



UNIVERSITAT  
POLITÈCNICA  
DE VALÈNCIA

**Aportaciones al modelado de la  
indisponibilidad de componentes y la  
fiabilidad humana para la mejora de  
la seguridad de las centrales nucleares  
informada en el riesgo**

---

**TESIS DOCTORAL**

Pablo Martorell Aigües

**Dirigida por:**

Dr. Sebastián Salvador Martorell Alsina

Dra. Ana Isabel Sánchez Galdón

Enero 2019



# Resumen

La seguridad ha sido, es y seguirá siendo una prioridad en la operación de las centrales nucleares para la producción de energía eléctrica. Uno de los grandes retos a los que se enfrenta la industria nuclear es el envejecimiento de las estructuras, sistemas y componentes (ESC) de seguridad. Actualmente, este hecho cobra especial relevancia porque un gran número de reactores está alcanzando el fin de su vida de diseño, debiendo afrontar próximamente una Revisión Periódica de Seguridad (RPS), que garantice el funcionamiento seguro de la central durante un periodo adicional denominado Operación a Largo Plazo (OLP).

El Análisis Probabilista de Seguridad (APS) es una herramienta fundamental para la gestión integral de la seguridad de una planta, tanto en el marco de la RPS como en la Toma de Decisiones Informada en el Riesgo (TDIR), siendo capaz de evaluar el incremento o disminución en el riesgo producido por un cambio determinado. Sin embargo, los modelos y datos actuales que lo integran no tienen en cuenta factores que influyen de forma determinante en el riesgo de una central. Por un lado, no tienen en cuenta el envejecimiento o la estrategia de pruebas y mantenimiento, en el caso del modelado de la fiabilidad e indisponibilidad de componentes. Por otro lado, no contemplan la imprecisión en el modelado de las acciones humanas, ni la inexactitud en la cuantificación de sus probabilidades de error.

La presente tesis doctoral pretende actualizar y mejorar los modelos del APS, con vistas a su aplicación en el contexto de la RPS y de la TDIR. En este sentido, se establecen dos objetivos principales. En primer lugar, el desarrollo de un modelo RAM (fiabilidad, mantenibilidad y disponibilidad) dependiente del tiempo para componentes de seguridad, ajustado con datos reales de planta y con un nivel de detalle suficiente para recoger explícitamente en la edad del mismo, el efecto de las pruebas y el mantenimiento. En segundo lugar, mostrar las aplicaciones del APS para la TDIR. En primer término, se define un modelo de riesgo dependiente de la edad, a partir del modelo RAM previamente formulado, con el que seleccionar la mejor estrategia de pruebas y mantenimiento en un horizonte temporal dado. En segundo término, para mejorar el modelado del APS y la cuantificación de las probabilidades de error humano (PEH), se propone una metodología de evaluación de impacto en el riesgo para cambios en las acciones humanas y las Especificaciones Técnicas de Funcionamiento, que aprovecha los resultados del uso conjunto de los análisis de seguridad determinista y probabilista.

Las aportaciones que conforman esta tesis doctoral se integran en la línea de investigación financiada por el Ministerio de Economía y Empresa en el proyecto ENE2016-80401-R, “Armonización de requisitos de vigilancia y mantenimiento en centrales nucleares con información en el riesgo” y la ayuda para contratos predoctorales para la formación de doctores BES-2014-067602.





# Resum

La seguretat ha sigut, és i continuarà sent una prioritat en l'operació de les centrals nuclears par a la producció d'energia elèctrica. Un del grans reptes als que s'enfronta la industria nuclear es l'envelliment de les estructures, sistemes i components de seguretat. Actualment, aquest fet té especial rellevància perquè un gran nombre de reactors està arribant a la fi de la seua vida de disseny, havent d'afrontar pròximament una Revisió Periòdica de Seguretat (RPS), que garantirà el funcionament segur de la central durant un període adicional conegut com Operació a Llarg Termini (OLP).

