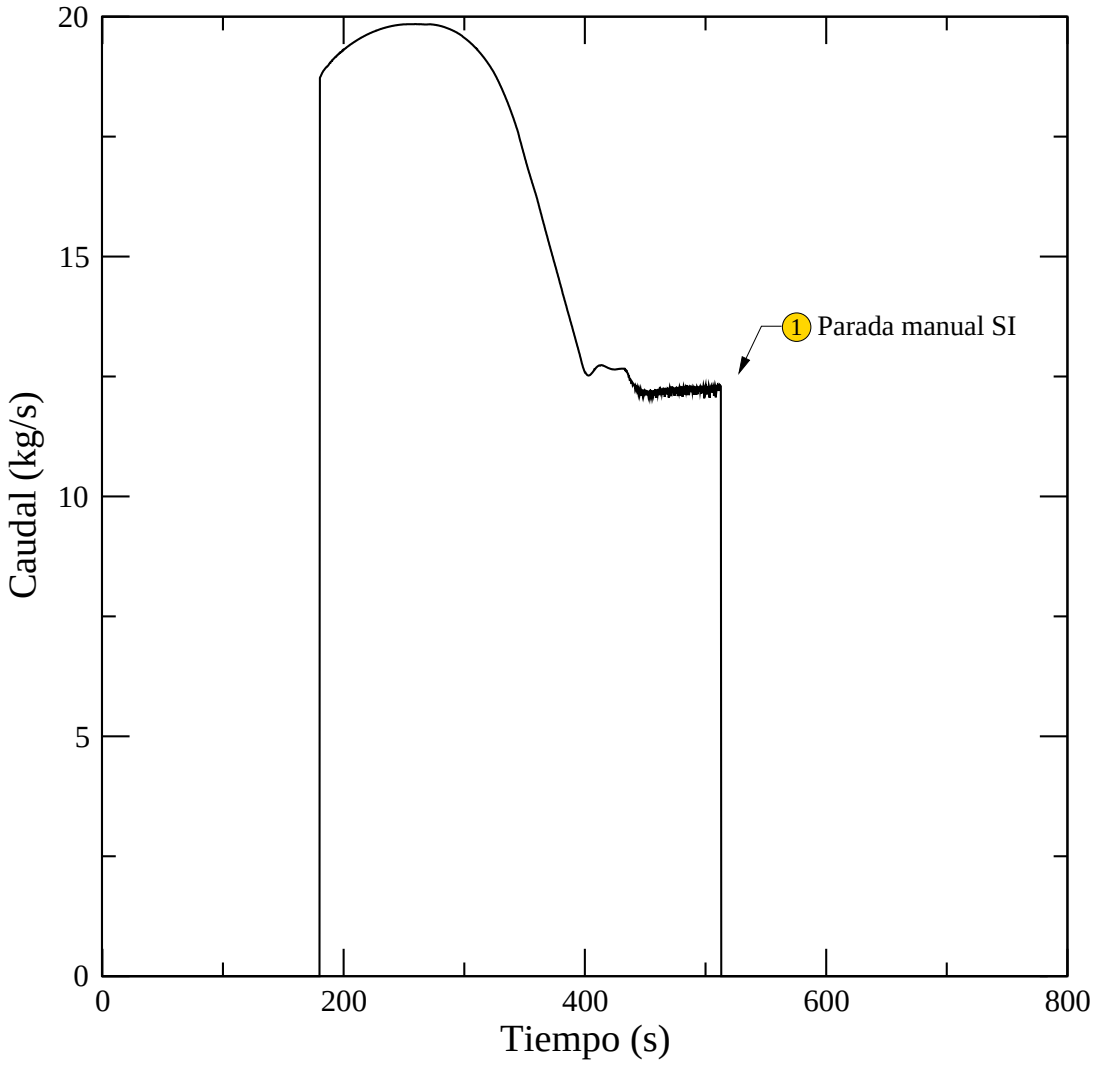
Gráfica 6.20: SLB no aislable: presión en el primario.



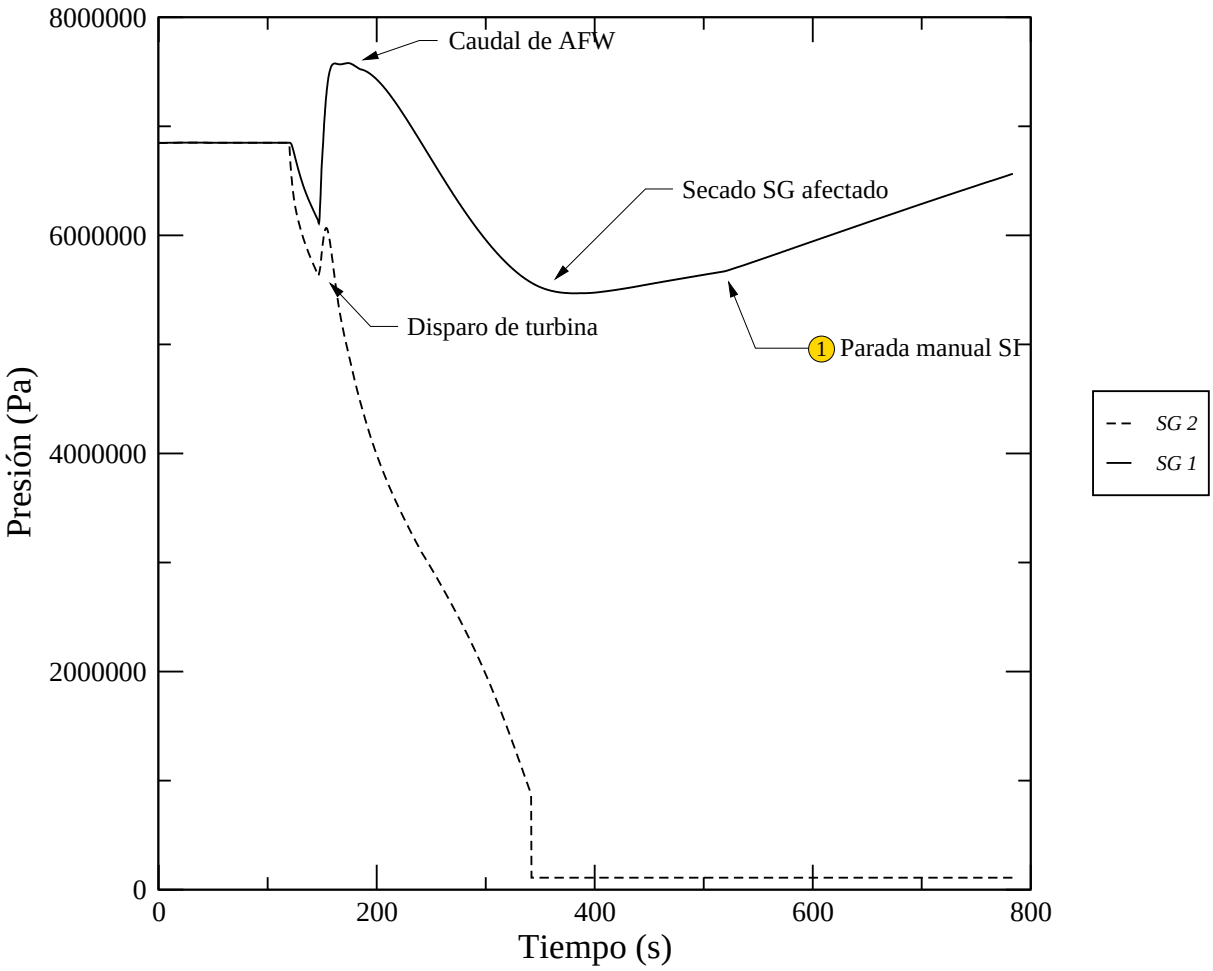
Gráfica 6.21: SLB no aislable: nivel en el presionador.



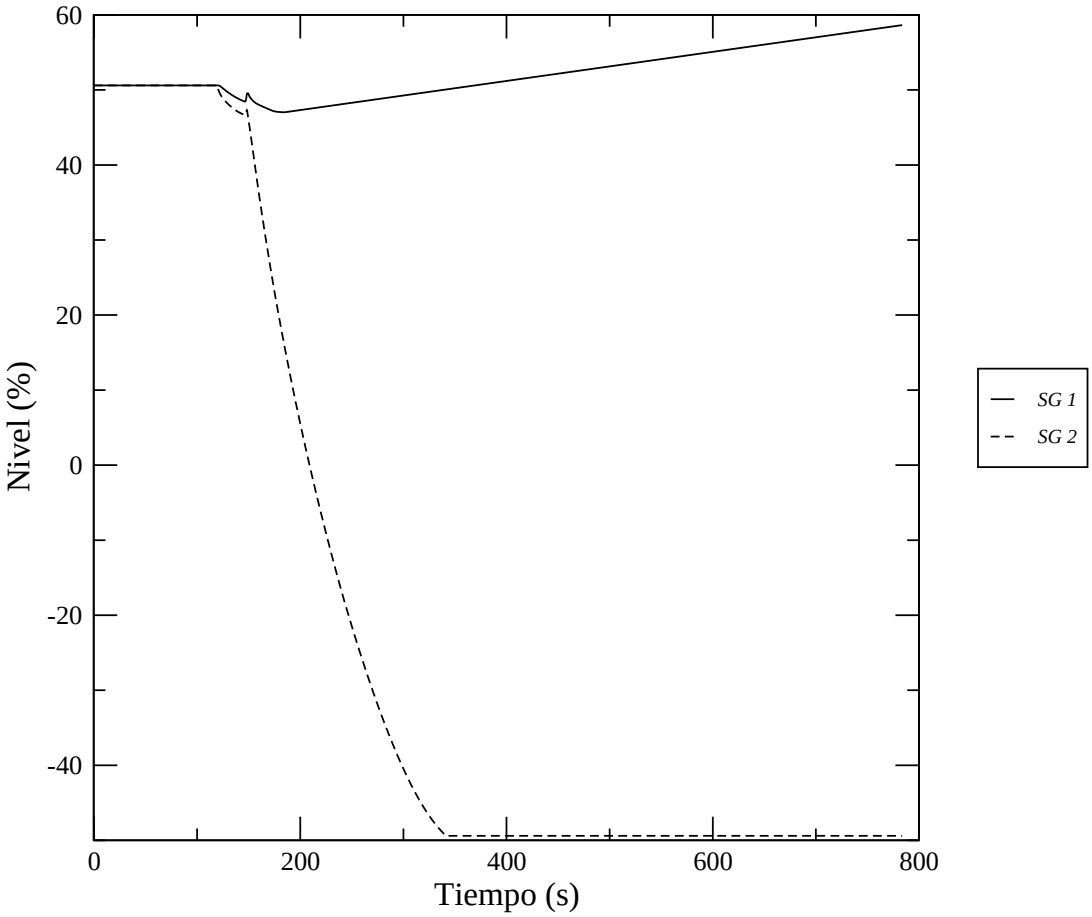
Gráfica 6.22: SLB no aislable: temperatura media, de referencia y en los lazos del primario.



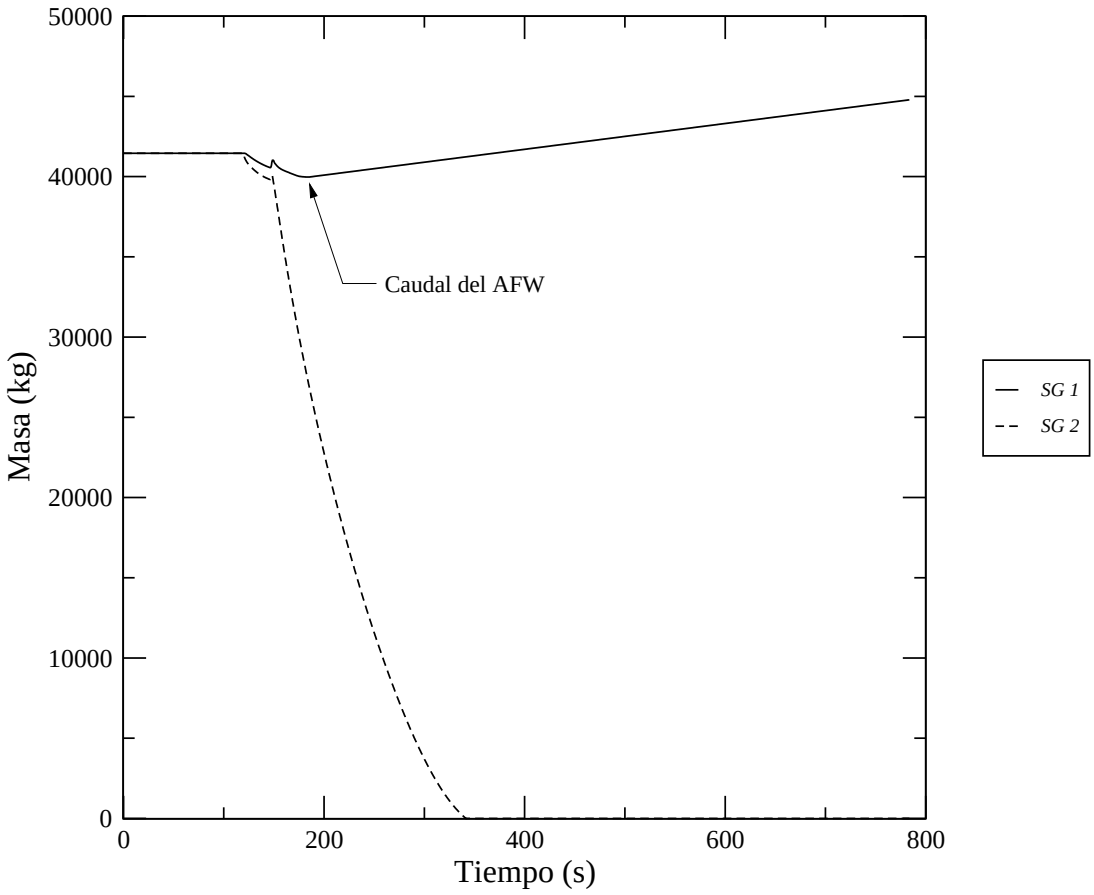
Gráfica 6.23: SLB no aislable: caudal de inyección de seguridad.



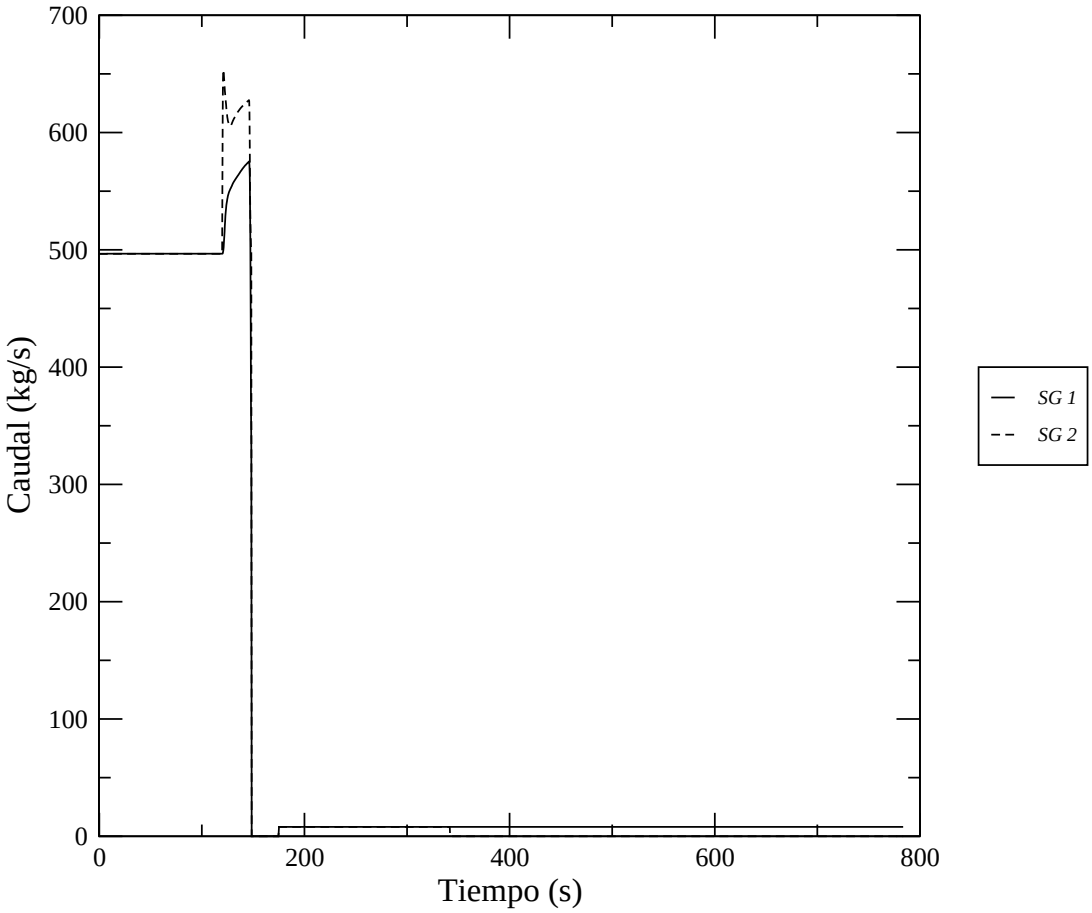
Gráfica 6.24: SLB no aislable: presión en los generadores de vapor.



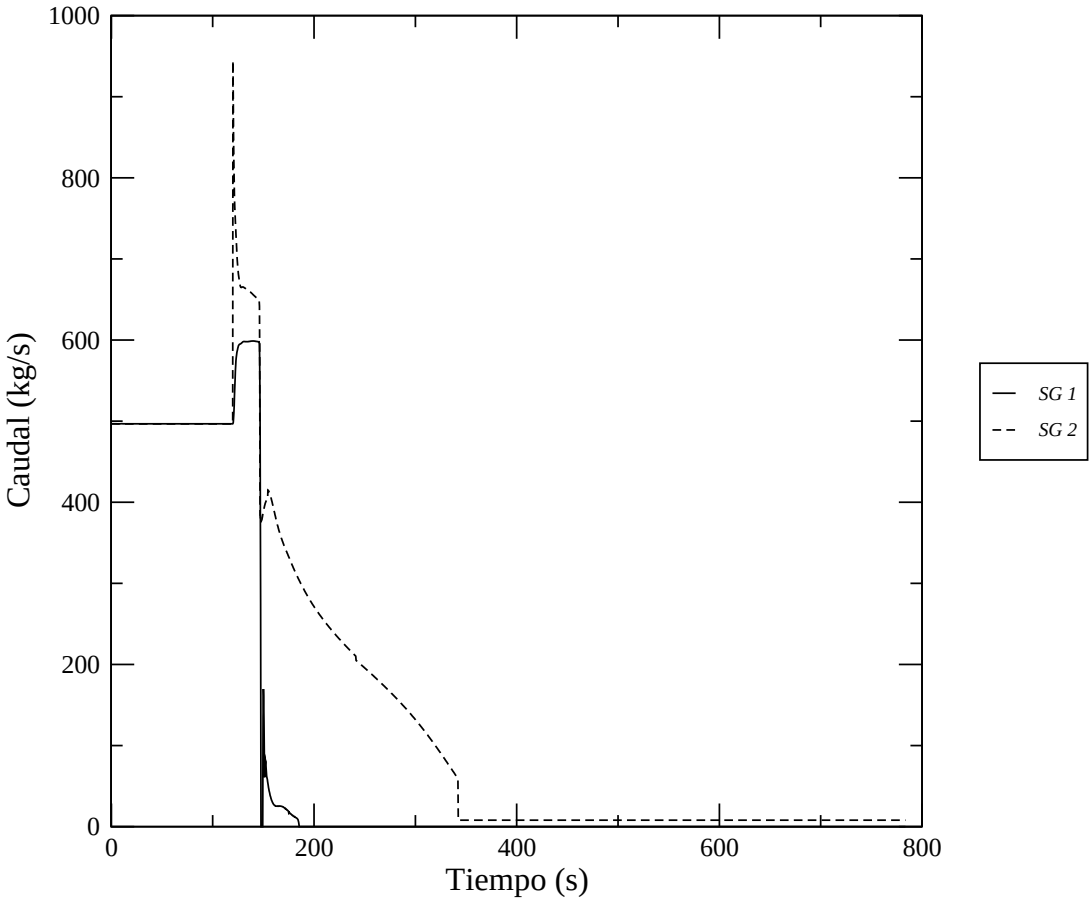
Gráfica 6.25: SLB no aislable: nivel de rango estrecho de los generadores de vapor.