L'Anàlisi Probabilista de Seguretat es una ferramenta fonamental per a la gestió integral de la seguretat d'una planta, tant en el marc de la RPS com en la presa de decisions informades en el risc (TDIR), sent capaç d'avaluar l'increment o disminució en el risc produït per un canvi determinat. No obstant això, els models i dades actuals que ho integren no tenen en compte factors que influeixen de forma determinant en el risc d'una central. Per una banda, no consideren l'envelliment o l'estratègia de proves i manteniment, en el cas del modelat de la fiabilitat i indisponibilitat de components. Per altra banda, no contempen la imprecisió en el modelat de les accions humanes, ni la inexactitud en la quantificació de la probabilitat d'error de les mateixes.

La present tesi doctoral pretén actualitzar i millorar els models APS, amb la intenció d'aplicar-los en el context de la RPS y la TDIR. En aquest sentit, s'estableixen dos objectius principals. En primer lloc, el desenvolupament d'un model RAM (fiabilitat, mantenibilitat i disponibilitat) dependent del temps per a components de seguretat, ajustat amb dades reals de planta i amb un nivell de detall suficient per a recollir explícitament en l'edat del mateix, la política de proves i manteniment a la que es sotmès. En segon lloc, mostrar les aplicacions de l'APS per a la TDIR. En primer terme, es defineix un model de risc dependent de l'edat, a partir del model RAM prèviament formulat, amb el qual seleccionar la millor estratègia de proves i manteniment en un horitzó temporal determinat. En segon terme, per a millorar el modelat de l'APS i la quantificació de les probabilitats d'error humà (PEH), es proposa una metodologia d'avaluació d'impacte en el risc per a canvis en les accions humanes i en les Especificacions Tècniques de Funcionament, que aprofita els resultats de l'ús conjunt dels anàlisis determinista i probabilista.

Les aportacions que formen part d'aquesta tesi doctoral s'integren en la línia d'investigació finançada pel Ministeri d'Economia i Empresa en el projecte ENE2016-80401-R, "Armonización de requisitos de vigilancia y mantenimiento en centrales nucleares con información en el riesgo" i l'ajuda per a contractes predoctorals per a la formació de doctors BES-2014-067602.



# Abstract

Safety always has been and always will be a priority in nuclear power plant operation to generate electricity. One of the major challenges of nuclear industry is the ageing of safety-related structures, systems and components (SSC). Presently, this fact gains relevance due to several reactors are reaching their design life, having to conduct a Periodic Safety Review (PSR) that assures safety operation for an additional period better-known as Long Term Operation (LTO)

Probabilistic Safety Assessment (PSA) is an essential tool in an integral NPP safety management, both PSR framework and Risk Informed Decision Making (RIDM), being able to evaluate a risk increase or decrease for any specific change on the plant. However, current PSA models and data do not consider factors, which have an impact in the overall risk of the plant. On the one hand, they do not take into account the effect of ageing nor maintenance and testing program, in the case of reliability and unavailability modelling. On the other hand, human actions modelling and their associated error probabilities are characterized by its inaccuracy and uncertainty.

This Ph. Dissertation aims to update and improve PSA models, in order to apply within the framework of PSR and RIDM. In this sense, two main objectives are established. Firstly, the development of a time dependent RAM (reliability, availability and maintainability) for safety-related components, fitted with a historical plant data and with enough level of detail to include the effects of testing and maintenance activities in the age of the component. Secondly, it shows PSA applications of new models in RIDM. In the first place, it defines an age-dependent risk model based on the RAM model previously formulated, which helps to select the best approach of maintenance and testing activities for a specific timeline. In the second place, to improve PSA modelling and human error probabilities (HEP) quantification, a methodology is proposed to evaluate the risk impact of human actions and TS changes, taking advantage of combining DSA and PSA insights.

The work of this thesis is part of the research supported by the Ministry of Economy and Business in the project ENE2016-80401-R, “Risk Informed Harmonization of Surveillance Requirements and Maintenance in Nuclear Power Plants”, and in the Doctoral Fellowship BES-2014-067602.



# Índice

<b>Capítulo 1 Introducción.....</b>	<b>1</b>
1.1. Motivación y antecedentes .....	1
1.2. Objetivos y organización del trabajo .....	3
<b>Capítulo 2 Estado del arte .....</b>	<b>7</b>
2.1. Marco normativo .....	7
2.1.1. Revisión Periódica de Seguridad y gestión del envejecimiento .....	7
2.1.2. Especificaciones Técnicas de Funcionamiento .....	9
2.1.3. Regla de Mantenimiento .....	10
2.1.4. Análisis de Fiabilidad Humana .....	11
2.2. Análisis Probabilista de Seguridad .....	13
2.2.1. Modelos RAM dependientes de la edad.....	18
2.2.2. Modelado de la PEH .....	20
2.3. Toma de decisiones informada en fiabilidad y riesgo .....	22
<b>Capítulo 3 Modelo de indisponibilidad en demanda dependiente del tiempo .....</b>	<b>27</b>
3.1. Modelo físico para un componente de seguridad .....	27
3.2. Modelo de indisponibilidad básico para un componente de seguridad .....	30
3.3. Modelo de la probabilidad de fallo a la demanda considerando el estrés causado por las demandas, la efectividad del mantenimiento y la eficiencia de las pruebas .....	32
3.3.1. Probabilidad de fallo a la demanda considerando el estrés causado por las demandas.....	32
3.3.2. Probabilidad de fallo a la demanda considerando la efectividad del mantenimiento .....	33

3.3.2.1	Modelo PAS.....	34
3.3.2.2	Modelo PAR.....	38
3.3.3.	Probabilidad de fallo a la demanda considerando la eficiencia de las pruebas ....	39
3.4.	Modelo de indisponibilidad para el modo de fallo en demanda .....	40
3.4.1.	Indisponibilidad debida a la falta de fiabilidad.....	40
3.4.1.1	Evaluación del <i>doubling time</i> .....	41
3.4.1.2	Indisponibilidad media debida a la falta de fiabilidad a lo largo de la vida del componente .....	42
3.4.2.	Indisponibilidad debida a los tiempos fuera de servicio .....	43
3.5.	Estudio de la evolución de la fiabilidad e indisponibilidad de un componente aplicando el modelo de probabilidad de fallo a la demanda dependiente del tiempo .....	43
3.5.1.	Fiabilidad dependiente del tiempo: modelos PAS y PAR .....	44
3.5.2.	Sensibilidad de $\rho(t)$ para el intervalo de mantenimiento.....	45
3.5.3.	Sensibilidad de $\rho(t)$ para la efectividad del mantenimiento .....	47
3.5.4.	Sensibilidad de $\rho(t)$ para el intervalo de pruebas .....	48
3.6.	Sensibilidad del <i>doubling time</i> para el mantenimiento y el intervalo de pruebas .....	50
3.7.	Indisponibilidad media en función de los intervalos de pruebas y mantenimiento .....	51
<b>Capítulo 4</b>	<b>Estimación de parámetros de un modelo de fiabilidad dependiente del tiempo .....</b>	<b>55</b>
4.1.	Modelos de fiabilidad bajo mantenimiento imperfecto .....	55
4.1.1.	Modelo de fiabilidad para fallos en espera .....	56
4.1.1.1	Modelo PAS.....	57
4.1.1.2	Modelo PAR.....	57
4.1.2.	Modelo de fiabilidad para fallos en demanda .....	58
4.1.2.1	Modelo PAS.....	58
4.1.2.2	Modelo PAR.....	59

4.2. Metodología de estimación de parámetros y selección del modelo.....	60
4.2.1. Función de verosimilitud para fallos en espera, $L_1(\xi)$ .....	61
4.2.2. Función de verosimilitud para fallos en demanda, $L_2(\xi)$ .....	62
4.3. Caso de aplicación .....	65
4.3.1. Histórico de fallos, mantenimientos y pruebas.....	65
4.3.2. Resultados de la estimación máximo verosímil .....	66
4.3.3. Indisponibilidad media debida a la falta de fiabilidad durante la vida útil del componente en función de los intervalos de pruebas y mantenimiento .....	67
4.3.4. Indisponibilidad media total durante la vida útil del componente en función de los intervalos de pruebas y mantenimiento .....	68
<b>Capítulo 5 Aplicación de un modelo RAM dependiente del tiempo para la Toma de Decisiones Informada en el Riesgo .....</b>	<b>71</b>
5.1. Modelo RAM dependiente de la edad .....	72
5.1.1. Modelo de indisponibilidad.....	72
5.1.1.1 <i>Indisponibilidad debida a la falta de fiabilidad</i> .....	73
5.1.1.2 <i>Indisponibilidad debida a los tiempos fuera de servicio</i> .....	75
5.2. Modelo de riesgo dependiente de la edad.....	76
5.2.1. Cambio en la contribución a la FDN anual .....	77
5.2.2. Incremento Condicional de la Probabilidad de Daño al Núcleo.....	78
5.3. Toma de decisiones .....	78
5.3.1. Criterios relativos a cambios en las ETF.....	79
5.3.2. Criterios relativos a cambios en la RM .....	81
5.4. Estudio de la optimización de la vigilancia y mantenimiento informada en el riesgo de un componente considerando envejecimiento.....	82
5.4.1. Parámetros RAM de la MOV .....	82
5.4.2. Formulación de los problemas de optimización .....	83
5.4.2.1 <i>Caso 1: optimización del mantenimiento en base a la RM</i> .....	84
5.4.2.2 <i>Caso 2: optimización del intervalo de pruebas de vigilancia en base a las ETF</i> .....	84