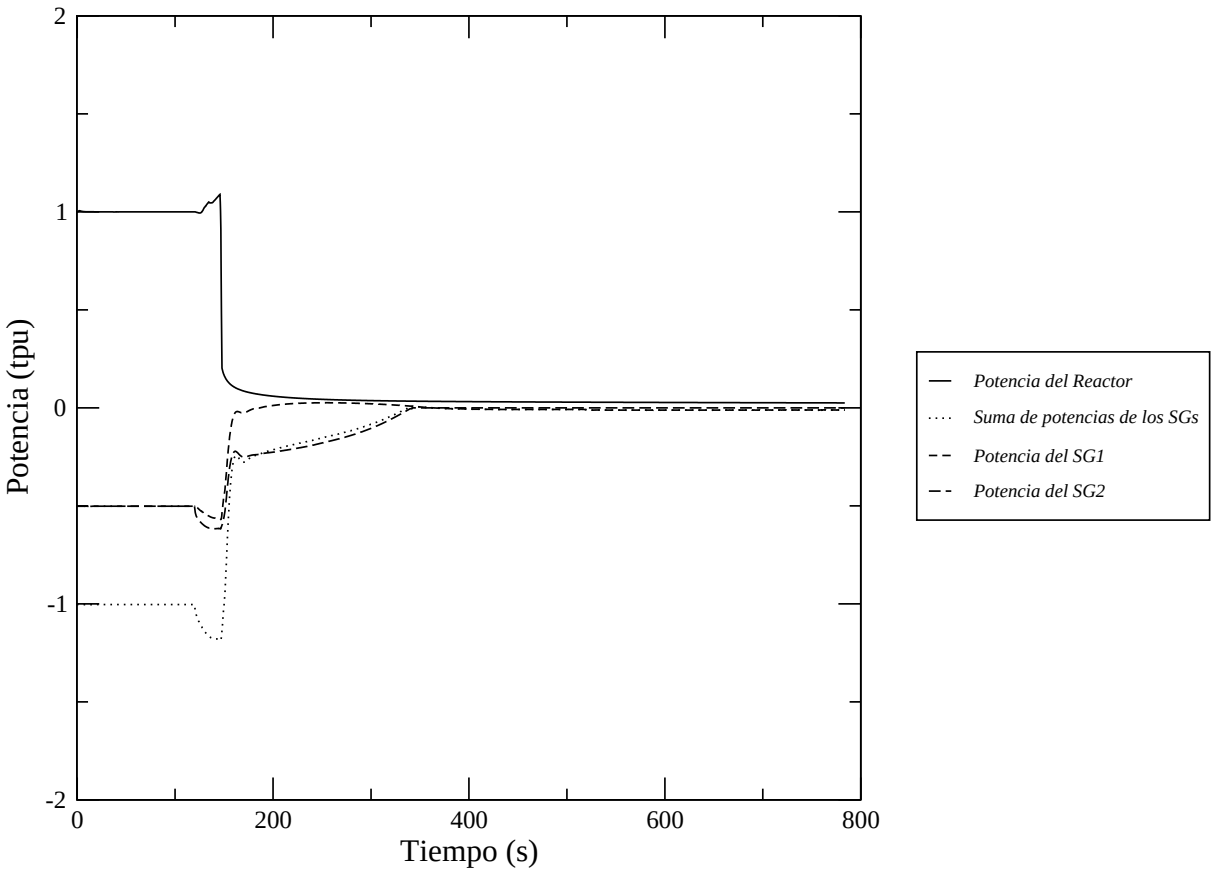
Gráfica 6.26: SLB no aislable: inventario en los generadores de vapor.



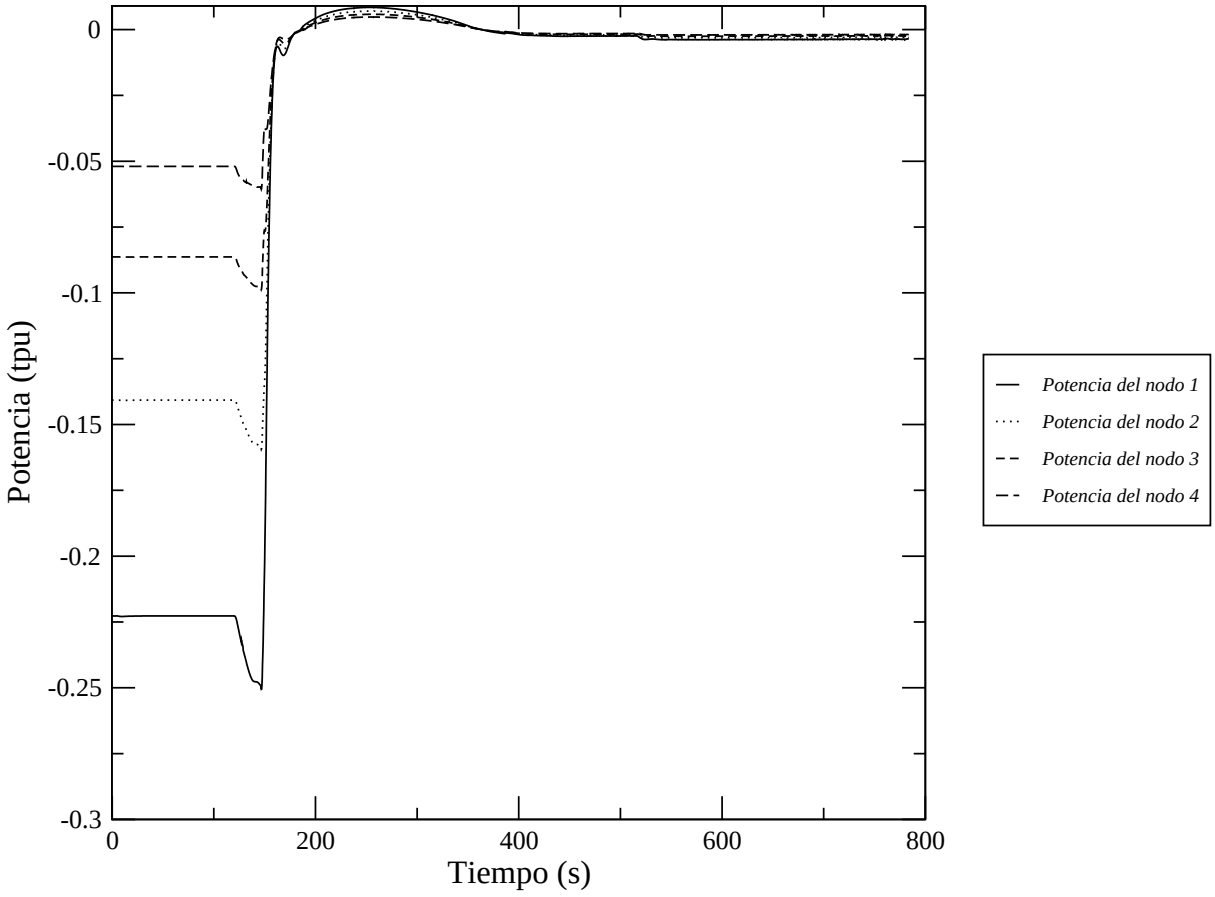
Gráfica 6.27: SLB no aislable: caudal de agua de alimentación de los generadores de vapor.



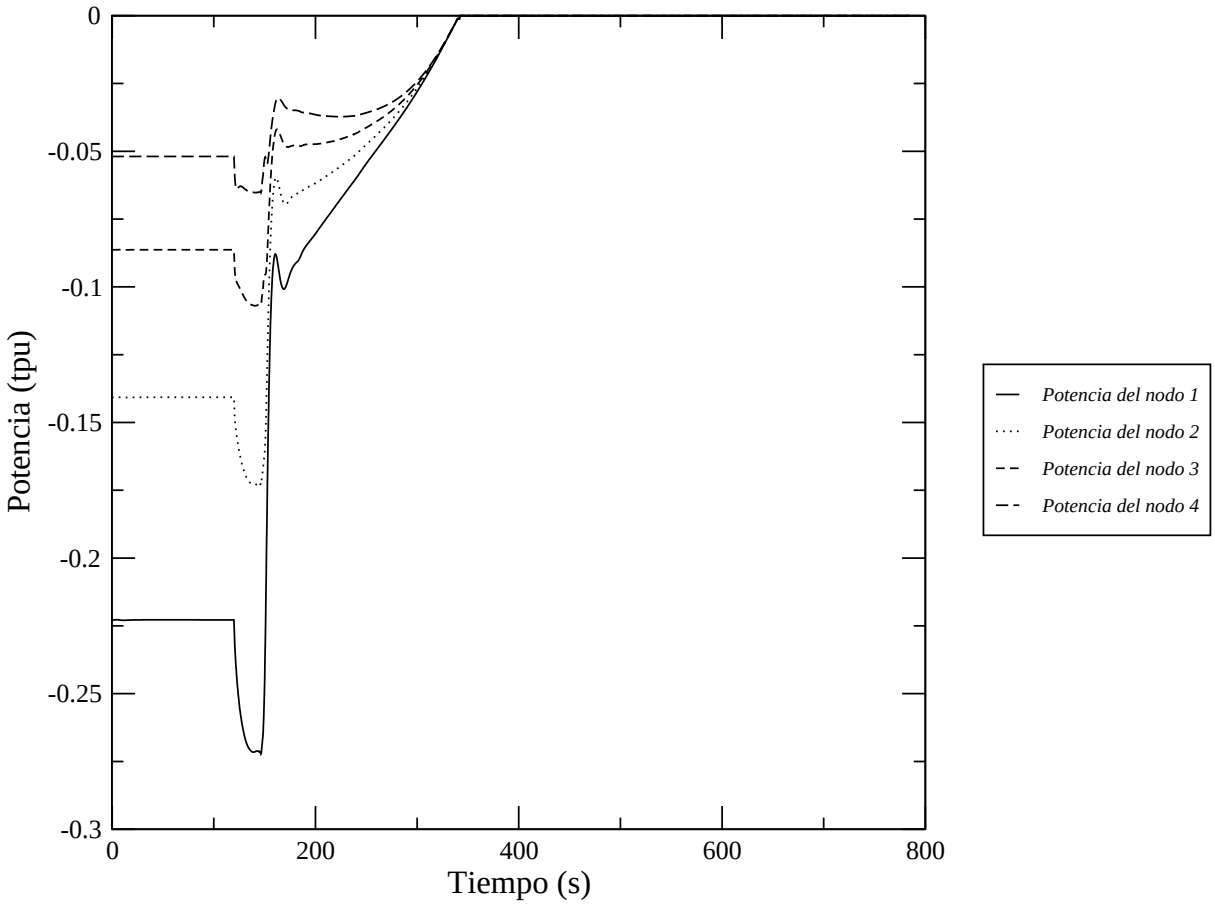
Gráfica 6.28: SLB no aislable: caudal de vapor de los generadores de vapor.



Gráfica 6.29: SLB no aislable: flujos caloríficos normalizados para cada generador de vapor.



Gráfica 6.30: SLB no aislable: flujos caloríficos normalizados para cada nodo de los generadores de vapor 1/3.



Gráfica 6.31: SLB no aislable: flujos caloríficos normalizados para cada nodo del generadore de vapor 2.

6.3 Pérdida total de agua de alimentación con pérdida de sumidero de calor

El otro tipo de secuencia considerado en la aplicación de la herramienta consiste en la simulación del transitorio de pérdida total de agua de alimentación (*Total Loss of Feedwater*, TLFW) con pérdida del sumidero de calor. En este tipo de secuencias se considera el fallo en demanda del AFWS, resultando la secuencia que se marca en el árbol de sucesos de la Figura 6.24.

La pérdida del agua de alimentación principal puede darse por rotura en el colector del agua de alimentación, tal como se postula en esta simulación, Figuras 6.25. Independientemente del suceso iniciador, el fallo subsiguiente en demanda del AFWS puede estar provocado, principalmente, por fallo en las operaciones de mantenimiento o de diseño, Bumgardner et al. (1994). Posterior al fallo en demanda, se considera la imposibilidad de realizar aporte de inventario a los SG por ninguna otra vía, p. ej. aporte de agua de condensado, lo que conlleva de forma inequívoca a la aplicación de la maniobra de F&B para mantener el núcleo refrigerado.

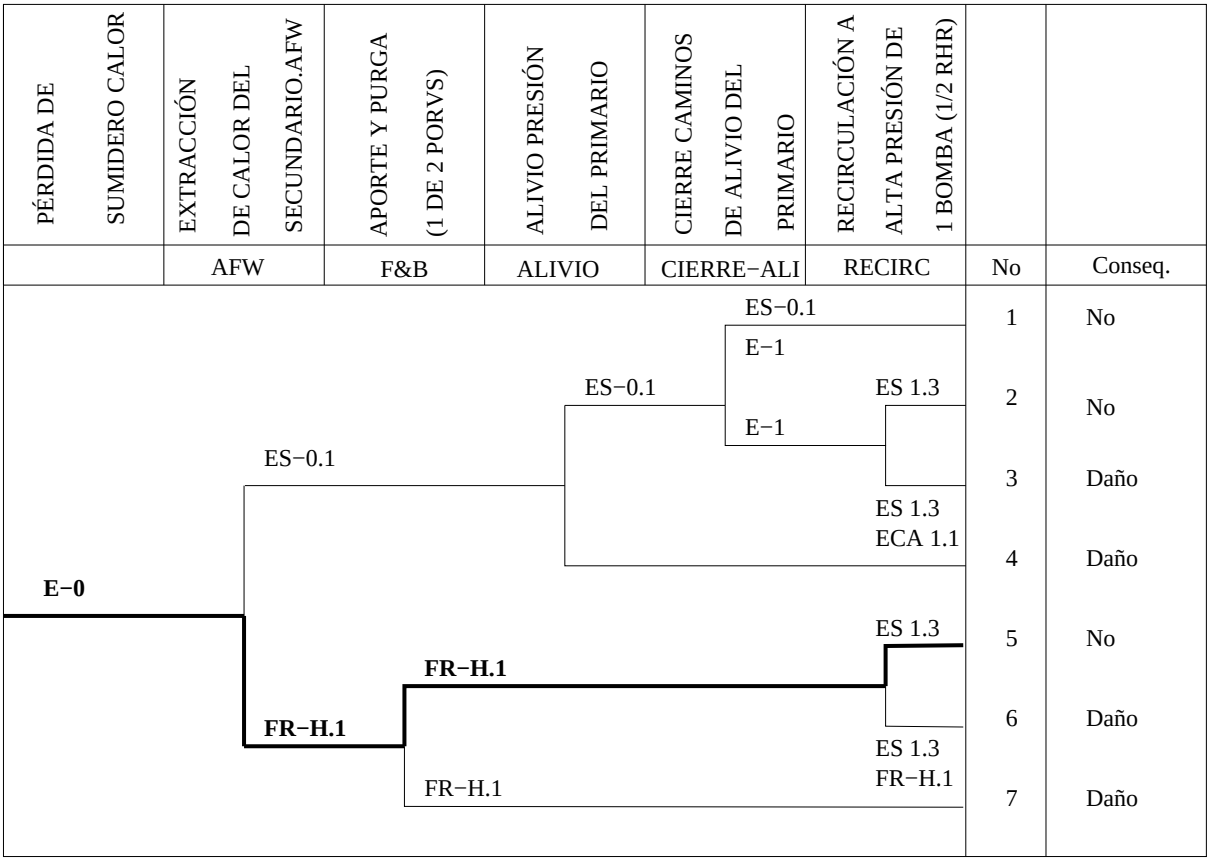


Figura 6.24: Árbol de sucesos de las secuencias de pérdida total de agua de alimentación para la aplicación de la herramienta.

El F&B del primario es una operación que conlleva:

- La consideración por parte del operador para su realización de aspectos que no están relacionados con la gestión de emergencias, situando en segundo plano la operación segura de la planta. Las consecuencias económicas de llevar a cabo el F&B para el explotador son muy costosas, siendo el responsable de la aplicación del F&B el operador.
- El diseño de los FRG de aplicación en los reactores PWR-W, conlleva la evaluación simultánea de dos objetivos opuestos: la recuperación del AFW y la entrada en F&B.

Este dos puntos, hacen que el juicio técnico del operador pueda decidir sus actuaciones considerando objetivos no relacionados con la operación segura de la planta durante la toma de decisiones, Dougherty (1993).

Además de estos aspectos, que ya de por sí hacen de este tipo de secuencias presenten interés en lo que respecta a la implementación de los EOP, cabe destacar los relacionados con la evaluación de las capacidades del código de simulación termohidráulico. En este sentido, los transitorios de simulación de pérdida de sumidero de calor conllevan el llenado del presionador, la refrigeración denominada de un solo paso (*Once Through Cooling*, OTC) y, en caso de no tener éxito la operación de F&B, la saturación del primario. Por ello, esta secuencia es muy interesante para evaluar el conjunto de la herramienta, aunque el estudio realizado en este trabajo es preliminar, orientado exclusivamente como prueba funcional del simulador integral.

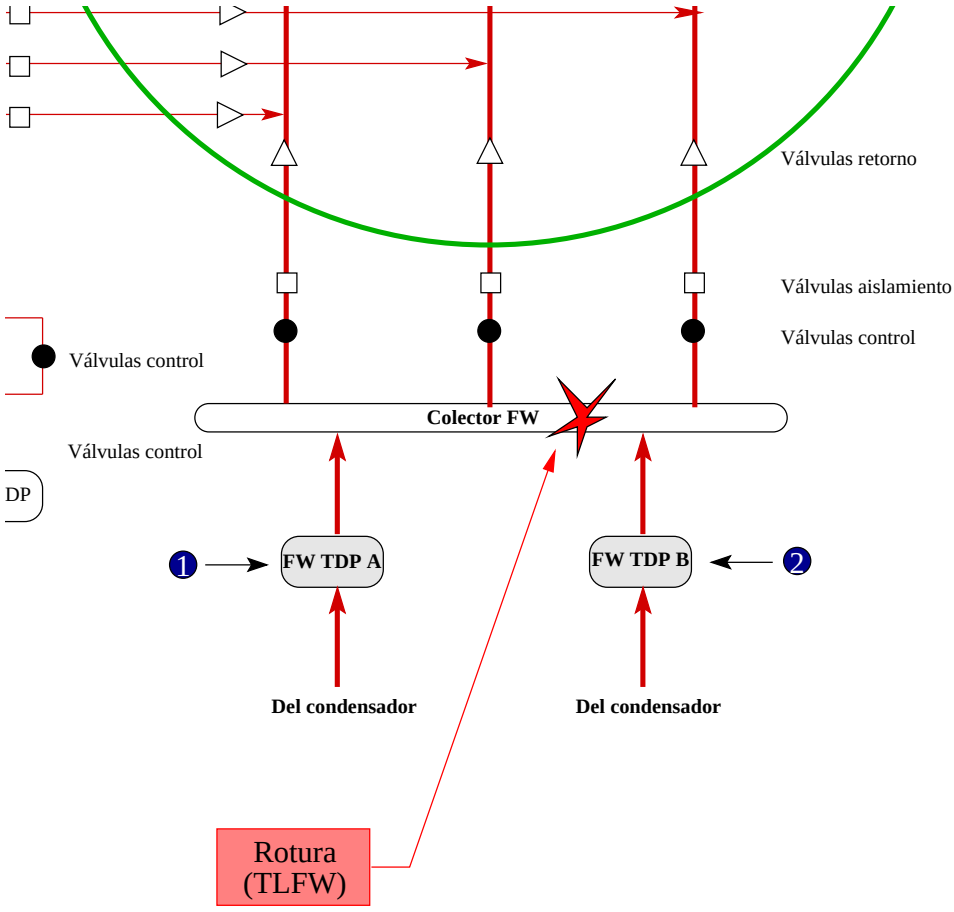


Figura 6.25: Localización de las roturas para las secuencias de TLFW.

6.3.1 Actuaciones del operador contempladas en los procedimientos para las secuencias de TLFW

Las actuaciones más relevantes del operador en las secuencias de TLFW con pérdida de sumidero de calor se muestran en el contexto de los EOP en la Figura 6.26. A diferencia de la secuencia de LSLB, la secuencia de TLFW suele ir acompañada de una fenomenología que hace que presente tiempos de diagnóstico ligeramente menores, Tablas 6.1 y 6.2. Además, la vigilancia del árbol de de las CSF se inicia en la fase temprana del incidente, tras transferencia desde el paso 4 del EOP E-0 al subprocedimiento ES-0.1, *Procedimiento de recuperación del disparo del reactor*, al no producirse señal de actuación de la SI al inicio del transitorio. Este aspecto, unido al hecho de que la condición roja de la FRG H.1, *Respuesta ante la pérdida de sumidero de calor*, se cumple a los pocos segundos tras la parada del reactor, conllevan que la gestión de la emergencia pase a realizarse por la FRG H.1 a los pocos minutos de la entrada en los EOP, Figura 6.26. De hecho, si se considerase la vigilancia realizada de las CSF mediante el sistema SPDS de la sala de control, dicha transferencia podría realizarse incluso antes. Por ello, el conjunto de actuaciones está fuertemente condicionado por los fallos de sistemas impuestos en la simulación y el seguimiento de un solo procedimiento, quedando definido de forma cerrada, Tabla 6.17.