5.4.2.3 <i>Caso 3: optimización de los intervalos de mantenimiento y pruebas en base al RITS-5b</i>	85
5.4.3. Resultados.....	86
5.4.3.1 <i>Caso 1</i> .....	86
5.4.3.2 <i>Caso 2</i> .....	86
5.4.3.3 <i>Caso 3</i> .....	87
5.4.4. Resumen de los resultados.....	90
<b>Capítulo 6 Evaluación del impacto en la fiabilidad humana y el riesgo para cambios en las ETF .....</b>	<b>91</b>
6.1. Importancia del factor humano en la Toma de Decisiones Informada en el Riesgo .....	91
6.2. Metodología.....	92
6.2.1. Modelado del impacto en el riesgo .....	93
6.2.1.1 <i>Modelado del Análisis Determinista de Seguridad</i> .....	93
6.2.1.2 <i>Análisis de Fiabilidad Humana: modelado de la probabilidad de error humano</i> .....	94
6.2.1.3 <i>Modelo APS refinado</i> .....	95
6.2.2. Evaluación del impacto en el riesgo .....	96
6.2.3. Análisis del impacto en el riesgo .....	98
6.3. Caso de aplicación .....	100
6.3.1. Descripción del sistema y cambio del CT propuesto.....	100
6.3.2. Modelado del impacto en el riesgo .....	101
6.3.2.1 <i>Modelo APS original</i> .....	101
6.3.2.2 <i>Modelo determinista</i> .....	102
6.3.2.3 <i>Cálculo de la PEH</i> .....	104
6.3.2.4 <i>Modelo APS refinado</i> .....	106
6.3.2.5 <i>Evaluación del impacto en la fiabilidad humana y el riesgo del cambio en el CT</i> ...	108
6.3.3. Aceptación del impacto en el riesgo .....	109
<b>Capítulo 7 Conclusions and contributions.....</b>	<b>113</b>



7.1. Conclusions .....	113
7.2. Scientific contributions.....	115
7.2.1. Articles in international scientific journals.....	116
7.2.2. Contributions to international conferences.....	117
7.2.3. Contributions to national conferences.....	120
<b>Capítulo 8 References .....</b>	<b>123</b>



# Figuras

Figura 2.1 Ejemplo de árbol de eventos y árbol de fallos de un APS.....	14
Figura 2.2 Niveles del APS.....	16
Figura 2.3 Principios básicos de las aplicaciones de APS .....	24
Figura 2.4 Criterios de aceptación para <i>FDN</i> .....	24
Figura 2.5 Criterios de aceptación para <i>FGLT</i> .....	25
Figura 3.1 Modelo físico del funcionamiento de un componente de seguridad .....	28
Figura 3.2 Modelo físico simplificado del funcionamiento de un componente de seguridad .....	30
Figura 3.3 $\rho(t)$ del componente para los modelos de mantenimiento imperfecto PAS y PAR .....	45
Figura 3.4 $\rho(t)$ del componente para diferentes periodos de mantenimiento del modelo PAS.....	46
Figura 3.5 $\rho(t)$ del componente para diferentes periodos de mantenimiento del modelo PAR .....	46
Figura 3.6 $\rho(t)$ del componente para diferentes efectividades del mantenimiento del modelo PAS.....	47
Figura 3.7 $\rho(t)$ del componente para diferentes efectividades del mantenimiento del modelo PAR .....	48
Figura 3.8 $\rho(t)$ del componente para diferentes intervalos de pruebas del modelo PAS .....	49
Figura 3.9 $\rho(t)$ del componente para diferentes intervalos de pruebas del modelo PAR .....	49
Figura 3.10 Posibles combinaciones de $p_1$ , $\varepsilon$ y $M/T$ para las que se alcanza el <i>doubling time</i> antes de 10 años.....	50