Actuación	Acción del operador	EOP-PASO	Subtarea
1	Disparo de las RCP	H.1-3	H.1-3.1
2	Despresurización del primario	H.1-6.b	H.1-6.b.1
3	Despresurización del secundario	H.1-6.e	H.1-6.e.1
4	Inicio de aporte al primario	H.1-9.1	H.1-9.1
5	Inicio de purga del primario	H.1-12.1	H.1-12.1

Tabla 6.17: Tareas significativas de los EOP considerados en las secuencias de TLFW.

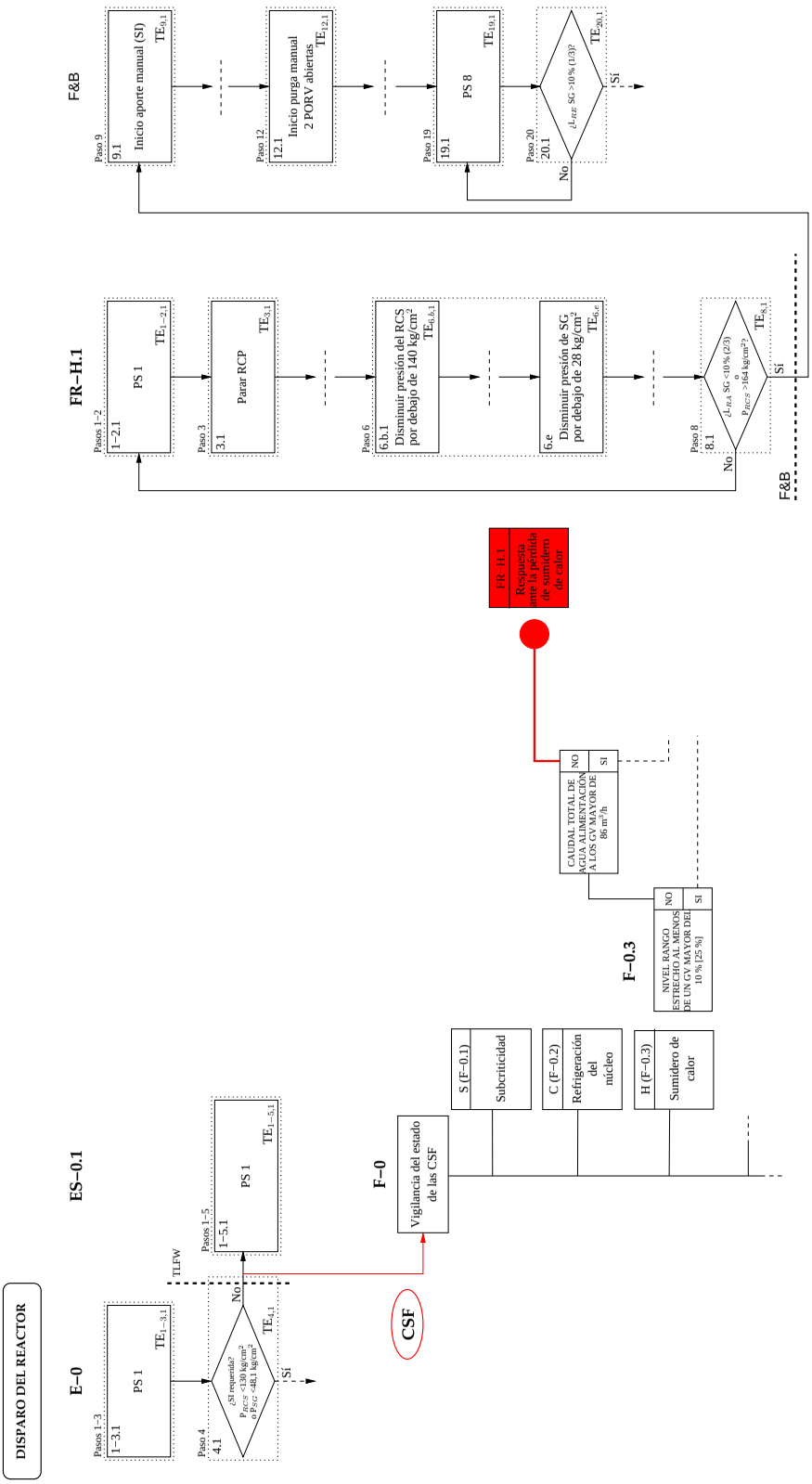


Figura 6.26: Esquema de la secuencia de accidente de TLFW con los EOP asociados.

6.3.2 Resultados obtenidos con la herramienta TRETA/COPMA-III para la secuencia de TLFW

En esta secuencia, se considera la pérdida del agua de alimentación normal por rotura en el colector a los 120 s. de la simulación. A partir de ese momento, el descenso que se produce en el nivel de los SG, provoca el disparo del reactor a los 149,63 s. por señales de bajo nivel en ambos SG, Figura 6.39. Esta misma señal, demanda la actuación del AFWS por señal W. Sin embargo, se postula su fallo en demanda. El disparo de turbina se produce a los 149,74 s. por señal de disparo del reactor. Debido a que el nivel de los SG disminuye de forma rápida en estos primeros segundos, y a que el caudal de agua de alimentación normal se pierde por señal de disparo de turbina, el árbol de vigilancia de las CSF relacionado con el sumidero de calor, Figura 6.26, presentaría condición roja desde los 168 s., Figuras 6.39 y 6.41, esto es, 48 s. tras el disparo del reactor, o lo que es lo mismo, tras la entrada en operación de emergencia. Este hecho conllevaría la transición a la FRG H.1 en dicho momento si en la sala de control se consultase el estado de las FRG en el SPDS, nada más entrar en operación de emergencia. En la simulación de la secuencia, sin embargo, no se ha supuesto la vigilancia de las CSF hasta que el seguimiento de los EOP lo demande, lo que pospone la entrada en la FRG H.1 a los 470 s.

Tras la entrada en operación de emergencia por disparo del reactor, se inicia la ejecución del EOP E-0 a los 300 s., verificando la actuación adecuada del sistema de disparo del reactor y que el núcleo se encuentra subcrítico, pasos 1 a 3 del procedimiento E-0. Tras dichas comprobaciones, se produce la transferencia al EOP ES-0.1, *Procedimiento de recuperación del disparo del reactor*, a los 410 s., al no ser necesaria la actuación de la SI, ya que las presiones del primario y del secundario son superiores a 130 y 48,1 /cm^2, respectivamente. A partir de este momento, y de forma simultánea a la ejecución del EOP ES-0.1, se inicia la vigilancia del árbol de estado F-0 de las CFS. La condición roja del árbol de sumidero de calor (condición que se cumple desde los 166,4 s.), hace que a los 470 s. y tras 60 s. de demora que se han postulado en la comprobación del estado de las CSF en el SPDS, se abandone el procedimiento ES-0.1 y se inicie la ejecución de la FRG H.1, *Respuesta ante la pérdida de sumidero de calor*. Durante este intervalo de tiempo, la bajada acusada del inventario de los SG se sigue produciendo debido al caudal de vapor del alivio al condensador, Figuras 6.38 y 6.42.

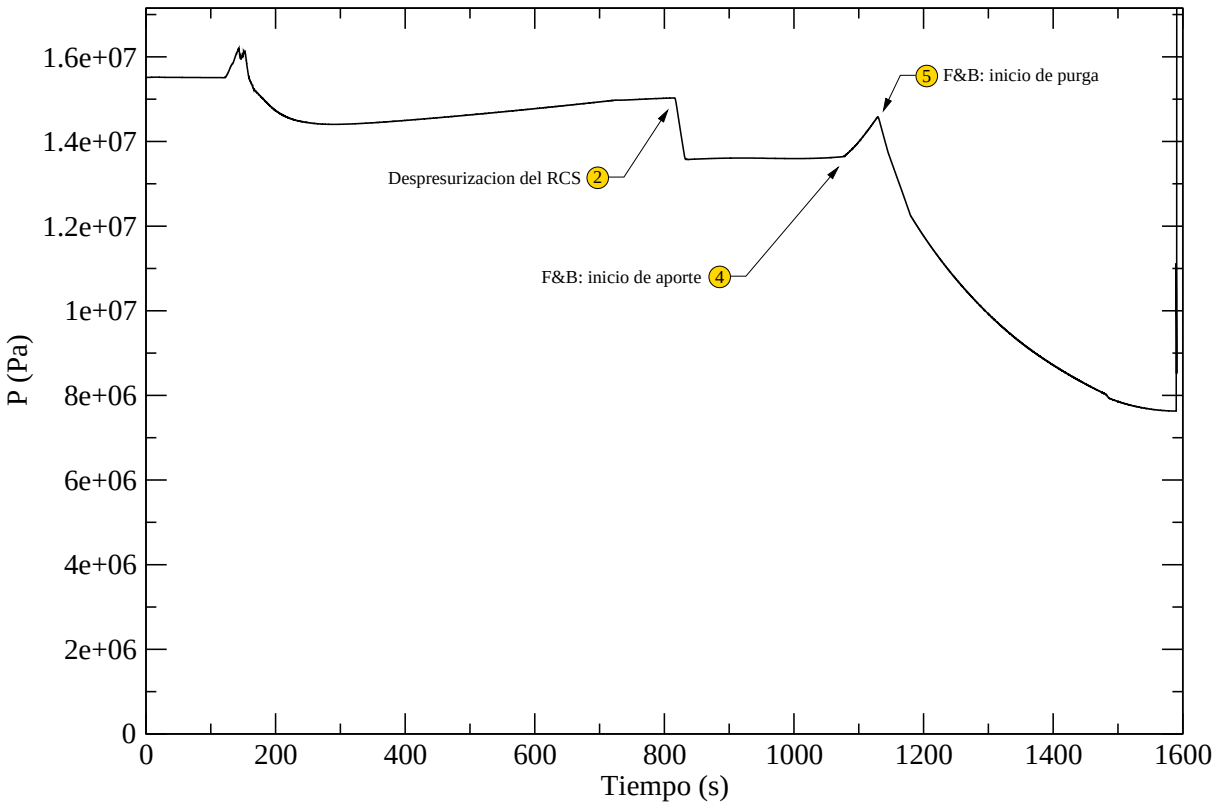
Una vez iniciado el procedimiento FR H.1, la primera actuación modelada del operador consiste en la parada de las RCP a los 725 s., paso 3 del procedimiento, Figura 6.43. La parada de las RCP se considera incondicionalmente, ya que de esta forma se reduce la tasa de pérdida de inventario de los SG al pasar a circulación natural, Figuras 6.33 y 6.44, y eliminar el aporte de calor de las RCP al primario, proporcionando más tiempo a las acciones de recuperación del aporte de inventario a los SG y, por lo tanto, aumentar la posibilidad de evitar la ejecución del F&B.

Las operaciones de intento de recuperación del sumidero de calor mediante el aporte del sistema de agua de condensado, requieren la despresurización del primario y del secundario a presiones inferiores a 140 y 28 kg/cm^2, acciones que se realizan a los 815 y 865 s., Figuras 6.32 y 6.37, instrucciones 6.b y 6.e, respectivamente. Mientras que se realizan estas acciones, el inventario de los SG no ha dejado de disminuir, alcanzándose la condición de inicio de F&B a los 870 s.,

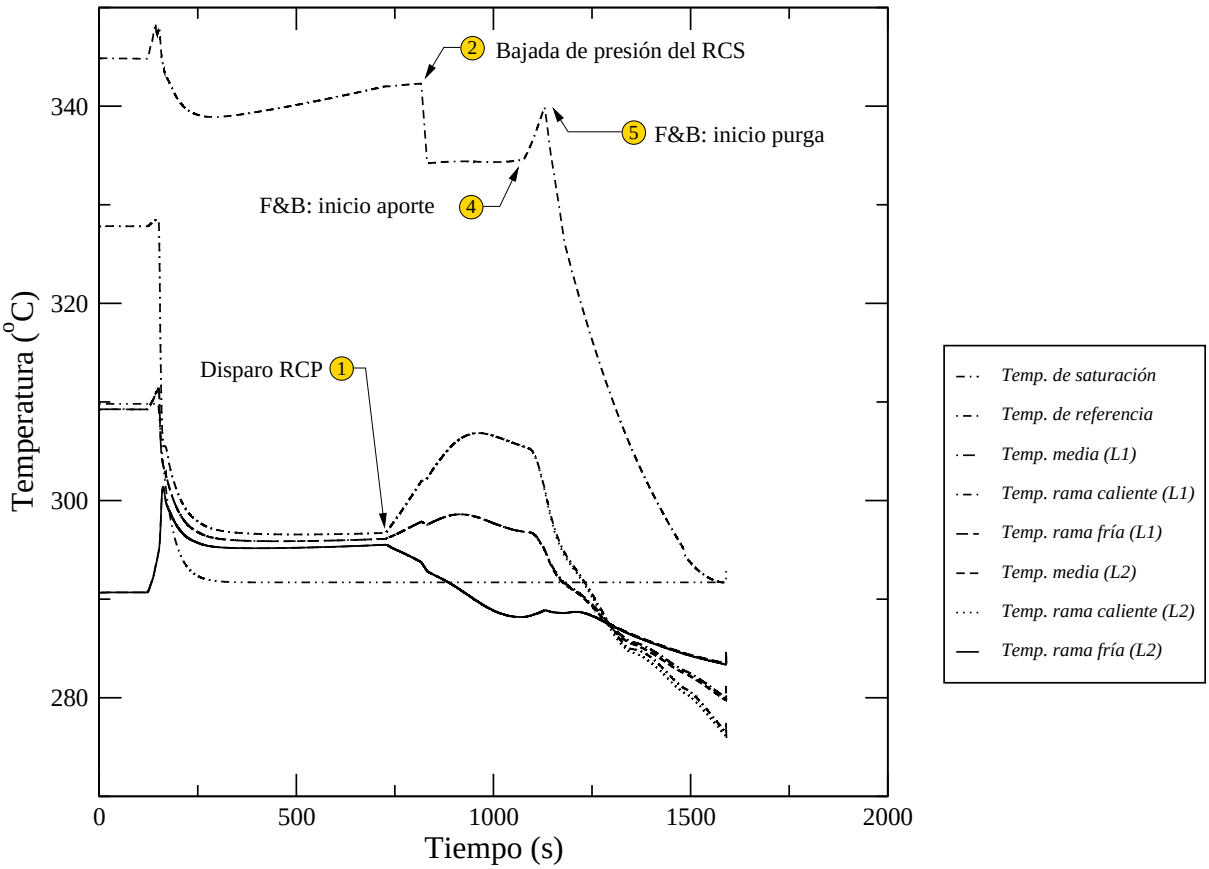
Figura 6.38. Al postular la imposibilidad de la recuperación del AFWS y del aporte mediante las bombas del condensado, la evaluación de dicha condición se realiza a los 975 s., iniciando el aporte al RCS mediante actuación manual de la SI a los 1070 s., paso 9 del procedimiento, Figura 6.35, y la purga del primario a los 1130 s., paso 12 del procedimiento, Figura 6.36. A partir de ese momento, alcanzar la situación de equilibrio dinámico del aporte y la purga depende de los caudales de aporte y purga, y el calor residual, Loomis y Cozzuol (1988).

ACTUACIONES AUTOMÁTICAS	
Tiempo (s.)	**Descripción**
120	Pérdida de agua de alimentación
149,63	Señal de disparo del reactor y de actuación del AFWS por señal de bajo nivel en los SG 1/3 y 2. Fallo en demanda del AFWS
149,74	Disparo de turbina
ACTUACIONES MANUALES / GESTIÓN DEL OPERADOR	
Tiempo (s.)	**Descripción**
166,4	CSF en condición roja (SPDS): terminal FR-H.1 del árbol F-0.3
300	**Entrada en EOP (EOP E-0)**
	Se supone diagnóstico del suceso como una TLFW
410	No se considera necesaria la SI. Subtarea 4.1
	Transferencia al EOP ES-0.1. Subtarea 4.1
	Se inicia la vigilancia de las CSF.
470	**Transferencia al FRG FR-H.1**. Subtarea 1-5.1
725	Disparo manual de las RCP. . Subtarea 3.1
815	Inicio de despresurización del primario. Subtarea 6.b.1
865	Inicio de despresurización del secundario. Subtarea 6.e.1
870	Se cumplen la condición de inicio de F&B
975	Se evalúa la condición de entrada de F&B. Subtarea 8.1
1070,15	Maniobra de F&B: inicio de aporte al RCS. Arranque de los dos trenes de inyección de alta presión del CVCS. Subtarea 9.1
1130	Maniobra de F&B: inicio de purga del RCS. Apertura de dos PORV del presionador. Subtarea 12.1
1500	Se equilibran el aporte y la purga al primario, con enfriamiento del núcleo. Criterio de éxito de F&B alcanzado

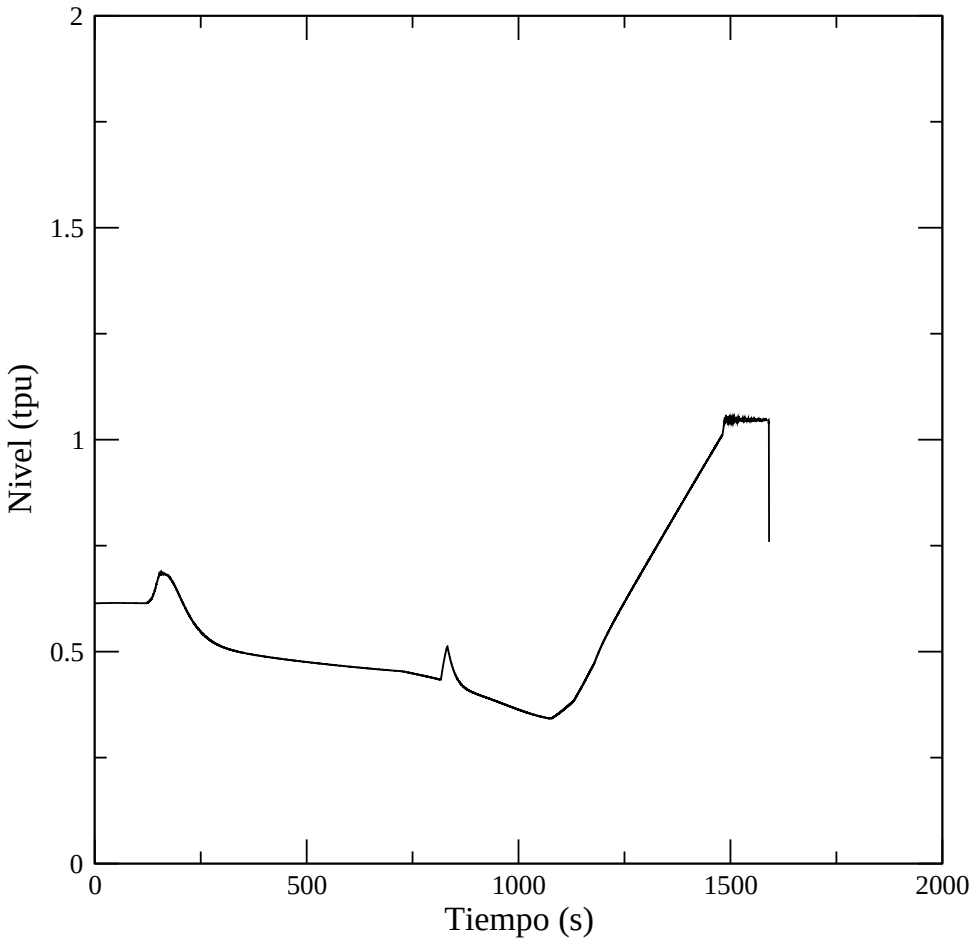
Tabla 6.18: TLFW: secuencia de actuaciones automáticas y manuales.



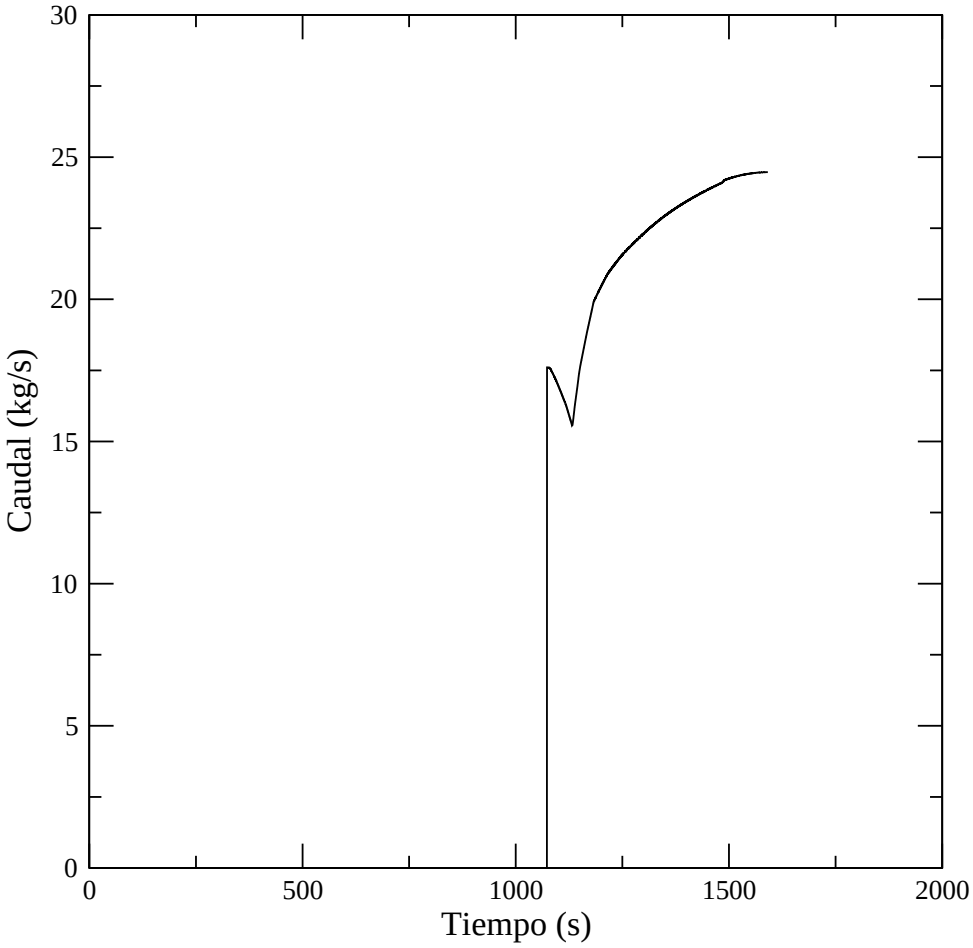
Gráfica 6.32: TLFW: presión en el primario.



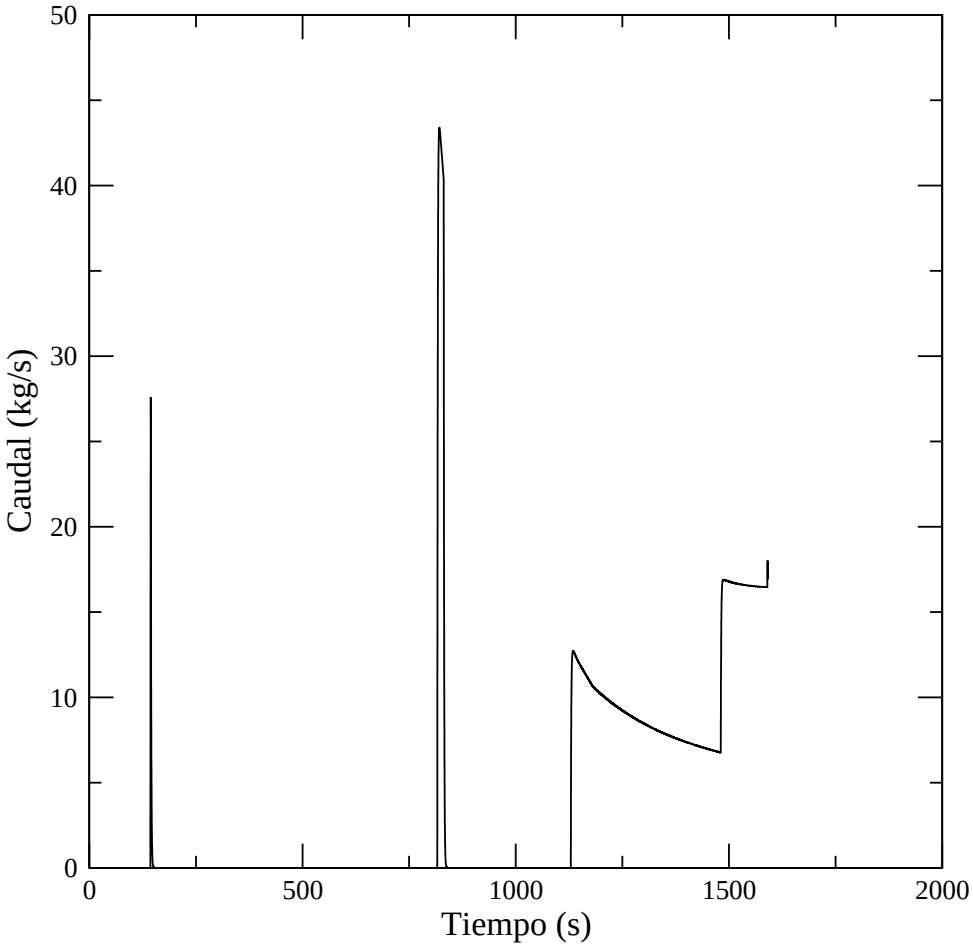
Gráfica 6.33: TLFW: temperaturas en los lazos del primario.



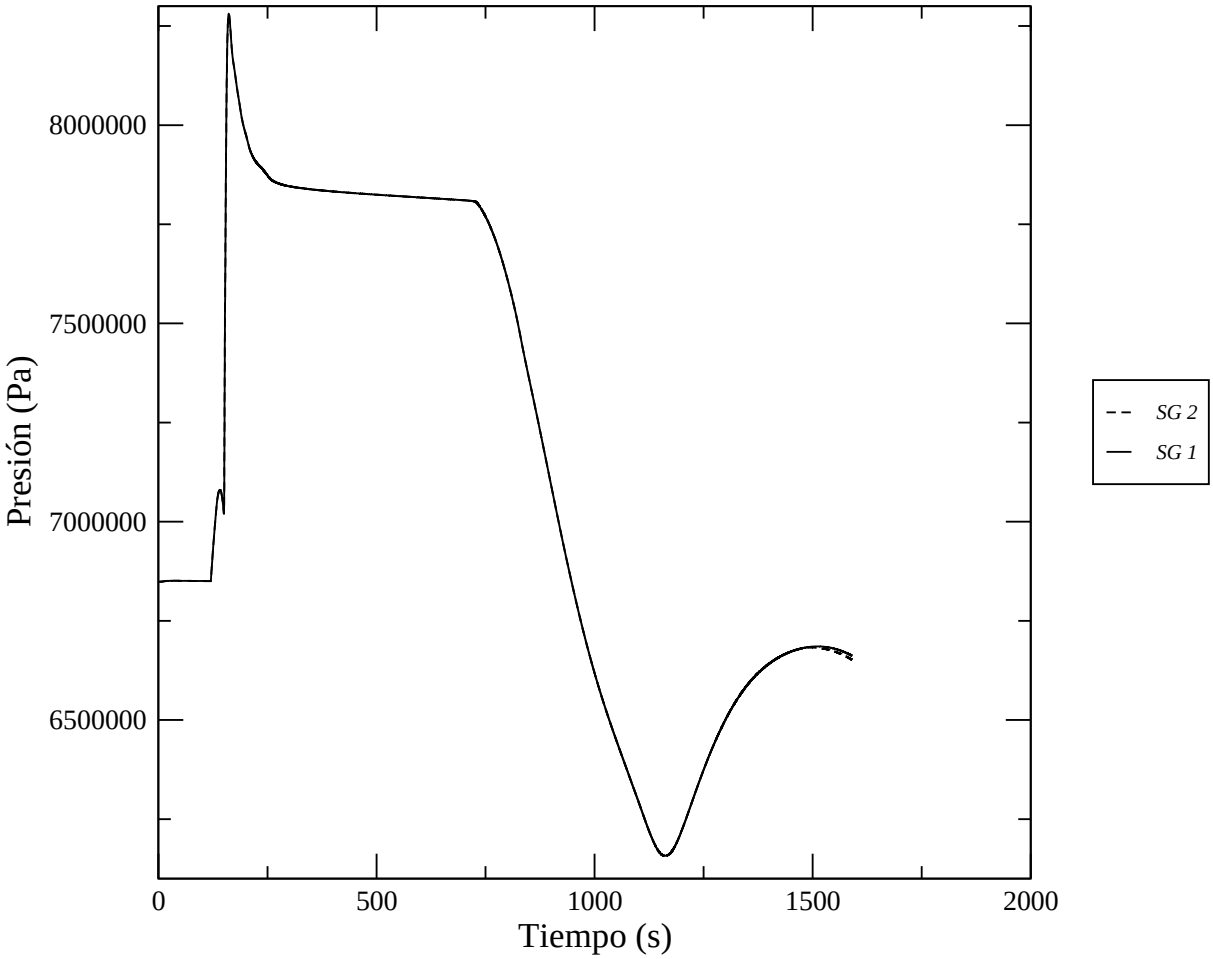
Gráfica 6.34: TLFW: nivel en el presionador.



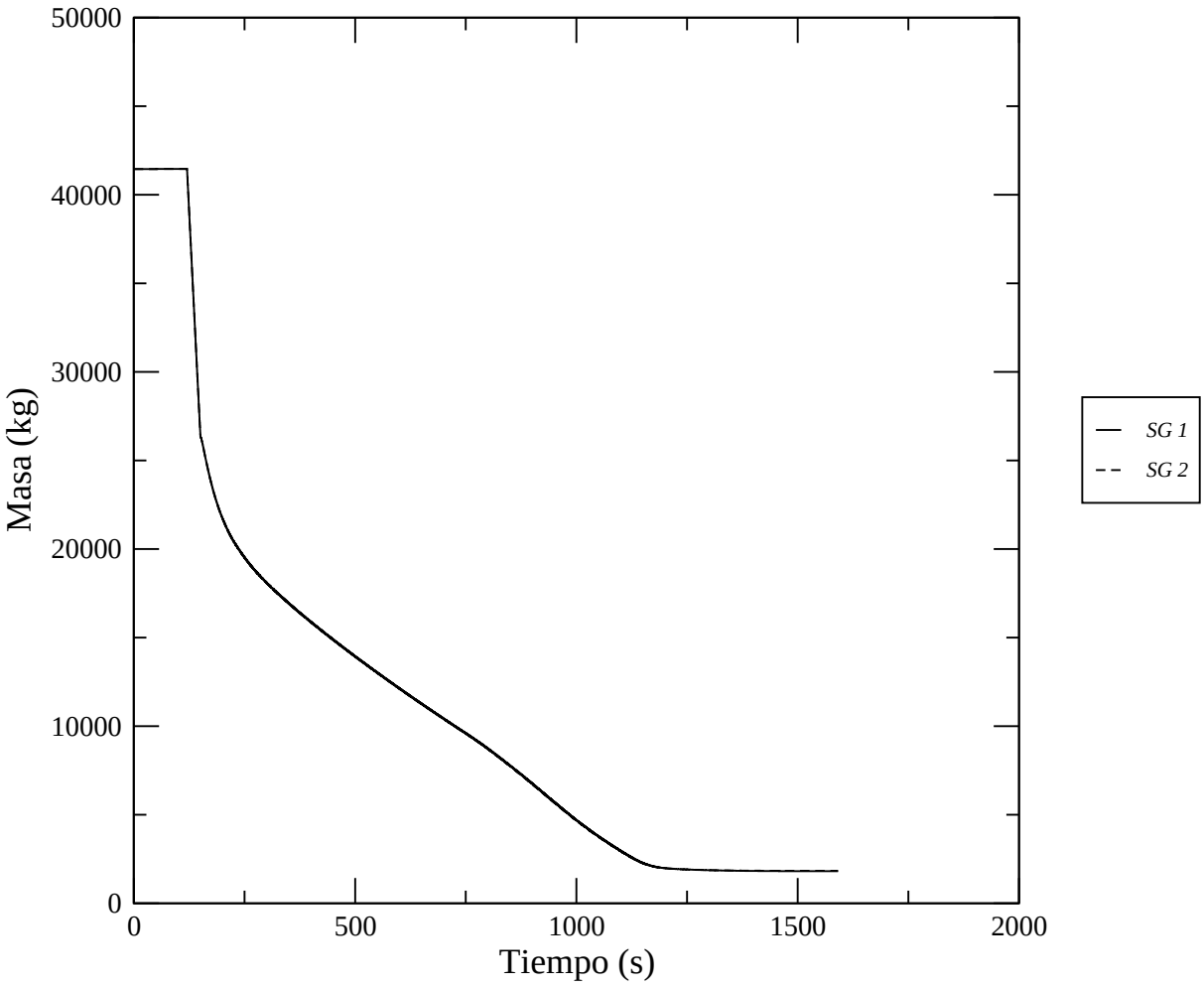
Gráfica 6.35: TLFW: caudal de inyección de seguridad.



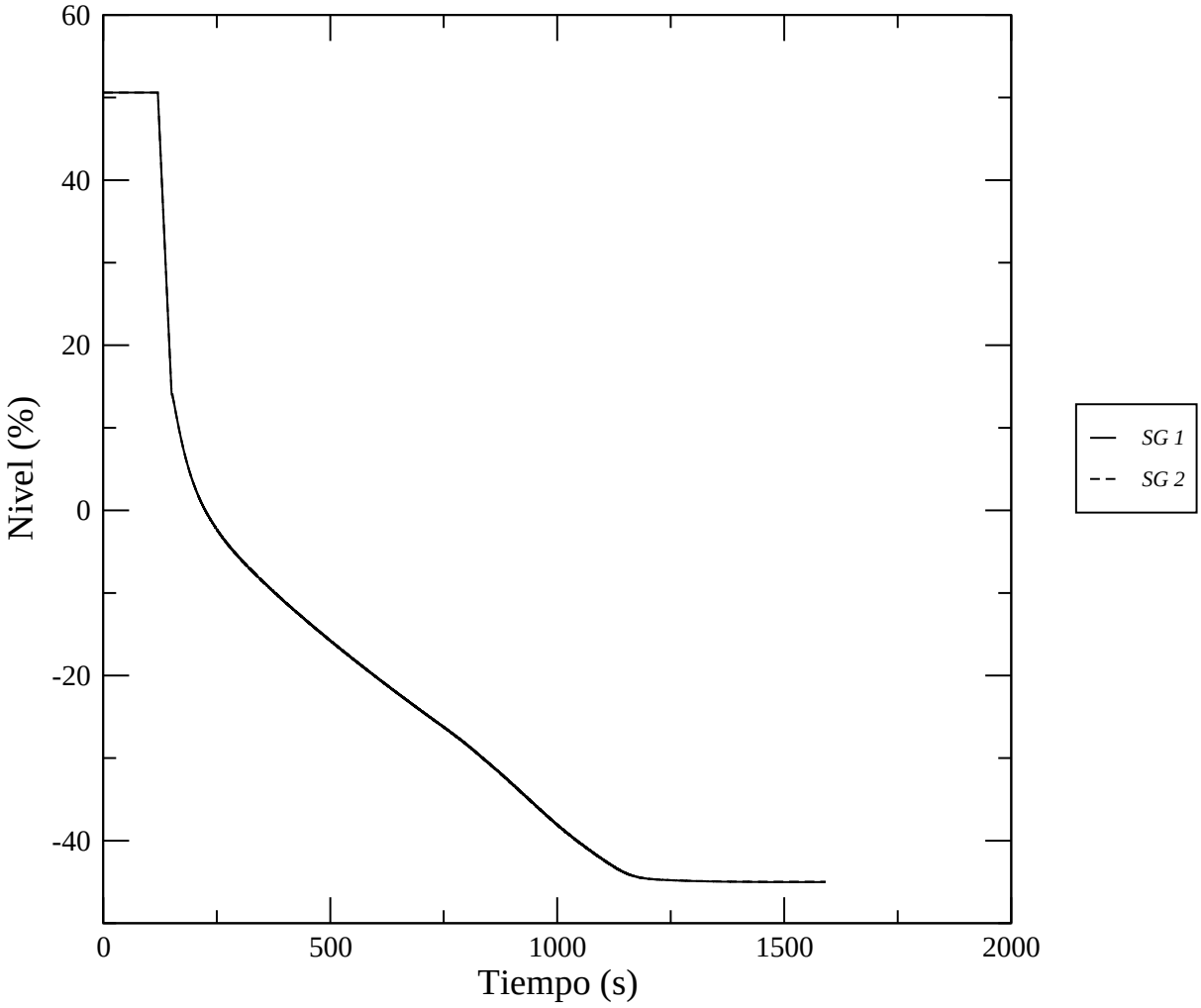
Gráfica 6.36: TLFW: caudal de las válvulas de alivio del presionador.



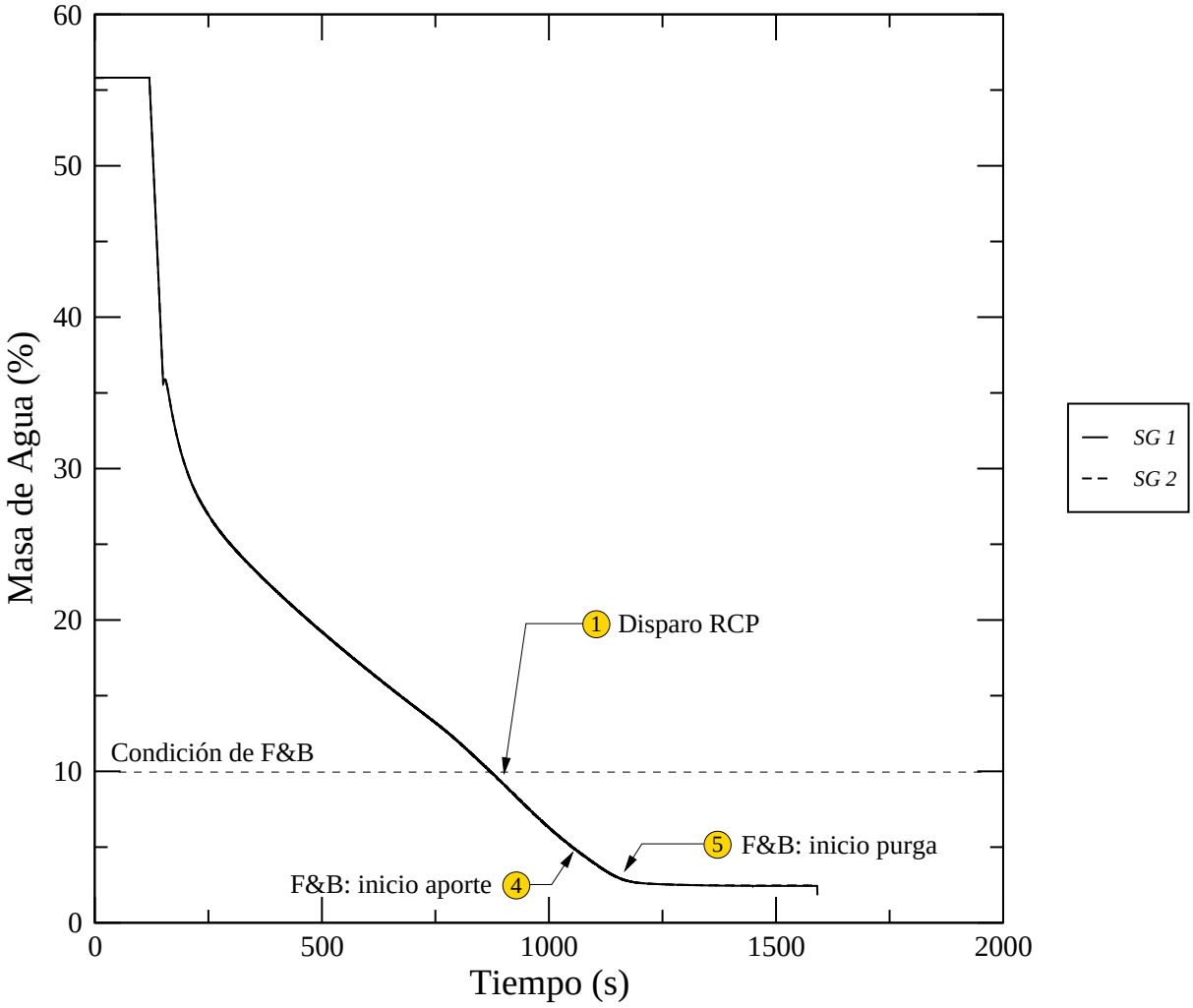
Gráfica 6.37: TLFW: presión en los generadores de vapor.