Figura 3.11 $t_D$ para diferentes intervalos de pruebas y mantenimientos del modelo PAR .....	51
Figura 3.12 Indisponibilidad para diferentes intervalos de mantenimiento y pruebas adoptando un modelo PAS .....	52
Figura 3.13 Indisponibilidad para diferentes intervalos de mantenimiento y pruebas adoptando un modelo PAR.....	53
Figura 4.1 $u_{R,S}$ y $u_{R,D}$ en función del intervalo de pruebas para distintos periodos de mantenimiento .....	68
Figura 4.2 $u_{R,S}$ y $u_{R,D}+u_T+u_M$ en función del intervalo de pruebas para distintos periodos de mantenimiento.....	69
Figura 4.3 Indisponibilidad total para diferentes intervalos de mantenimiento y pruebas.....	70
Figura 5.1 Indisponibilidad debida a los tiempos fuera de servicio en función de $M$ , para $T_{APS}$ .....	86
Figura 5.2 Indisponibilidad debida a la falta de fiabilidad y al tiempo fuera de servicio debido a las pruebas en función de $T$ , para $M_{opt1}$ .....	87
Figura 5.3 Indisponibilidad total en función de $T$ y $M$ .....	88
Figura 5.4 Variación de la $\Delta FDN$ en función de $T$ y $M$ .....	89
Figura 5.5 Proyección en el plano $TM$ de la variación de la $\Delta FDN$ .....	89
Figura 6.1 Esquema de la TDIR para cambios en las ETF .....	92
Figura 6.2 Criterios de aceptación definidos en la RG 1.174 para $\{FDN, \Delta FDN\}$ 98	
Figura 6.3 Criterios de aceptación definidos en la RG 1.177 para $\{FDN_1, ICPDN_M\}$ .....	99
Figura 6.4 Modelo original del árbol de eventos para la pérdida del RHR.....	101
Figura 6.5 Simulaciones TH para la secuencia de pérdida del RHR .....	103
Figura 6.6 Ventanas temporales disponibles durante la secuencia de pérdida del RHR .....	104
Figura 6.7 Modelo refinado del árbol de eventos para la pérdida del RHR.....	106

Figura 6.8 Modificación del árbol de fallos correspondiente a la función de seguridad E1 .....	107
Figura 6.9 Impacto del cambio en el CT para $\{FDN, \Delta FDN\}$ .....	110
Figura 6.10 Impacto del cambio en el CT para $\{FDN_I, ICPDN_M\}$ .....	111



# Tablas

Tabla 3.1 Valor de los parámetros de la MOV para el caso base .....	44
Tabla 4.1 Datos de fallos recopilados para dos motoválvulas idénticas de una central nuclear .....	66
Tabla 4.2 EMV de los parámetros del modelo de fiabilidad para fallos en espera bajo modelos de mantenimiento imperfecto PAS y PAR .....	66
Tabla 4.3 EMV de los parámetros del modelo de fiabilidad para fallos en demanda bajo modelos de mantenimiento imperfecto PAS y PAR.....	67
Tabla 5.1 Parámetros RAM y valores iniciales de $T$ y $M$ para la MOV .....	83
Tabla 5.2 Resumen de los resultados de los distintos $MOP$ .....	90
Tabla 6.1 PEH obtenida para cada ventana temporal .....	105
Tabla 6.2 PEH obtenida para cada ventana temporal tras el cambio en el CT .....	108
Tabla 6.3 Impacto del cambio en el CT en $FDN_1$ e $ICPDN_M$ .....	109
Tabla 6.4 Impacto del cambio en el CT en $\Delta FDN$ .....	109
Tabla 7.1 Link between contributions and thesis chapters .....	116