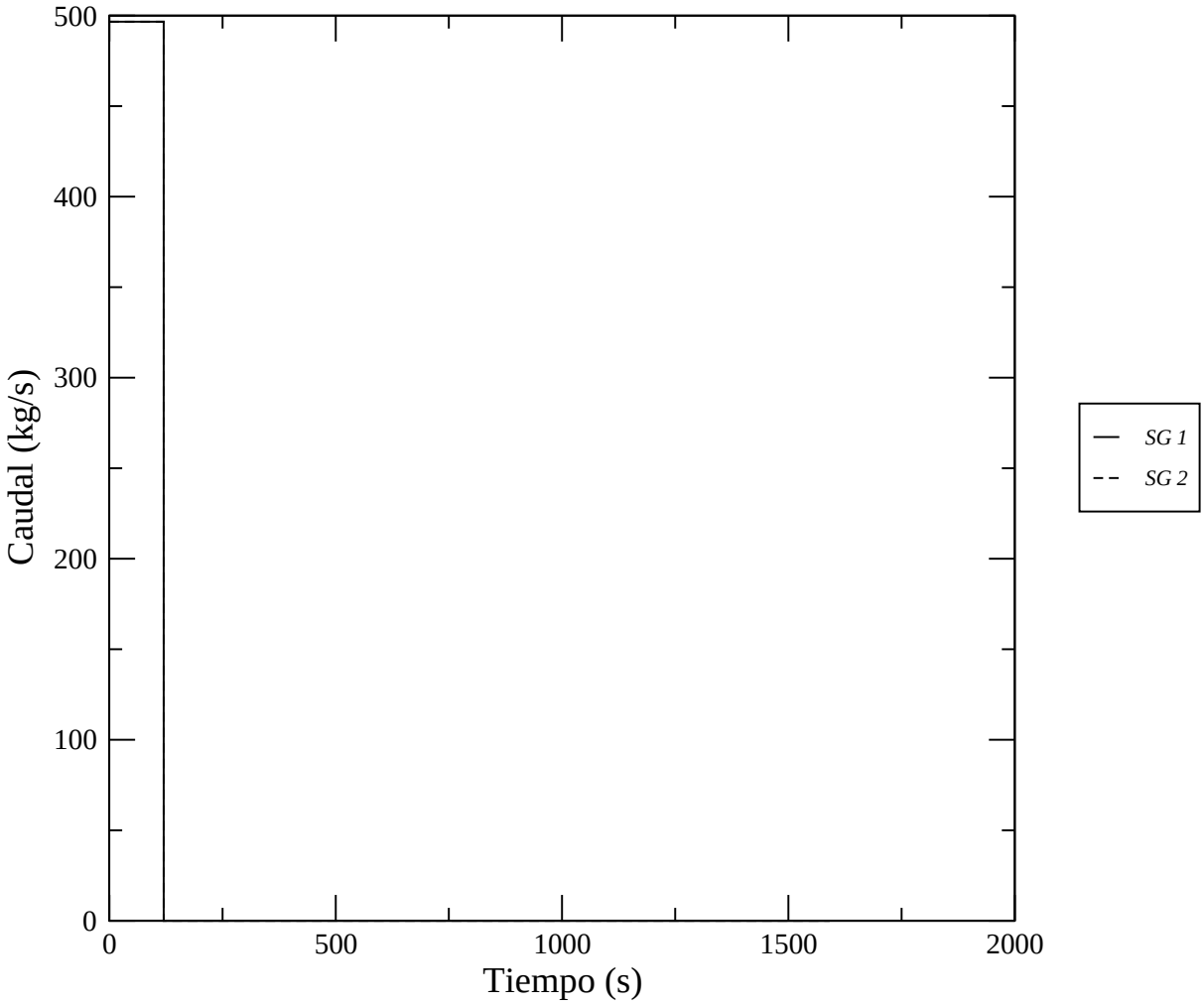
Gráfica 6.38: TLFW: inventario de los generadores de vapor.



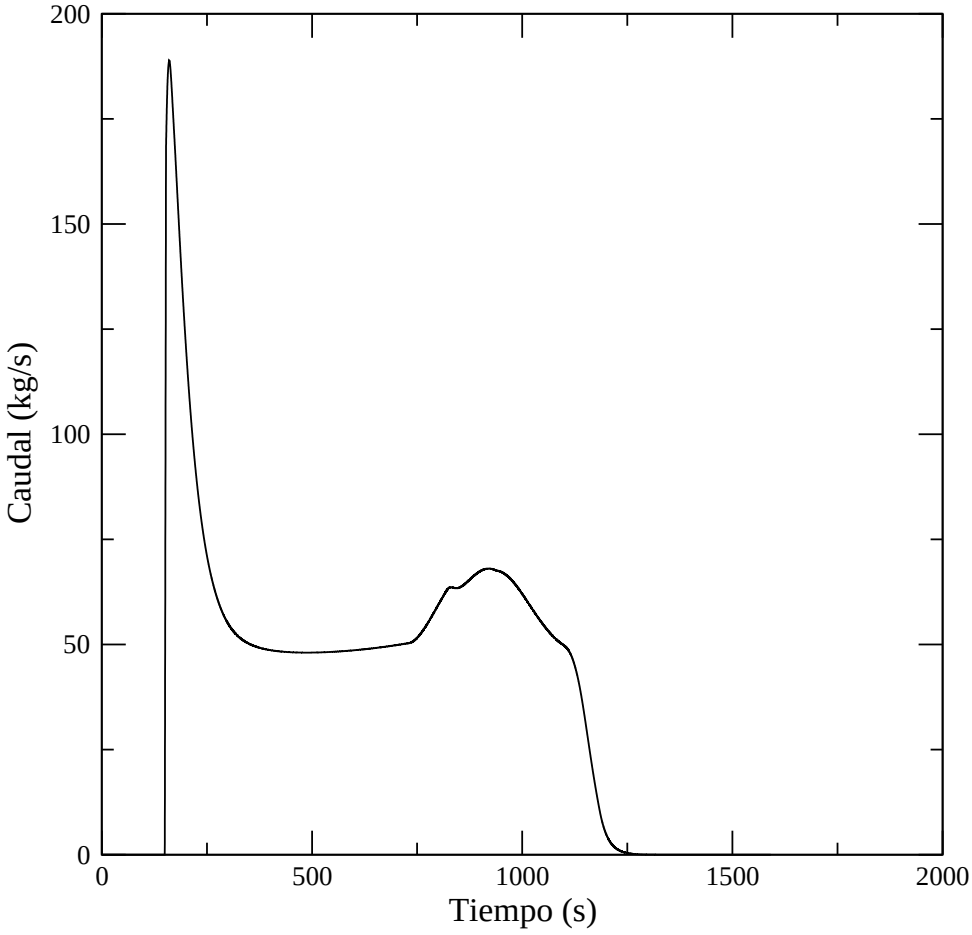
Gráfica 6.39: TLFW: nivel de rango estrecho de los generadores de vapor.



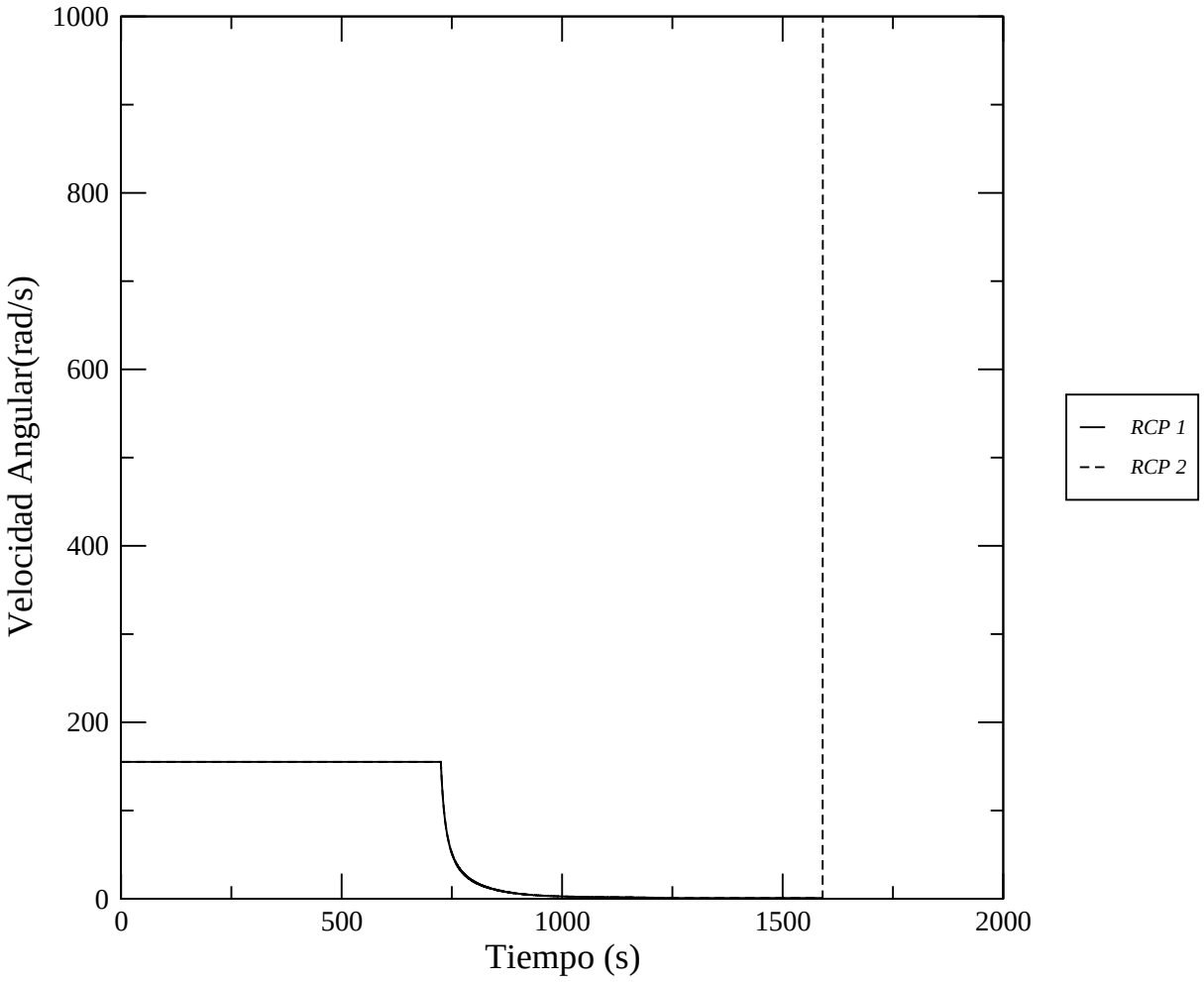
Gráfica 6.40: TLFW: nivel de rango ancho de los generadores de vapor.



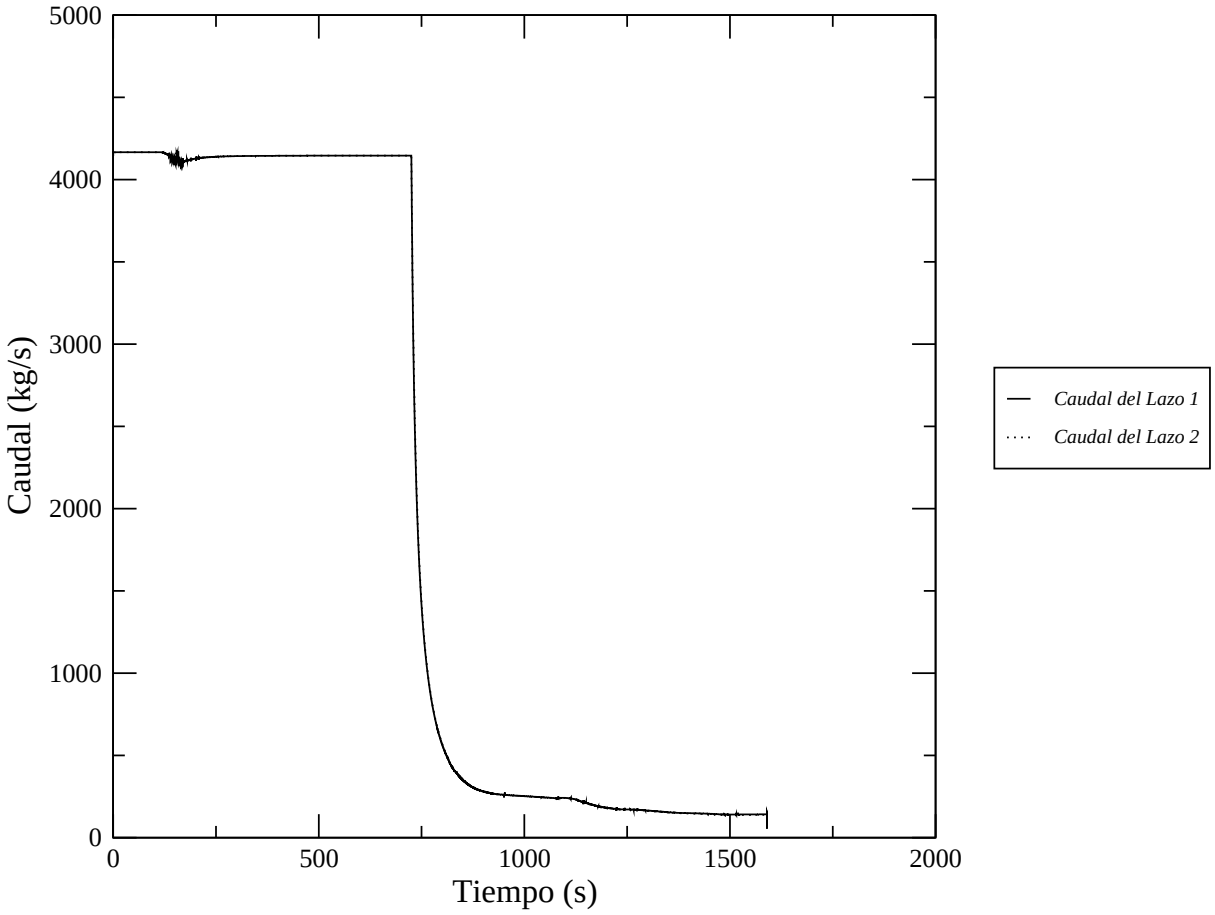
Gráfica 6.41: TLFW: caudal de agua de alimentación de los generadores de vapor.



Gráfica 6.42: TLFW: caudal de alivio al condensador.



Gráfica 6.43: TLFW: velocidad angular de las bombas de refrigeración del reactor.



Gráfica 6.44: TLFW: caudal en los lazos de refrigeración del reactor.

6.4 Conclusiones de la aplicación del simulador integral a las secuencias seleccionadas

En el proceso de aplicación de la herramienta se han consolidado muchos de los aspectos resaltados a lo largo del trabajo, tanto respecto a las limitaciones del modelo de plata y el código TRETA y el simulador de procedimientos COPMA-III, pudiendo ser reiterativos algunos de los comentarios.

6.4.1 Conclusiones relacionadas con la simulación del modelo de planta y el código TRETA

Partiendo de que los resultados obtenidos de la simulación de las secuencias consideras han sido satisfactorios, se debe considerar tal como se comentó en el Capítulo 3, que durante la simulación de los transitorios de verificación del modelo y de las secuencias de aplicación del simulador integral se encontraron varias limitaciones en los modelos y métodos de cálculo del código TRETA:

- No simulaba la degradación de la transferencia de calor en los SG por descubrimiento de tubos al no considerar este fenómeno en el módulo UASG.
- Tanto el llenado como el vaciado del presionador eran singularidades del sistema de ecuaciones implementado en el módulo PRES, que no estaban consideradas. Este módulo realizaba el balance de volúmenes de ambas fases en el presionador sin considerar el volumen total, Expósito (2003).
- Los módulos PIPE presentan gran sensibilidad en el cálculo, siendo frecuentes los fallos de simulación por flujos inversos o falta de convergencia en el caudal transportado. Este hecho se agrava con el acople al modelo de bombas, sobre todo en situaciones de circulación natural.

Tras el estudio de estas limitaciones se implementaron las siguientes soluciones:

- Un modelo lineal de secado de tubos en el módulo de cálculo del coeficiente de transferencia de calor de los generadores de vapor, módulo UASG.
- Modificación de los cálculo del módulo del presionador, reduciendo en caso de llenado el volumen total de las fases al del presionador, reajustando el valor de la presión considerando la compresibilidad de las fases, módulo PRES.

Sin embargo, la realización de las modificaciones necesarias en los módulos PIPE no se plantearon por no ser prioridad del trabajo, pudiéndose considerar:

- La necesidad de incluir modelos bifásicos en los módulos encargados de calcular el transporte de las propiedades termohidráulicas del fluido (módulos PIPEI, PIDED y PIPEM). Esta limitación es de espacial importancia en transitorios con condiciones degradadas de refrigeración o los relacionados con las bajadas de presión rápidas, p. ej. TLFW o LOCA. Para paliar estas deficiencias se podría considerar la implementación de los modelos del código TIZONA.

- Se debe mejorar el modelo de bombas del primario, que en su estado actual impide simular secuencias en las que las que se produzca la pérdida de circulación natural.

En cuanto al modelo de planta desarrollado, tras haber verificado que su comportamiento es adecuado en la simulación de las secuencias de aplicación, solo cabe hacer referencia a la necesidad de realizar un ajuste de los caudales de las PORV del presionador y la SI contra datos de planta o, en su defecto, resultados de simulaciones con modelos de plantas PWR-W realizadas con códigos *best estimate*. Este hecho es fundamental para simular de forma adecuada la fenomenología asociada a la operación de F&B.

6.4.2 Conclusiones relacionadas con la simulación del modelo de procedimientos y el código COPMA-III

Los resultados relacionados con la simulación de los modelos de procedimientos considerados han sido satisfactorios. Sin embargo, y al igual que para el caso del código TRETA, se han detectado ciertas limitaciones:

- Las especificaciones de diseño del núcleo del sistema COPMA-III no consideran la gestión síncrona de las actividades, lo que obliga a tiempos de espera cada vez que se quiere sincronizar la simulación del proceso con la de los procedimientos, prolongando las simulaciones a tiempos a veces prohibitivos. En lo que respecta a la simulación de los tiempos de actuación su impacto no es relevante. El motivo consiste en que cada ciclo de cálculo de TRETA se corresponde con tiempos entre dos y tres órdenes de magnitud inferiores a los considerados en los tiempos de ejecución de los pasos, perdiendo importancia desde este punto de vista la falta de sincronización.

- Las capacidades de computerización de procedimientos son buenas y cubren las especificaciones de la herramienta, aunque se debe mejorar el tratamiento de la jerarquía de los diferentes tipos procedimientos de emergencia, ORG y FRG, y la capacidad de interrumpir la ejecución de procedimientos en función de la prioridad de los mismos, aplicando un control de jerarquía de los mismos. Este aspecto se ha puesto de manifiesto en la simulación de las secuencias de LSLB y TLFW, afectando de mayor a esta última, obligando a que la implementación de las FRG se haga integrada secuencialmente en la ejecución de los ORG, y no en paralelo.

Ambas limitaciones son de gran importancia y, ligadas a que el desarrollo de COPMA-III depende del equipo de desarrollo del HRP, parece necesaria el uso de un simulador de procedimientos diferente. Dentro de las líneas de trabajo actuales se está colaborando con la empresa INDIZEN en el desarrollo de un simulador de procedimientos denominado SIMPROC, específico para la simulación automática de procedimientos. En el Capítulo 7 se explica en detalle en que consiste esta colaboración.

En lo que respecta a la estimación de la carga de trabajo y los tiempos de ejecución de los pasos de los EOP, y al no ser uno de los objetivos de esta tesis, su tratamiento ha sido superficial, cubriendo exclusivamente las necesidades de las simulaciones orientadas para la comprobación de la funcionalidad de la herramienta. Sin embargo, como parte del trabajo realizado, se ha realizado un estudio del tratamiento de estos aspectos, presentando un resumen de los resultados en el Capítulo 7.

Capítulo 7

Conclusiones

Índice

A lo largo de los capítulos que componen esta tesis se ha presentado el desarrollo del simulador integral TRETA/COPMA-III. Esta nueva herramienta se caracteriza principalmente por su modularidad y su capacidad de interconexión con otros códigos. Las especificaciones de la interfase de conexión, desarrollada empleando las librerías SWBus, proporcionan gran flexibilidad a la hora de considerar su acoplamiento con otros simuladores que amplían las capacidades de la herramienta, como por ejemplo, módulos de simulación cognitiva del operador o módulos de cálculo de probabilidades de fallo en las actuaciones registradas en los EOP. El prototipo presentado, en su estado actual, tiene implementada la funcionalidad necesaria para desarrollar simulaciones de procesos físicos en instalaciones industriales considerando la interacción de actuaciones humanas procedimentadas o planeadas.

De forma individual, los diferentes códigos que componen el simulador presentan capacidades avanzadas en sus modelos. Así, el simulador TRETA presenta gran versatilidad a la hora de definir el grado de complejidad en la simulación de los procesos, abarcando en el caso de las centrales nucleares un amplio rango de operación, tanto en operación normal como en situaciones de emergencia. En lo que respecta al simulador COPMA-III, permite la simulación automática de actuaciones humanas procedimentadas o planeadas, es decir, de todas aquellas actuaciones manuales de las cuales se pueda desarrollar un modelo determinista a priori, incluyendo aspectos de tiempos de ejecución y carga de trabajo obtenidos por estudios adicionales.

Respecto al carácter modular de la herramienta, cabe destacar que hace posible incluso la sustitución de los simuladores de proceso o de procedimientos y la implementación de cualquier otro simulador que se considere más apropiado para otras necesidades, mediante la implementación de la API desarrollada, pudiéndose emplear para ello cualquier protocolo de comunicaciones, tanto empleando el código TRETA como la PDB de COPMA-III.

En las secciones de este capítulo se describirán:

- Las limitaciones encontradas en ambos códigos durante la realización de este trabajo, Secciones 7.1 y 7.2.
- La evaluación de la implementación de la interfase de comunicaciones, Sección 7.3.
- Las líneas de trabajo futuras para la resolución de las limitaciones encontradas y la integración de la herramienta en la metodología ISA, Sección 7.4.

7.1 Conclusiones relativas al modelo de planta PWR-W y el simulador TRETA

Durante la realización del trabajo se superaron diversas limitaciones del simulador TRETA realizando mejoras en el código, entre las que se pueden destacar:

- Un modelo lineal de secado de tubos en el módulo de cálculo del coeficiente de transferencia de calor de los generadores de vapor (UASG).

- Ajustes del módulo del cálculo del presionador relacionados con el llenado y vaciado del mismo (PRES).

Sin embargo, otras de las limitaciones encontradas en el código no fueron subsanadas por no ser prioridad del trabajo planteado. Estas han sido:

- La necesidad de incluir modelos bifásicos en los módulos encargados de calcular el transporte de las propiedades termohidráulicas del fluido (módulos PIPEI, PIDED y PIPEM). Esta limitación es de espacial importancia en transitorios con condiciones degradadas de refrigeración o los relacionados con bajadas de presión rápidas, p. ej. TLFW o LOCA. Para paliar estas deficiencias se podría considerar la implementación de los modelos del código TIZONA.

- Se debe mejorar el modelo de bombas del primario, que en su estado actual impide simular secuencias en las que las que se produzca la pérdida de circulación natural.

- Tanto la arquitectura de cálculo de los elementos del modelo de un sistema, como de forma individual, los módulos PIPEI, PIPED y PIPEM, no permiten el cálculo de caudales inversos. Por ello se requiere mejorar estos módulos para que consideren esta posibilidad y plantear una solución a nivel de modelo que permita el paso de información de bloques en orden inverso a la secuencia natural de cálculo del código TRETA.

- La fuerte modularidad del código, el carácter desacoplado de los modelos y su implementación a nivel de cálculo requieren la incorporación de técnicas numéricas de convergencia mediante realimentaciones. En el desarrollo del simulador TRETA se consideraron técnicas numéricas de convergencia unidimensionales, lo que aporta problemas numéricos en las simulaciones. En este sentido se tendría que considerar la posibilidad de mejorar estas técnicas dotándolas de carácter vectorial, empleando los métodos SIMPLEX o técnicas SIMPLEX mejoradas, mediante el uso del algoritmo de Powell, la familia de métodos denominados *Direction set methods* mejorados mediante aceleradores lineales tipo Sargent o algoritmos estadísticos, como por ejemplo los algoritmos genéticos, Expósito y Queral (2005b). Además, deben mejorarse los criterios de relajación de la convergencia en los ciclos de cálculo del modelo.

- Se debería incorporar la capacidad de variar el paso de tiempo en el *driver*, ajustándolo a las necesidades de simulación. En su defecto se debería implementar esta capacidad en el módulo encargado del cálculo del presionador, PRES.

- Incorporar la posibilidad de guardar puntos temporales de la simulación por petición del usuario, mediante la especificación de las peticiones en el fichero de entrada.

En cuanto al modelo de planta desarrollado, se puede considerar:

- El ajuste de los parámetros de los controles manuales para una simulación más realista de los tiempos y el modo de control humano.

- La mejora y la validación más extensiva de los modelos de sistemas frontales, especialmente el SIS y el CVCS, y de válvulas tanto del primario como del secundario, así como el ajuste de los caudales del modelo de alivio de vapor al condensador.

- El desarrollo de un modelo de balance de planta.

7.2 Conclusiones relativas al modelo de EOP-W y el simulador COPMA-III

Los aspectos a destacar, en cuanto al empleo del sistema COPMA-III para la simulación de los procedimientos dentro de los objetivos de la herramienta desarrollada, son:

- Las especificaciones de diseño del núcleo del sistema COPMA-III no consideran la gestión síncrona de las actividades, lo que obliga a tiempos de espera cada vez que se quiere sincronizar la simulación del proceso con la de los procedimientos. Inviable para la mayoría de las aplicaciones del simulador integral.

- Complejidad excesiva en el núcleo, tanto de funcionamiento como de configuración, que no proporciona funcionalidad para las aplicaciones consideradas.

- El sistema COPMA-III tiene en desarrollo la capacidad de guardar y recuperar puntos de la simulación, siendo esta capacidad un requerimiento para la integración del simulador en la metodología ISA. Cabe destacar que el código TRETA ya la tiene implementada.

- Las capacidades de computerización de procedimientos son buenas y cubren las especificaciones de la herramienta, aunque se debería mejorar el tratamiento de la jerarquía de procedimientos (ORG y FRG), la gestión de las condiciones de vigilancia (instrucciones MONITOR) de forma que su vigencia esté ligada a las actividades padres, capacidad de interrumpir la ejecución de procedimientos en función de la prioridad de los mismos, aplicando un control de jerarquía de los mismos. Adicionalmente, se debería considerar la necesidad de implementar un modelo de toma de decisiones, para cubrir las necesidades de simulación de procedimientos relacionadas con los terminales de color amarillo en la vigilancia de las CSF.

- Inclusión de probabilidades de fallo al considerar las acciones del operador y posibilidad de modificar, mediante un simulador externo, los valores por defecto de los parámetros TASKEXEC y TASKLOAD.

- Durante el seguimiento de los procedimientos, el sistema de simulación de procedimientos debe ser capaz de considerar posibles desviaciones del operador durante el seguimiento de los procedimientos, tal y como se exponen en el Capítulo 1, a saber: EoC, EoO, etc.

Una de las limitaciones más importante es que su desarrollo depende de terceros, en este caso del equipo de desarrollo del sistema COPMA-III del HRP. Dentro de las líneas de trabajo futuras, se está trabajando en las especificaciones de una solución propia para la simulación de procedimientos de operación, denominado SIMPROC, producto de la experiencia adquirida en este y otros trabajos. Los detalles de dicho proyecto se comentan de forma resumida en la Sección 7.4.

De forma general, durante la computerización de los EOP, se han encontrado problemas a la hora de determinar estrategias de actuación del operador en ciertos pasos de los procedimientos, Sección 4.5:

- Actuaciones específicas que están estipuladas formalmente pero su contenido no consta en los procedimientos escritos.
- Actuaciones delegadas al criterio del operador.
- Vigilancia de condiciones de operación de sistemas, estado de componentes o variables físicas.
- Las actuaciones de control sobre variables físicas.
- La computerización de precauciones y notas del EOP escrito.
- Pasos cuya computerización presentan dificultades en su interpretación y/o computerización.

Todos estos problemas recibieron soluciones parciales que deben ser verificadas en futuros trabajos.

Durante todo el trabajo realizado con los EOP surgió la necesidad de fundamentar el modelado de los mismos en fuentes de información menos teóricas, ya que la aproximación empleada mediante el uso de los propios procedimientos y sus bases no es realista. Este tipo de consideraciones es habitual en los trabajos de evaluación de los procedimientos y, principalmente, para modelar los procedimientos de forma adecuada se requiere la consulta a los instructores de operadores y a los propios operadores, principalmente a los SRO, ya que son los que ejecutan los procesos de toma de decisiones y distribuyen las tareas.

En la parte correspondiente a la estimación de la carga de trabajo de las actuaciones registradas en los EOP y los tiempos de ejecución, en los últimos años se han realizado diversidad de aproximaciones para la estimación y evaluación de la carga cognitiva y física de los procedimientos. Se pueden destacar los trabajos de Park y Jung (2006a), Park et al. (2001 2002 2004ab) para la evaluación de la carga cognitiva mediante técnicas de encuestas a operadores, como la NASA-TLX, o técnicas más objetivas, como el flujo de cantidad de información o la cuantificación de la entropía asociada a cada paso. Otros trabajos emplean la teoría de la información para estimar estos parámetros, Kim et al. (2003). Dentro de las metodologías relacionadas con los tiempos de ejecución de actuaciones, se puede destacar GOM, Card et al. (1983). Esta metodología ha

sido aplicada para la evaluación de tiempo de ejecución de instrucciones de procedimientos mostrando validez contra datos de simuladores de sala de control, Da~Silva et al. (2003).

Además de considerar estos aspectos, y tal como se a justificado durante la realización del trabajo, en la simulación de factores relacionados con el operador se hace necesaria la implementación de modelos de toma de decisiones. Se han realizado multitud de aproximaciones a la simulación automatizada de este aspecto, p. ej. Choi et al. (1998), y de hecho, se deberán considerar a la hora de implementar un módulo de simulación de procesos cognitivos en el simulador de procedimientos.

7.3 Conclusiones relativas a la interfase de comunicaciones del simulador integral

La funcionalidad de la interfase es suficiente para los objetivos de la herramienta tal y como se consideraron en su desarrollo inicial, demostrando sus capacidades para la simulación de procedimientos.

Dentro de los desarrollos futuros se debe considerar:

- Las mejoras propuestas, principalmente las relacionadas con el sistema COPMA-III, implican la necesidad de implementar en la interfase de comunicaciones la capacidad de gestionar la información relativa a la ejecución de los procedimientos atendiendo a su jerarquía.
- El hecho de que la interfase de comunicaciones se haya desarrollado empleando una librería de comunicaciones dependiente de terceros, la librería SWBus del HRP, podría conllevar limitaciones en el desarrollo de mejoras futuras. Por ello, al igual que se ha comentado para el sistema COPMA-III y relacionado con la definición de especificaciones del desarrollo propio SIMPROC, se debería considerar la implementación de la API desarrollada en una solución no condicionada por estos aspectos dentro de ese proyecto.

7.4 Líneas de trabajo consideradas a corto y medio plazo

Las principales líneas de trabajo que se van a llevar a cabo relacionadas con este trabajo son la colaboración del autor de esta tesis, en calidad de miembro de los equipos de investigación, en dos proyectos subvencionados por instituciones nacionales:

- «Investigación de sistema basado en XML de simulación de procedimientos para plantas nucleares (SIMPROC)», dentro del programa PROFIT del Ministerio de Industria.
- «*Incorporation of the Stimulus-Driven Theory of Probabilistic Dynamics in the Integrated Safety Analysis Methods (STIM)*», dentro del programa CICYT del Ministerio de Ciencia y Tecnología.

7.4.1 Desarrollo del simulador de procedimientos SIMPROC

La empresa Indizen Technologies y el departamento de Sistemas Energéticos de la Universidad Politécnica de Madrid (DSE), con la asistencia técnica del Consejo de Seguridad Nuclear, está trabajando en la definición, diseño y desarrollo de una herramienta informática, denominada SIMPROC, que incorpora una tecnología propia para la simulación de procedimientos de operación en entornos industriales. Este proyecto está enmarcado dentro de la convocatoria 2006 del programa PROFIT, financiado por el Ministerio de Industria de España, y tiene una duración de dos años, entre 2007 y 2008.

El objetivo principal es aprovechar toda la experiencia previa y, en este sentido, el trabajo realizado en esta tesis servirá de referencia para el apoyo en las tareas de definición de las especificaciones de diseño de simulador SIMPROC.

7.4.2 Incorporación del simulador integral en la metodología ISA

Por último, dentro del marco del proyecto CICYT "*Incorporation of the Stimulus-Driven Theory of Probabilistic Dynamics in the Integrated Safety Analysis Methods (STIM)*", se considera la necesidad de incorporar el simulador integral en el conjunto de herramientas en que se basa la metodología ISA, elemento central de dicho proyecto, Figura 7.1. Este proyecto está subvencionado por el Ministerio de Ciencia y Tecnología de España, con una duración de tres años, entre 2006 y 2009.

En la actualidad no existe todavía una teoría rigurosa que tenga en cuenta de forma coherente los factores probabilistas y deterministas a la hora de verificar los márgenes de seguridad en la aplicación de la regulación informada por el riesgo. Dicha teoría requeriría del uso coherente de los argumentos probabilistas y deterministas o, dicho de otra forma, una armonización de los principios del DBA y del PSA, como ha sido puesto de manifiesto en numerosas publicaciones, Bley et al. (1992) y Siu (1994). Entre las posibles candidatas se encuentra la *Theory of Probabilistic Dynamics* (TPD), Devooght (1998), Devooght y Smidts (1992 1996), en su versión mejorada mediante la inclusión de la denominada teoría de estímulos, denominada la *Stimulus-Driven Theory of Probabilistic Dynamics* (SDTPD), Izquierdo y Labeau (2004).

Este proyecto tiene por objetivo definir e integrar la SDTPD en el ámbito de la metodología de Análisis Integrado de la Seguridad (*Safety Integrated Analysis*, ISA). El estado de desarrollo de los diferentes elementos que componen la metodología ISA es, Figura 7.1:

Planificador de Eventos (B1)

Encargado de desplegar las ramas del árbol en función de la evolución dinámica del accidente y de los criterios de desarrollo de secuencias que se definan. El gestor DENDROS permite la modularización y paralelización del proceso de generación de árboles. El cálculo de la probabilidad de fallo de la contención se realiza por medio del código EVNTRE, mediante el tratamiento de árboles de sucesos de progresión de accidentes. Los datos de entrada se formulan como preguntas sobre la probabilidad de ocurrencia de los fenómenos

que conducen al fallo de la contención. Cada una de éstas puede tener dos o más respuestas, en función de qué fenómenos se hayan satisfecho. La selección de la probabilidad para cada rama se basa, por tanto, en la satisfacción de ciertas funciones lógicas.

Modelo de Planta (B2)

Adaptado para la ejecución de la simulación en árbol que demanda el planificador de eventos. Para aplicaciones en APS nivel 1, se dispone de TRETA para plantas PWR-W, TIZONA para plantas BWR-GE, así como BABIECA para modelos de propósito general, que pueden combinarse con los anteriores. BABIECA dota al sistema, además, de capacidad de acoplamiento con otros códigos. Por ejemplo, se han acoplado los modelos de PWR y BWR con MAAP para extender las capacidades de simulación al contexto del accidente severo. Los códigos anteriores son usados con el propósito de confirmar la completitud del árbol de sucesos. Una vez identificada una cierta secuencia como relevante desde el punto de vista de seguridad se puede reproducir, con mayor nivel de detalle, con otros códigos como RELAP5 o MELCOR, y en el futuro con TRACE cuando se encuentre disponible. Adicionalmente, se utilizan técnicas de post-proceso desarrolladas para confirmar la calidad de los resultados de estos códigos de detalle. También se puede usar el post-proceso para generar datos de entrada a modelos de cálculo más simplificados que permitan realizar análisis más extensos o más rápidos sin perder a cambio la consistencia con el cálculo detallado.

Modelo de Operador (B3)

Elemento basado en el trabajo realizado en esta tesis, considerando la posibilidad de integrar tanto COPMA-III como el simulador SIMPROC, cuando este último se encuentre desarrollado. Ambos programas permiten la simulación automatizada de los procedimientos de operación de emergencia, y su integración en la metodología ISA correrá a cargo del equipo de investigación del DSE, del cual el autor es miembro.

Calculador de Probabilidades (B4)

Hasta el momento, el cálculo de probabilidades efectuado en las aplicaciones realizadas se ha hecho de manera enteramente desacoplada y posterior al cálculo dinámico. Sin embargo, se han desarrollado algoritmos alternativos de cálculo basados en Diagramas Binarios de Decisión (*Binary Decision Diagrams*, BDD), para su incorporación en un nuevo módulo del sistema. También se han desarrollado herramientas para convertir la información disponible de los árboles de fallo de los APS al formato BDD.

Integración del riesgo (B5)

Se ha desarrollado un código de cálculo para la estimación de términos fuente y en la propagación de incertidumbres, incorporándose la integración de resultados y elaboración de medidas de riesgo de los APS-2. Por otra parte, los conceptos, los principios básicos y el planteamiento teórico del método ISA han sido establecidos en cooperación con la Universidad Libre de Bruselas (*Université Libre de Bruxelles*, ULB), sobre la base de los conceptos y desarrollos de la TPD y la extensión teórica denominada SDTPD, que pretende estudiar la evolución dinámica de sistemas sujetos a transiciones discretas que

alteran dicha evolución dinámica y a su vez dependen de ella, ya que las transiciones sólo se pueden producir en determinadas condiciones dinámicas y con probabilidades que también dependen del estado dinámico. Este conjunto de ecuaciones matemáticas proporciona la evolución temporal de las probabilidades de las secuencias y se encuentra realizado en gran parte, estando pendientes algunos desarrollos. La integración de esta teoría en el marco de la ISA y su verificación mediante su aplicación práctica a un ejemplo concreto constituyen el cometido fundamental de este proyecto.

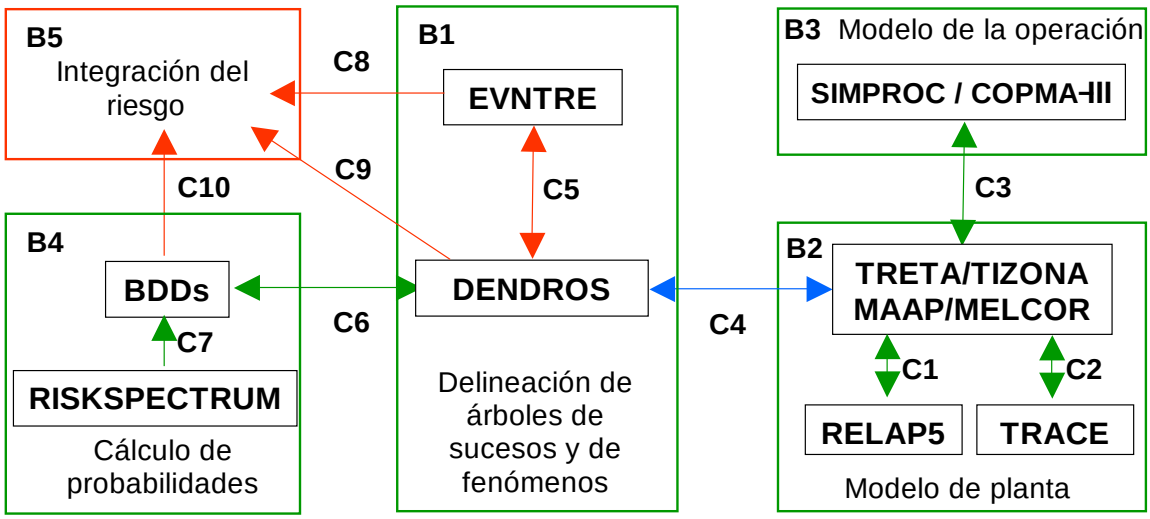


Figura 7.1: Estado actual de desarrollo de los elementos que componen la metodología ISA y su relación (tareas hechas en azul, en realización en verde y por realizar en rojo).

Bibliografía

A. Alemberti, P. Castagna, S. Nilsen y A. Santinelli. AUTOGRAPH: From free text to graph structured representation: a tool to improve quality and understanding of procedures logical flow. Es una publicación interna., 1996.

ANS. Time response design criteria for safety-related operator actions. En *ANSI/ANS*, number 58.8. American Nuclear Society, 2001.

A. Baddeley. Is Working Memory Still Working? *American Psychologist*, 56:849–864, 2001.

A. D. Baddeley. *Human Memory: Theory and Practice*. Oxford University Pres, 1990.

A. D. Baddeley y G. J. Hitch. Working Memory. En G.A. Bower, editor, *Recent advances in learning and motivation*, volúmen 8, pág. 47–90. Academic Press, 1974.

L. Bainbridge. Ironies of Automatization. *Automatica*, 19:775–779, 1983.

Ø. Berg y S. Nilsen. The Computerized Procedure System COPMA-III used in Human Factors Experiments. 2002.

J. A. Bernard. Applications of artificial intelligence to reactor and plant control. *Nuclear Engineering and Design*, 113:219–227, 1989.

M. O. Bes y C. W. Johnson. Towards a Framework for the Use of Cognitive Models to Analyse Accidents. En Safeware Engineering Corporation, editor, *Second Workshop on Human Error, Safety and Systems Development*, Seattle, USA, 1998.

R. Bisio, E. Hulsund y S. Nilsen. Brief introduction to the COPMA-III tool. Informe técnico, Institute for Energy Technology, 2000.

R. Bisio, E. Hulsund y S. Nilsen. Brief introduction to the COPMA-III tool. Artículo de publicación interna, 2005.

D. Bley, S. Kaplan y D. Johnson. The strengths and limitations of PSA: where we stand. *Reliability Engineering and System Safety*, 38:3–26, 1992.

D. C. Bley y J. W. Stetkar. The significance of sequence timing to human factors modeling. En *Human Factors and Power Plants, Conference Record for 1988 IEEE Fourth Conference*, pág. 259–267, 1988.

E. Borgonovo, C.L. Smith, G.E. Apostolakis, S. Deriot y J. Dewailly. Insights from using influence diagrams to analyze precursor events. En *International Congress of Probabilistic Safety Assessment and Maintenance*, 2000.