# Acrónimos y siglas

AAA	Sistema de Agua de Alimentación Auxiliar
ADS	Análisis Determinista de Seguridad
AEC	<i>United States Atomic Energy Comission</i>
AFH	Análisis de Fiabilidad Humana
AH	Acción Humana
AMR	<i>Ageing Management Review</i> / Estudios de Gestión del Envejecimiento
APS	Análisis Probabilista de Seguridad
APSE	Análisis Probabilista de Seguridad Extendido
APSOM	Análisis Probabilista de Seguridad en Otros Modos de operación
ASEP	<i>Accident Sequence Evaluation Program</i>
ATHEANA	<i>A Technique for Human Event Analysis</i>
BAO	<i>Bad As Old</i>
CLO	Condiciones Límite de Operación
CREAM	<i>Cognitive Reliability and Error Analysis Method</i>
CSN	Consejo de Seguridad Nuclear
CT	<i>Completion Time</i> / Tiempo de indisponibilidad permitido
DG	<i>Diesel generator</i> / Generador diésel
EMV	Estimadores de máxima verosimilitud
EPRI	<i>Electronic Power Research Institute</i> / Instituto de Investigación de Energía Eléctrica
ESC	Estructuras, Sistemas y Componentes
ET	<i>Event Tree</i> / Árbol de sucesos
ETF	Especificaciones Técnicas de Funcionamiento
FDN	Frecuencia de Daño al Núcleo
FGLT	Frecuencia de Grandes Liberaciones Tempranas

FT	<i>Fault Tree</i> / Árbol de fallos
GAN	<i>Good As New</i>
GS	Guía de Seguridad
GV	Generador de Vapor
IAEA	<i>International Atomic Energy Agency</i> / Organización Internacional de la Energía Atómica
ICPDN	Incremento Condicional de la Probabilidad de Daño al Núcleo
IDHEAS	<i>Integrated Human Event Analysis System</i>
IE	<i>Initiating Event</i> / Suceso Iniciador
IEC	<i>International Electrotechnical Commission</i>
IS	Instrucción de Seguridad
MDP	<i>Motor driven pump</i> / Motobomba
MOV	<i>Motor operated valve</i> / Motoválvula
NARA	<i>Nuclear Action Reliability Assessment</i>
NEA	<i>Nuclear Energy Agency</i>
NPAP	<i>Nuclear Plant Ageing Research</i> / Investigación sobre el Envejecimiento de las Centrales Nucleares
NRC	<i>Nuclear Regulatory Commission</i> / Comisión Reguladora Nuclear de Estados Unidos
OF	<i>Objective Function</i> / Función objetivo
OLP	Operación a Largo Plazo
OP	<i>Optimization Problem</i> / Problema de optimización
PAR	<i>Proportional Age Reduction</i>
PAS	<i>Proportional Age Setback</i>
PEH	Probabilidad de Error Humano
PGE	Programas de Gestión del Envejecimiento
PGE-LP	Plan de Gestión de Envejecimiento a Largo Plazo
PGV	Plan de Gestión de Vida
PIE-GE	Plan Integrado de Evaluación y Gestión del Envejecimiento

PSF	<i>Performance Shaping Factors</i> / Factores de influencia
PWR	<i>Pressurized Water Reactor</i> / Reactor de Agua a Presión
RAM	<i>Reliability, Availability and Maintainability</i> / Fiabilidad, disponibilidad y mantenibilidad
RG	<i>Regulatory Guide</i> / Guía Reguladora
RHR	<i>Residual Heat Removal System</i> / Sistema de Extracción del Calor Residual
RM	Regla de Mantenimiento
RMTS	<i>Risk Management Technical Specifications</i>
RPS	Revisión Periódica de Seguridad
RV	Requisitos de Vigilancia
RWST	<i>Refueling Water Storage Tank</i> / Depósito de almacenamiento de agua de recarga
SF	<i>Surveillance Frequency</i> / Frecuencia de Vigilancia
SHARP	<i>Systematic Human Action Reliability Procedure</i>
SHERPA	<i>A systematic human error reduction and prediction approach</i>
SLIM	<i>Integrated Human Event Analysis System</i>
SPAR-H	<i>Standardized Plant Analysis Risk-Human Reliability Analysis</i>
SRR	Sistema de Refrigerante del Reactor
TDIR	Toma de Decisiones Informada en el Riesgo
THERP	<i>Technique for Human Error Rate Prediction</i>
TLAA	<i>Time Limited Ageing Analyses</i> / Análisis de Envejecimiento en Función del Tiempo
TMI	Three Mile Island
TRC	<i>Time Reliability Correlation</i>
TSTF	<i>Technical Specifications Task Force</i>
UE	Unión Europea