J. D. Bumgardner, R. C. Lloyd, N. E. Moffitt, B. F. Gore y T.V. Vo. Auxiliary Feedwater System Risk-Based Inspection Guide for the McGuire Nuclear Power Plant. Informe técnico NUREG/CR-5830, Pacific Northwest Laboratory, 1994. PNL-7784.

M. Byrne y S. Bovair. A working memory model of a common procedural error. *Cognitive Science*, 21:31–61, 1997.

P. C. Cacciabue. Human factors impact on risk analysis of complex systems. *Journal of Hazardous Materials*, 71:101–116, 2000.

P. C. Cacciabue. A Methodology of Human Factors Analysis for Systems Engineering: Theory and Applications. *IEEE transactions on systems, man and cybernetics - Part A: Systems and humans*, 27(3):325–339, 1997a.

P. C. Cacciabue. A Methodology of Human Factors Analysis for Systems Engineering: Theory and Applications. En *IEEE Transaction on Systems, Man and Cybernetics*, 1997b.

P. C. Cacciabue, F. Decortis, B. Drozdowicz, M. Masson y J. P. Nordvik. COSIMO: A Cognitive Simulation Model of Human Decision Making and Behavior in Accident Management of Complex Plants. *IEEE Transactions on systems, man and cybernetics*, 22(5):1058–1074, Septiembre/Octubre 1992.

S.K. Card, T.P. Moran y A.P. Newell. *The Psychology of Human-Computer Interaction*. Erlbaum, 1983.

M. Champ y Y. Cornille. Evaluation of feed and bleed cooling mode in case of total loss of feedwater on 900 MWe PWR. En *CSNI specialist meeting on international coolant system depressurization*, 1989.

B. Chandrasekaran, R. Bhatnagar y D. D. Sharma. Real-time disturbance control. *Communication of the ACM*, 34(8):33–47, Agosto 1991.

S. H. Chang, K. S. Kang, S. S. Choi, H. K. Jeong y C. U. Yi. Development of the on-line operator aid system OASYS using a rule-based expert system and fuzzy logic for nuclear power plants. *Nuclear Technology*, 112:266–294, 1995.

Chun-Chang Chao y Chin-Jang Chang. Development of a dynamic event tree for pressurized water reactor steam generator tube rupture event. *Nuclear Technology*, 130:27–38, Abril 2000.

J-P. Chatry y F. Poizat. A safety breakthrough: EDF computerized emergency operation approach. En *7th International Conference on Nuclear Engineering, ICONE-7037*. ICONE, 1999.

S. S. Choi, S. H. Chang y D. H. Lee. Automating strategies of emergency operation shutdown in pressurized water reactors. *IEEE Transactions on Nuclear Science*, 45(1):17–29, 1998.

N. Chomsky. *Syntactic Structures. The Hague: Mouton*. The Hague: Mouton, 1957.

CNA. Procedimientos de opereracion de emergencia. Rev. 1.C.4. Informe técnico RC/C4/5, CN de Almaraz, 2000.

K. M. Corker y B. R. Sinith. An architecture and model for cognitive engineering simulations analysis. Application to advanced aviation automation. En *AIAA Computing in Aerospace 9 Conference*, 1993.

N. Cowan. The magical number 4 in short-term memory: A reconsideration of mental storage capacity. *Behavioral and Brain Sciences*, 24(1):87–185, 2001.

CSNI. Critical operator actions: human reliability modeling and data issues. Informe técnico NEA/CSNI/R(98)1, CSNI, 1998.

CSNI-PWG5. Assessing human reliability in nuclear power plants. Informe técnico 75, CSNI, 1983.

N. G. Da Silva, M. A. Bayout y M. J. Coelho. Evaluation of the NPP operator cognitive workload during an emergency. En *Transactions of the 17 International Conference on Structural Mechanics in Reactor Technology (SMIRT 17)*, 2003.

V. N. Dang. Human Reliability Analisys (HRA). Applications and Methods Development. Informe técnico, Paul ScherrerInstitute, 2006.

V. N. Dang. *Modeling operator cognition for accident sequence analysis: Development of an operator-plant simulation*. Tesis doctoral, Massachusetts Institute of Technology, 1996.

V. N. Dang y B. Reer. Decision and commission errors - From identification to quantification issues. En *IEEE seventh human factors meeting*, 2002.

J. Devooght. The Current Practice of PRA in relation with Dynamic Reliability. En *Workshop on Dynamic Reliability*, volúmen 1, pág. 19–20, Maryland, Septiembre 1998.

J. Devooght y C. Smidts. Probabilistic Reactor Dynamics-I: The Theory of Continuous Event Trees. *Nuclear Science and Engineering*, 111:229–240, 1992.

J. Devooght y C. Smidts. Probabilistic dynamics as a tool for dynamic PSA. *ReliabilityEngineering and System Safety*, 52:185–196, 1996.

E. Dougherty. Guest editorial: Human reliability analysis - where shouldst thou turn? *Reliability Engineering and System Safety*, 29(3):283–300, 1990.

E. Dougherty. Context and human reliability analysis. *ReliabilityEngineering and System Safety*, 41:25–47, 1993.

EPA. New ways to prevent chemical incidents. Informe técnico 550-B-99-012, Environmental Protection Agency (EPA), 1999.

A. Expósito. Simulación numérica de transitorios de despresurización en sistemas no adiabáticos. Informe técnico, Universidad Politécnica de Madrid. Departamento de Sistemas Energéticos, 2003.

A. Expósito y C. Queral. Computerización del EOP E-0 de la CN de Almaraz con el código COPMA-III. Informe técnico, ETSI de Minas, 2004a.

A. Expósito y C. Queral. Computerización del EOP E-2 de la CN de Almaraz con el código COPMA-III. Informe técnico, ETSI de Minas, 2004b.

A. Expósito y C. Queral. Descripción de los EOP de un PWR-W. Informe técnico, ETSI de Minas, 2004c.

A. Expósito y C. Queral. Computerización del EOP E-1 de la CN de Almaraz con el código COPMA-III. Informe técnico, ETSI de Minas, 2005a.

A. Expósito y C. Queral. Implementación de técnicas de optimización multidimensional para mejorar la convergencia de cálculo del modulo PIPEIB del código TIZONA. Informe técnico, ETSI de Minas, 2005b.

A. Expósito y C. Queral. Prueba de comunicaciones COPMA-III/TRETA mediante la simulación de secuencias de rotura del secundario. Informe técnico, ETSI de Minas, 2006a.

A. Expósito y C. Queral. Modelo de planta de un PWR-W para el código TRETA. Informe técnico, ETSI de Minas, 2006b.

A. Expósito, C. Queral y I. Gonzalez. Análisis de las secuencias de rotura en el secundario. Informe técnico, Universidad Politécnica de Madrid, DSE., 2004.

F. R. Farmer. Siting criteria - a new approach. En *Symposium on the containment and siting of nuclear power reactors,* volúmen 3-7, pág. 303–329. International Atomic Energy Agency, 1967. SM-89/34.

FCFRNS. Safety Guide 2.8: Probabilistic safety analyses (PSA). Informe técnico, Finnish Centre For Radiation And Nuclear Safety (FCFRNS), 1996.

L. Festinger. *A theory of cognitive dissonance*. Stanford University Press, 1957.

R. E. Fields. *Analysis of erroneous actions in the design of critical systems*. Tesis doctoral, University of York, 1999.

P. M. Fitts. The information capacity of the human motor system in controlling the amplitude of movement. *Journal of Experimental Psychology*, 47(6):381–391, 1954.

P.M. Fitts. Human engineering for an effective air-navigation and traffic-control. Informe técnico, Ohio State University. Division of Anthropology and Psychology. Committee on Aviation Psychology., 1951.

J. Forester, C. Thompson, M. Drouin y E. Lois. Human action perspectives based on individual plant examination results. En *International topical meeting on probabilistic safety assessment - moving toward risk based regulation*, 1996.

J. Forester, A. Kolaczkowski y E. Lois. Evaluation of Human Reliability Analysis Methods Against Good Practices. NUREG 1842, NRC, 2006.

S. Freud. *The psychopathology of everyday life*. Pelican Books, 1940.

Y. Fujita, H. Sakuta y I. Yanagisawa. Human reliability analysis using simulated human model. En *Proceedings of the 2nd International Conference on Probabilistic Safety Assessment Methods*, 1993.

H. Furukawa, T. Inagaki y Y. Niwa. Operator's situation awareness under different levels of automation; Evaluations through probabilistic human cognitive simulations. En IEEE, editor, *Conference on Systems, Man, and Cybernetics, 2000 IEEE International*, volúmen 2, pág. 1319–1324, 2000.

D. Gertman, H. Blackman, J. Marble, J. Byers y C. Smith. The SPAR-H HumanReliability Analysis Method. NUREG/CR-6883 INL/EXT-05-00509, INL, 2005.

D. I. Gertman, W. E. Gilmore, W. J. Galyean y M. R. Groh. Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR). Informe técnico NUREG/CR-4639, Nuclear Regulatory Commission, 1988.

D. I. Gertman, B. P. Hallbert, M. W. Parrish, M. B. Sattision, D. Brownson y J. P. Tortorelli. Review of findings for human performance contribution to risk in operating events. NUREG NUREG/CR-6753, INEEL, Agosto 2001.

D. I. Gertman, B. P. Hallbert y D. A. Prawdzik. Human Performance Characterization in the Reactor Oversight Process. NUREG/CR NUREG/CR-6775, Nuclear Regulatory Commission, 2002.

M. Green. *Root Cause Analysis*. Human Reliability Associates, 1991.

M. Green y A. D. Livingston. Procedures development: common deficiencies and possible solutions. En *Operating procedures for nuclear power plants and their presentation*. Agencia Internacional de la Energía Atómica (IAEA), 1992.

M. Grozdanovic y Z. Jankovic. Interaction Between Human Factors And The Automatization. *Working and Living Environmental Protection*, 2(2):101–113, 2002.

R.E. Hall, J.R. Fragola y J.W. Wrethall. Post Event Human Decision Errors: OperatorAction Tree / Time Reliability Correlation. Informe técnico NUREG/CR-3010, United States Nuclear Regulatory Commission, 1982.

L. N. Haney, H. S. Blackman y B. J. Bell. Comparison and Application of Quantitative Human Reliability Analysis Methods for the Risk Methods Integration and Evaluation Program (RMIEP). NUREG/CR NUREG/CR-4835, Idaho National Engineering Laboratory, 1989.

G. W. Hannaman y A. J. Spurgin. Systematic Human Action Reliability Procedure (SHARP). Informe técnico NP-3583, Electric Power Research Insitute, 1984.

C. R. Hardy, S. M. Randall y A. Singh. A Software Tool for Integrated Accident Analysis of Nuclear Plant and Operator Response. *IEEE Transactions on Nuclear Science*, 41(4):1394–1399, 1994.

J. C. Higgins, J. M. O'Hara, P. M. Lewis, J. J. Persensky y J. Bongarra. Development of a Risk Screening Method for Credited Operator Actions. En *7th Human Factors Meeting*, 2002.

J.C. Higgins, J.M. O'Hara, P.M. Lewis, J.J. Persensky, J.P. Bongarra, S.E. Cooper y G.W. Parry. Guidance for the review of changes to human actions. Final report. Informe técnico NUREG-1764, BNL, Febrero 2004.

J. W. Hines y R. E. Uhrig. Trends in computational intelligence in nuclear engineering. *Progress in Nuclear Energy*, 46(3-4):167–175, 2005.

S. Hirschberg. Human reliability analysis in probabilistic safety assessment for nuclear power plants. Technical opinion papers 4, CSNI, 2004.

S. Hirschberg. Dependencies, Human Interactions And Uncertainties In Probabilistic Safety Assessment. Final Report of the NKA Project RAS 470. Informe técnico, Nordic liaison committee for atomic energy (NKA), 1990. ISBN 87 7303 454 1.

S. Hirschberg. Human Reiability Analisys (HRA). Informe técnico, Paul ScherrerInstitute, 1999.

E. Hollnagel. Looking for errors of omission and commission or *The Hunting of the Snark* revisited. *Reliability Engineering and System Safety*, 68:135–145, 2000.

E. Hollnagel. Human reliability assessment in context. *Nuclear Engineering and Technology*, 37(2):159–166, Abril 2005a.

E. Hollnagel. *International Encyclopedia of Ergonomics and Human Factors. 2nd Edition.*, capítulo Part 3. Performance Related Factors: Human Reliability Analysis, pág. 466–469. Taylor & Francis, 2005b.

E. Hollnagel. *Human Computer Interaction and Complex Systems*, capítulo The Phenotype of Erroneous Actions: Implications for HCI Design. Academic Press, Inc., Orlando, FL, USA, 1991. ISBN 0127426604.

E. Hollnagel. *Human Reliability Analysis: Context and Control (Computers and People)*. Academic Press, 1994. ISBN: 0123526582.

E. Hollnagel. A cognitive task analysis of the SGTR scenario. Informe técnico RAK-1(96)R3, NKS, Abril 1996.

E. Hollnagel. *Cognitive Reliability and Error Analysis Method*. Elsevier, 1998.

E. Hollnagel y A. Bye. Principles for modelling function allocation. *International Jornal of Human-Computer Studies*, 52:253–265, 2000.

E. Hollnagel y D. D. Woods. Cognitive systems engineering: New wine in new bottles. *International Journal of Man-Machine Studies*, 18:583–600, 1983.

E. Hollnagel, P. C. Cacciabue y J-C Rouchet. The use of integrated system simulation for risk and reliability assessment. En *7th International Symposium on Loss Prevention and Safety Promotion in the Process Industry*, 1992.

A. Hornaes y J. E. Hulsund. The EOP visualization module integrated into the plasma on-line nuclear power plant safety monitoring and assessment system. *Nuclear Technology*, 135: 123–130, 2001.

J. Hortal. Conection of Copma-II with a simmulation code. A simple example. Informe técnico, Consejo de Seguridad Nuclear, 2002.

J. Hortal. Conexión del sistema COPMA-II con códigos de simulación. Informe técnico Revisión 1. STN/MOSI/IN/23/96, Consejo de Seguridad Nuclear, 1996a.

J. Hortal. Conexión del sistema COPMA-II con códigos de simulación. Informe técnico CSN/PIN/MOSI/9606/19, Consejo de Seguridad Nuclear, 1996b.

J. Hortal y S. Nilsen. Procedure V&V by simulation using Copma-III. Transferring past experience. 2002.

HRP. *COPMA-II user's manual. Rev. 2.00*. Institutt for EnergiteTeknikk, HRP, 1995.

HRP. The Software Bus user's guide. Institutt for EnergiteTeknikk, HRP, 2002a.

HRP. http://www.external.hrp.no/swbus, 2002b.

K. S. Hsueh y A. Mosleh. The development and application of the accident dynamic simulator for dynamic probabilistic risk assessment of nuclear power plants. *Reliability Engineering and System Safety*, 52:Elsevier, 1996.

A. A. Husseiny, Z. A. Sabri, D. Packer, J. W. Holmes, S. K. Adams y R. J. Rodriguez. Operating procedure automation to enhance safety of nuclear power plants. *Nuclear Engineering and Design*, 110:277–297, 1989.

IAEA. Safety Assessment and Verification for Nuclear Power Plants. SAFETY GUIDE NS-G-1.2, International Atomic Energy Agency, 2001.

IAEA. Implementation of accident management programmes in nuclear power plants. Safety report series 32, IAEA, 2004.

IAEA. Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1). Safety Series 50, IAEA, 1992.

IAEA. Database on operator support systems (OSSDB) in nuclear power plants: status evaluation. Informe técnico IAEA-IWG-NPPCI-96/8, IAEA, 1996.

IAEA. Good practices with respect to the development and use of nuclear power plant procedures. Informe técnico IAEA-TECDOC-1958, IAEA, 1998.

J. M. Izquierdo. TRETA: a general simulation program with application to transients in Nuclear Power Plants. *Revista de la SNE*, October 1987.

J. M. Izquierdo y P.E. Labeau. The stimulus-driven theory of probabilistic dynamics as a framework for probabilistic safety assessment. En *PSAM7/ESREL04 conference*, pág. 14–18, Berlin, Junio 2004.

J. M. Izquierdo, G. Cojazzi, E. Meléndez y M. Sánchez. The DYLAM-TRETA Package. Informe técnico 1.92.111 ISE/IE 2358/92, Joint Research Centre (Ispra), 1994.

Z. Jakubowski y D. Beraha. An expert system - Based aid for analysis of emergency operating procedures in NPPs. En Nuclear Society of Slovenia, editor, *III Regional Meeting: Nuclear Energy in Central Europe*. Nuclear Society of Slovenia, Septiembre 1996.

W. D. Jung, J. W. Kim y J. J. Ha. A Study on Development of the Step Complexity Measure for Emergency Operating Procedures Using Entropy Concepts. Informe técnico KAERI/TR-1794/2001, KAERI, 2001.

M. Kaarstad, K. Kirwan, B. Follesø, T. Endestad y B. Torralba. Human error - the first pilot study. Informe técnico HWR-417, OECD Halden Reactor Project, 1994.

M. Kaarstad, K. Follesø, S. Collier, G. Hauland y B. Kirwan. Human error - the second pilot study. Informe técnico HWR-421, OECD Halden Reactor Project, 1995.

D. Karin. *Cognitive Error Analysis in Accident and Incident Investigation in Safety-Critical Domains*. Tesis doctoral, Department of Computing Science. University of Glasgow., 2002.

A. Keller. *Teoría general del conocimiento*. Herder, 1988.

J. H. Kim, S. J. Lee y P. H. Seong. Investigation on Applicability o Information Theory to Prediction of Operator Performance in Diagnosis Tasks at Nuclear Power Plants. *IEEE Transactions on Nuclear Science*, 50:1238–1252, 2003.

J. W. Kim, J. Wondea y J. Park. A systematic approach to analyzing errors of commission from diagnosis failure in accident progression. *Reliability Engineering and System Safety*, 89(2): 137–150, 2005.

M. C. Kim y P. H. Seong. An analytic model for situation assessment of nuclear power plant operators based on Bayesian inference. *Reliability Engineering and System Safety*, XX:1–13, 2005. In press.

M. C. Kim y P. H. Seong. A computational method for probabilistic safety assessment of I&C systems and human operators in nuclear power plants. *Reliability Engineering and System Safety*, 91:580–593, 2006.

B. Kirwan. Human Error Identification in Human Reliability Assessment. Part 1: Overview of Approaches. *Applied Ergonomics*, 23(5):299–318, 1992a.

B. Kirwan. Human Error Identification in Human Reliability Assessment. Part 2: Detailed Comparison of Techniques. *Applied Ergonomics*, 23(6):371–381, 1992b.

K. D. Kohlhepp. *Evaluation of the use of engineering judgments applied to analytical Human Reliablity Analysis (HRA) methods*. Tesis doctoral, Texas A&M University, 2005.

J. Lacuna. Análisis y simulación de transitorios en centrales nucleares de agua a presión mediante el sistema de simulación TRETA. Aplicación a los casos de disparo de turbina y sobrevelocidad de bombas del primario. Proyecto fin de carrera, Departamento de Ingeniería Nuclear, Universidad Politécnica de Madrid., 1999.

J. M. Lanore, J. L. Caron, A. Ellia-Hervy y J. L'Henoret. Interaction between thermal/hydraulics, human factors and system analysis for assessin feed and bleed risk benefits. En *International SNS/ENS/ANS topical meeting on probabilistic safety assessment and risk management*, 1987.

J. M. Lanore, S. Charron, F. Jeffroy y P. Probst. Improvement of feed and bleed actuation. En *Proceedings of ICON5: 5th International Conference on Nuclear Engineering*, 1997.

K. P. LaSala. Human Performance Reliability: A Historial Perspective. *IEEE Transactions on Reliability*, 1998.

S. J. Lee y P. H. Seong. Development of automated operating procedure system using fuzzy colored petri nets for nuclear power plants. *Annals of Nuclear Energy*, 31:849–869, 2003.

S. J. Lee y P. H. Seong. Development of automated operating procedure system using fuzzy colored petri nets for nuclear power plants. *Annals of Nuclear Energy*, 31:849–869, 2004.

M. Legaud, A. Villemeur y A. Olliot. *Anticipated and Abnormal Plant Transients in Light Water Reactors*, volúmen 2, capítulo Operator actions following abnormal transients: Tests on simulators, pág. 1169–1176. Plenum Press, New York, 1984.

G. G. Loomis y J. M. Cozzuol. Decay Heat Removal Using Feed-and-Bleed for U.S. Pressurized Water Reactors. Informe técnico NUREG/CR-5072, Idaho National Engineering Laboratory, 1988. EGG-2526.

B. O. Y. Lydell. Human reliability methodology. A discussion of the state of the art. *Reliability Engineering and System Safety*, 36:15–21, 1992.

A. P. Macwan. *Methodology for analysis of operator errors of commission during nuclear power plant accidents with application to probabilistic risk assessement.* Tesis doctoral, University of Maryland, 1992.

A. P. Macwan, K.S. Hsueh y A. Mosleh. An approach to modeling operator behavior in integrated dynamic accident sequence analysis. En *Use of Probabilistic Safety Assessment for Operational Safety PSA'91*, number IAEA-SM-321/4, 1991.

P. Marsden. *Human Factors in Nuclear Safety*, capítulo Procedures in the Nuclear Industry, pág. 99–116. Taylor & Francis, 1996.

P. Marsden y M. Green. Optimizing procedures in manufacturating systems. *International Journal of Industrial Ergonomics*, 17:43–51, 1996.

K. L. Mc Fadden. Risk models for analyzing pilot-error at US airlines: a comparative safety study. *Computers and Industrial Engineering*, 44:581–593, 2003.

D. Meister. A Comparative Analysis of Human Reliability Models. Contract n00024-71-c-1257, Naval Sea Systems Command, 1971.

E. Meléndez. DYLAM-TRETA linkage. Technical note I.92.72 ISEI/SER 2296/92, Institute for Systems Engineering and Informatics, 1992.

A. X. Miao, G. L. Zacharias y S-P Kao. A computation situation assessment model for nuclear power plant operations. *IEEE transactions on systems, man and cybernetics - Part A: Systems and humans*, 27(6):728–742, 1997.

G. A. Miller. The magical number seven, plus or minus two: some limits on our capacity for processing information. *The Psychological Review*, 63:81–97, 1956.

A. Mosleh y Y. H. Chang. Model-based human reliability analysis: prospects and requirements. *Reliability Engineering and System Safety*, 83:241–253, 2004.

G. A. Murphy. Selected Safety-Related Events. *Nuclear Safety*, 34(1):113–114, 1993.

NEA. Nuclear Regulatory Challenges Related to Human Performance. Informe técnico 5334, Nuclear Energy Agency, 2004. ISBN 92-64-02089-6.

Y. Niwa y E. Hollnagel. Integrated computerization of operating procedures. *Nuclear Engineering and Design*, 213:289–301, 2002.

Y. Niwa, E. Hollnagel y M. Green. Guidelines for computerized presentation of emergency operating procedures. *Nuclear Engineering and Design*, 167(2):113–127, Noviembre 1996.

D. Norman. *User-Centered System Design: New Perspectives on Human Computer Interaction*. Lawrence Erlbaum Associates Inc., 1986.

D. A. Norman. Categorisation of Action Slips. *Psychological Review*, 88(1):1–15, 1981.

D. A. Norman. *The Psychology of Everyday Things*. Basic Books, 1988.

D. A. Norman. Commentary: Human Error and the Design of Computer Systems. En *Communications of the ACM 33*, 1990.

NRC. Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA). Informe técnico NUREG-1624, Nuclear Regulatory Commission, 2000.

NRC. TMI-2 lessons learned task force status report and short-term recommendations. Informe técnico NUREG-0578, Nuclear Regulatory Commission, 1979.

NRC. Information To Licensees Regarding NRC Inspection Manual Section On Resolution Of Degraded And Nonconforming Conditions. Generic letter 91-18, Nuclear Regulatory Commission, 1991.

NRC. Crediting of operator actions in place of automatic actions and modifications of operator actions, including reponse times. Information Notice 97-78, Nuclear Regulatory Commission, 1997.

NRC. Loss of Main and Auxiliary Feedwater Event at the Davis-Besse Plant on June 9, 1985. Informe técnico NUREG-1154, Nuclear Regulatory Commission, 1985.

J. M. O'Hara. A quasi-experimental model of complex human-machine system validation. *International Journal of Cognition, Technology and Work*, 1:37–46, 1999.

J. M. O'Hara y W. S. Brown. Software tool for the use of human factors engineering guidelines to conduct control room evaluations. En *HCI International'99: International Conference on Human-Computer Interaction*, 1999.

J. M. O'Hara, J. Higgins y W. Stubler. Computer-based Procedure Systems: Technical Basis and Human Factors Review Guidance. Informe técnico NUREG/CR-6634, BNL, 2000a.

J. M. O'Hara, J . C. Higgins y J. Kramer. Automation of Emergency Operating Procedures: Finding the right balance. En *International Topical Meeting on Nuclear Plant Instrumentation, Controls and Human-Machine Interface Technologies*. NPIC & HMIT 2000, 2000b.

J. M. O'Hara, J. C. Higgins, J.J. Persensky, P.M. Lewis y J.P. Bongarra. Human Factors Engineering Program Review Model. Informe técnico NUREG-0711, NRC, 2004. Rev. 2.

R. G. Orendi, D. S. Petras, M. H. Lipner, R. R. Oft y S. V. Fanto. Human-factors considerations in emergency procedure implementation. En *Conference Record for 1988 IEEE Fourth Conference on Human Factors and Power Plants, 1988.*, pág. 214–221, 1988.

F. Owre. Role of the man-machine interface in accident management strategies. *Nuclear Engineering and Design*, 209:201–210, 2001. Tenemos la ponencia de FISA-99.

R. Parasuraman. Humans and Automation: Use, Misuse, Disuse, Abuse. *Human Factors*, 39 (2):230–253, 1997.

R. Parasuraman, Sheridan T. B. y C. D. Wickens. A model for types and levels of human interaction with automation. *IEEE Transactions on Systems, Man and Cybernetics - Part A: Systems and Humans*, 30(3):286–297, Mayo 2000.

J. Park y W. Jung. The requisite characteristics for diagnosis procedures based on empirical findings of the operators' behavior under emergency situations. *Reliability Engineering and System Safety*, 81:197–213, 2003a.

J. Park y W. Jung. The operators' non-compliance behavior to conduct emergency operating procedures - comparing with the work experience and the complexity of procedural steps. *Reliability Engineering and System Safety*, 82:115–131, 2003b.

J. Park y W. Jung. The appropriateness of the systematic framework to develop diagnosis procedures of nuclear power plants - an experimental verification. *Reliability Engineering and System Safety*, 91:53–65, 2006a.

J. Park y W. Jung. OPERA - a human performance database under simulated emergencies of nuclear power plants. *Reliability Engineering and System Safety*, XX(X):XX–XX, 2006b. En impresión.

J. Park, W. Jung, K. Jaewhan, H. Jaejoo y S. Yunghwa. The step complexity measure for emergency operating procedures: comparing with simulation data. *Reliability Engineering and System Safety*, 74:63–74, 2001.

J. Park, W. Jung, J. Ha y C. Park. The step complexity measure for emergency operating procedures: measure verification. *Reliability Engineering and System Safety*, 76:45–59, 2002.

J. Park, K. Jeong y J. Wondea. Identifying cognitive complexity factors affecting the complexity of procedural steps in emergency operating procedures of a nuclear power plant. *Reliability Engineering and System Safety*, 89:1–16, 2004a.

J. Park, J. Kim y W. Jung. Comparing the complexity of procedural steps with the operators' performance observed under stessful conditions. *Reliability Engineering and System Safety*, 83:79–91, 2004b.

J. Park, W. Jung, J. Kim y J. Ha. Analysis of human performance observed under simulated emergencies of nuclear power plants. Informe técnico KAERI/TR-2895/2005, KAERI, 2005.

I. Parzer, B. Mavko y B. Krajnc. Simulation of a hypothetical Loss of Feedwater accident in a modernized nuclear power plant. *Journal of Mechanical Engineering*, 49:430–444, 2003.

S. Petelin, J. Marn, B. Mavko y O. Gortnar. RELAP5 and MAAP analyses of RCS feed and bleed. En *International Meeting PSA/PRA and Severe Accidents '94*, pág. 17–20, Abril 1994.

S. Petelin, B. Mavko y O. Gortnar. Analysis of operator actions during the accident caused by total loss of secondary heat sink. *Nuclear Engineering and Design*, 159:169–175, 1995.

H. E. Pople, W. E. Spangler y M. T. Pople. EAGOL: An Artificial Intelligence System for Process Monitoring, situation Assessment and Response Planning. *IEEE*, pág. 298–304, 1994.

S. Poveda. Análisis y simulación de transitorios en centrales nucleares de agua a presión mediante el sistema de simulación TRETA. Aplicación a los casos de recharzo de carga y rotura de la línea de vapor. Proyecto fin de carrera, Departamento de Ingeniería Nuclear, Universidad Politécnica de Madrid., 1999.

P. Pyy. *Human reliability analysis methods for probabilistic safety assessment*. Tesis doctoral, Lappeenranta University of Technology, 2000.

P. Pyy y K. Andersson. Integrated sequence analysis - A solution to HRA problems? En *Sixth Conference on Human Factors and Power Plants, 1997. 'Global Perspectives of Human Factors in Power Generation'.*, pág. 9/1–9/6. IEEE, Junio 1997.

P. Pyy, J. P. Bento y Y. Flodin. An analysis of errors of commission in the Nordic nuclear power plants based on plant operating experience. Informe técnico NKS-74, NKS, Diciembre 2001. ISBN 87-7893-130-4.

W. Qin y P. G. Seong. A validation method for emergency operating procedures of nuclear power plants based on dynamic multi-level flow modeling. *Nuclear Engineering and Technology*, 37(1):118–126, February 2005.

C. Queral y M. A. García. Desarrollo de instrumentos de evaluación de guías de gestión de accidentes. Informe técnico, Consejo de Seguridad Nuclear, 1997.

C. Queral, E. Meléndez, J. M. Izquierdo, J. Hortal, M. Sánchez y R. Herrero. TIZONA: A Computer Code with an Advanced Two Phase Thermal Hydraulic Package. En *Mathematics and Computation, Reactor Physics and Environmental Analysis in Nuclear APplications*, 1999.

C. Queral, A. Expósito, J. A. Quiroga, A. Ibarra y I. González. Métodos de validación y verificación de procedimientos de operación de una central PWR. Informe de tareas realizadas en el año 2002. Informe técnico, ETSI de Minas, 2002a.

C. Queral, A. Expósito, J. A. Quiroga, A. Ibarra y I. González. Métodos de validación y verificación de procedimientos de operación de una central PWR. Informe de tareas realizadas en el año 2003. Informe técnico, ETSI de Minas, 2003.

C. Queral, A. Expósito, J. A. Quiroga, A. Ibarra y I. González. Métodos de validación y verificación de procedimientos de operación de una central BWR. Informe de tareas realizadas en el año 2004. Informe técnico, ETSI de Minas, 2004a.

C. Queral, A. Expósito, J. A. Quiroga, A. Ibarra y I. González. Métodos de validación y verificación de procedimientos de operación de una central PWR. Informe de tareas realizadas en el año 2004. Informe técnico, ETSI de Minas, 2004b.

C. Queral, A. Expósito, J. A. Quiroga, A. Ibarra y I. González. Métodos de validación y verificación de procedimientos de operación de una central BWR. Informe de tareas realizadas en el año 2005. Informe técnico, ETSI de Minas, 2005.

C. Queral, A. Expósito, J. A. Quiroga, A. Ibarra y I. González. Métodos de validación y verificación de procedimientos de operación de una central BWR. Informe de tareas realizadas en el año 2006. Informe técnico, ETSI de Minas, 2006.

César Queral, Javier Mulas, Nicolás Burbano, Ignacio Collazo y Alberto Concejal. Obtención del modelo de planta de la CN de Almaraz para TRAC-M a partir del modelo de RELAP5/mod3. Informe técnico, Dpto. Sistemas Energéticos. ETSI de Minas (UPM), 2002b.

J. A. Quiroga, A. Ibarra y A. Expósito. Implementación de la interfase de comuniciones de los códigos TRETA y COPMA-III. Informe técnico, ETSI de Minas, 2006.

J. Rasmussen. Skills, rules, knowledge: signals, signs and symbols and other distinctions in human performance models. En *IEEE Transactions: Systems, Man and Cybernetics SMC-13*, pág. 257–267, 1983.

J. Rasmussen. *Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering*. Elsevier Science Inc., New York, NY, USA, 1986. ISBN 0444009876.

J. Rasmussen. *The definition of human error and a taxonomy for technical system design,*. John Wiley & Sons, 1987.

N. C. Rasmussen. Reactor Safety Study, An Assessment of Accident Risks in U. S. Nuclear Power Plants. Informe técnico NUREG-75/014, U. S. Nuclear Regulatory Commission (NRC), October 1975. WASH-1400.

J. Reason. *Human Error*. Cambridge University Press, 1990.

L. V. Rigby. The Nature of Human Error. En *American Society for Quality Control. Annual Technical Conference, 24.th.*, pág. 457–466, 1970.

E. M. Roth, R. J. Mumaw y P. M. Lewis. An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies. Informe técnico NUREG/CR-6208, Nuclear Regulatory Commission, 1994.

H. Roth-Seefrid, A. Feigel y H.-J. Moser. Implementation of feed-and-bleed procedures in Siemens PWRs. *Nuclear Engineering and Design*, 148:133–150, 1994.

W. B. Rouse. Human-computer interaction in the control of dynamic systems. *Computing Surveys*, 13(1), Marzo 1981.

W. B. Rouse y S. Rouse. Analysis and classification of human error. En *IEEE Transactions on Systems, Man and Cybernetics*, volúmen 4, pág. 539–549, 1983.

D. Roverso. Intelligence Systems Integration: Guiding Principles, Examples, and Lessons Learned. *Progress in Nuclear Energy*, 46(3-4):190–205, 2005.

T. G. Ryan. *The Integration of Human Factors (HF) in the SAR Process. Training Course Text*. INEL, 1995.

K. Sasou, K. Takano y S. Yoshimura. Modelling a team's decisionmaking process. *Safety Science*, 24(1):13–33, (1996).

J. C. Schryver. Operator model-based design and evaluation of advanced systems: computational models. En *Conference Record for 1988 IEEE Fourth Conference on Human Factors and Power Plants, 1988.*, pág. 121–127, 1988.

R. Seifert y K. Brauser. The Task Taxonomy Method: A Basis For An Expert System On Human Reliability. Informe técnico, Messerschmitt-Boelkow-Blohm GMBH. Helicopter And Military Aircraft Group, 1987.

S-H. Shen, C. Smidts y A. Mosleh. A methodology for collection and analysis of human error data based on a cognitive model: IDA. *Nuclear Engineering and Design*, 172:157–186, 1997.

S. Shorrock, B. Kirwan y E. Smith. Human error prediction in Air Traffic Management: A comparasion of two approaches. En *IBC Conference on Preventing Human Errors and Violations*, 2003.

N. Siu. Risk Assessment for Dynamic Systems: An Overview. *Reliability Engineering and System Safety*, 43:43–73, 1994.

A. B. M. Skjerve y G. Skraaning. The quality of human-automation cooperation in human-system interface for nuclear power plants. *International Journal Human-Computer Studies*, 61:649–677, 2004.

A. J. Spurgin y B. O. Y. Lydell. Critique of current Human Reliability Analysis Methods. En IEEE, editor, *IEEE 7th Human Factors Meeting*, 2002.

H. J. Störig. *Historia universal de la filosofía*. Tecnos, 1995.

O. Sträter. *Evaluation of human reliability on the basis of operational experience*. Tesis doctoral, Faculty of Economics and Social Sciences, Munich Technical University., 2000.

O. Sträter. Considerations on the elements of quantifying human reliability. *Reliability Engineering and System Safety*, 83:255–264, 2004.

Sun. *COPMA-III (1.0 β) Users Guide*. Institutt for EnergiteTeknikk, 2002a.

Sun. http://java.sun.com/docs/books/tutorial/idl/index.html, 2002b.

Sun. http://www.omg.org/gettingstarted/corbafaq.htm, 2002c.

Sun. http://java.sun.com/docs/books/tutorial/rmi/index.html, 2002d.

Sun. http://java.sun.com/docs/books/tutorial/native1.1/index.html, 2002e.

J. F. Sureda. *Nota técnica de prevención: Fiabilidad humana: evaluación simplificada del error humano (I)*, 2001a. NTP-619.

J. F. Sureda. *Nota Técnica de Prevención: Fiabilidad humana: evaluación simplificada del error humano (II)*, 2001b. NTP-620.

J. F. Sureda. *Nota Técnica de Prevención: Fiabilidad humana: evaluación simplificada del error humano (III)*, 2001c. NTP-621.

A. Swain. A method for performing a human factors reliability analysis. Monografía SCR-685, Sandia National Laboratories, Albuquerque, NM, USA, 1963.

A. Swain y H. Guttman. Handbook of human reliability analysis with emphasis on nuclear power plant applications. Informe técnico NUREG/CR-1278, Sandia National Laboratory, 1983.

A. D. Swain. Human reliability analysis: Need, status, trends, and limitations. *Reliability Engineering and System Safety*, 29:301–313, 1990.

Tecnatom. Perdida del refrigerante del reactor o secundario. Informe técnico RP/S-I, Tecnatom, S.A., 1986.

Tecnatom. *Tecnología de centrales. Vol. III*. Tecnatom, S.A., 2000.

J. Theureau. Use of nuclear reactor control room simulators in research & development. *Cognition, Technology & Work*, 2:97–105, 2000.

J. Theureau, F. Jeffroy y P. Vermersch. Controling a Nuclear Reactor in Accidental Situations with Symptom-based Computerized Procedures: a Semiological & Phenomenological Analysis. En *CSEPC 2000*, 2000.

E.A. Trager. Case Study Report on Loss of Safety System Function Events. Informe técnico AEOD/C504, Office for Analysis and Evaluation of Operational Data. Nuclear Regulatory Commission (NRC), 1985.

R. Travis, J. Taylor, A. Fresco y J. Chung. Generic Risk Insights for Westinghouse and Combustion Engineering Pressurized Water Reactors. Informe técnico NUREG/CR-5637, BrooKhaven National Laboratory, 1990. TI91 004176.

M. Triviño, C. Queral, M. A. García y C. García. Simulación de secuencias de pérdida de suministro eléctrico en la CN de Cofrentes. Informe técnico, Iberdrola, 1997.

I. Veci. Proyecto de computerización de los procedimientos de emergencia. Elaboración de un modelo de los procedimientos para la C.N. de José Cabrera. EOP-E-3: Rotura de tubos en el generador de vapor. Informe técnico Revisión 0. STN/MOSI/IN/34/2000, Consejo de Seguridad Nuclear, 2000a.

I. Veci. Modelo de procedimientos para la central nuclear de Jose Cabrera EOP-ES-0.2. Informe técnico Revisión 0. STN/PPTT/IN/06/96, Consejo de Seguridad Nuclear, 2000b.

I. Veci. Proyecto de simulación de los procedimientos de emergencia. Análisis y clasificación de las actividades del operador. Estudio preparatorio de un modelo de procedimiento. Informe técnico Revisión 0. SEP/PPTT/IN/031/93, Consejo de Seguridad Nuclear, 1993.

I. Veci. Proyecto de simulación de los procedimientos de emergencia. Elaboración de un modelo de procedimientos para la central nuclear de José Cabrera. Documento base. Rev. 0. Informe técnico Revisión 0. SEP/PPTT/IN/021/94, Consejo de Seguridad Nuclear, 1994a.

I. Veci. Modelo de procedimientos para la central nuclear José Cabrera. EOP-E-0. Informe técnico Revisión 0. SEP/PPTT/IN/030/94, Consejo de Seguridad Nuclear, 1994b.

I. Veci. Proyecto de computerización de los procedimientos de emergencia. Elaboración de un modelo de procedimientos para la central nuclear de José Cabrera. Documento base. Rev. 1. Informe técnico Revisión 2. SEP/PPTT/IN/027/95, Consejo de Seguridad Nuclear, 1995.

K. J. Vicente. *Cognitive work analysis: Toward safe, productive, and healthy computer-based work*. Lawrence Erbaum Associates, 1999.

A. Villemeur, J. M. Moroni, F. Mosneron-Dupin y T. Meslin. A simulator-based evaluation of operators' behavior by Electricite de France. En *Proceedings of the International Topical Meeting on Advanced in Human Factors in Nuclear Power Systems*, pág. 374–379, Knoxville, Tennessee, 1986.

Westinghouse. *Analisis de transitorios y accidentes con el analizador integral de planta. CN Valdellos II.* Westinghouse España, 1993.

Westinghouse. *Curso del reactor de agua ligera a presión (PWR)*. Westinghouse España, 1994.

D. A. Wiegmann y S. A. Shappell. Human factors analysis of post-accident data: Applying theoretical taxonomies of human error. *International Journal of Aviation Psychology*, 7(1): Lawrence Erlbaum Associates, Inc., 1997.

WOG. Documentos de base E-1, E-2, ECA-1, ECA-2. Informe técnico WOG-97-188, Westinghouse Electric Corporation, 1997.

D. Woods, Johannesen L., R. Cook y N. Sarter. Behind human error: Cognitive systems, computers and hindsight. Informe técnico SOAR 94-01, Human Systems Information Analysis Center, 1994.

D. D. Woods, E. M. Roth y H. Pople. Cognitive environment simulation: An artificial intelligence system for human performance assessment. En *Modelling Human Intention Formation*, volúmen 2. NRC, 1987.