# Notación

## Capítulo 3: Modelo de indisponibilidad en demanda dependiente del tiempo

$n$	Número de pruebas realizadas en el equipo
$t$	Tiempo cronológico
$t'$	Tiempo transcurrido desde la última prueba de vigilancia
$T$	Intervalo de pruebas de vigilancia
$M$	Periodo de mantenimiento preventivo
$v$	Tiempo transcurrido desde el último reemplazo
$\rho_0$	Probabilidad de fallo a la demanda residual
$\lambda_0$	Tasa de fallos en espera residual
$p_1$	Factor de degradación asociado a los fallos a la demanda
$p_2$	Factor de degradación asociado a los fallos en espera
$\alpha$	Factor de envejecimiento lineal
$f(t)$	Función de degradación dependiente del tiempo
$\rho(t)$	Probabilidad de fallo a la demanda dependiente del tiempo
$\varepsilon$	Efectividad del mantenimiento
$f_m^-$	Función de degradación justo antes de llevar a cabo la actividad de mantenimiento $m$
$f_m^+$	Función de degradación justo después de llevar a cabo la actividad de mantenimiento $m$
$\rho_m^-$	Probabilidad de fallo a la demanda justo antes de llevar a cabo la actividad de mantenimiento $m$
$\rho_m^+$	Probabilidad de fallo a la demanda justo después de llevar a cabo la actividad de mantenimiento $m$
$m$	Número de mantenimiento preventivo
$t_D$	<i>Doubling time</i>
$m_D$	Número de mantenimiento en el que tiene lugar el <i>doubling time</i>

$\Delta\rho_m^+$	Incremento medio en la probabilidad de fallo a la demanda hasta la actividad de mantenimiento $m$
$\rho_m$	Probabilidad de fallo a la demanda media entre dos actividades de mantenimiento consecutivas $m-1$ y $m$
$\rho_{m^*}$	Probabilidad de fallo a la demanda media para la vida útil del componente
$RP$	Vida útil del componente
$\Delta\rho_{m^*}$	Incremento medio en la probabilidad de fallo a la demanda para la vida útil del componente
$\rho_{m^*}^D$	Probabilidad de fallo a la demanda asociada con los fallos detectados por las pruebas para la vida útil del componente
$\rho_{m^*}^U$	Probabilidad de fallo a la demanda asociada con los fallos no detectados para la vida útil del componente
$u_{R,m}(t)$	Indisponibilidad debida a la falta de fiabilidad dependiente del tiempo
$u_R$	Indisponibilidad media debida a la falta de fiabilidad para la vida útil del componente
$u_T$	Indisponibilidad media debida a las pruebas de vigilancia
$u_M$	Indisponibilidad media debida al mantenimiento preventivo
$u_C$	Indisponibilidad media debida al mantenimiento correctivo
$u_O$	Indisponibilidad media debida al reemplazamiento del componente
$\varphi$	Tiempo fuera de servicio medio debido a las pruebas de vigilancia
$\delta$	Tiempo fuera de servicio medio debido al mantenimiento preventivo
$\mu$	Tiempo fuera de servicio medio debido al mantenimiento correctivo
$\theta$	Tiempo fuera de servicio medio debido a los reemplazamientos

#### **Capítulo 4: Estimación de parámetros de un modelo de fiabilidad dependiente del tiempo**

$\lambda_0$	Tasa de fallos en espera residual
$\rho_0$	Probabilidad de fallo a la demanda residual
$\lambda_m(t)$	Tasa de fallos en espera dependiente del tiempo en el periodo $m$ tras el mantenimiento $m-1$

$\rho_m(t)$	Probabilidad de fallo a la demanda dependiente del tiempo en el periodo $m$ tras el mantenimiento $m-1$
$w_m(t)$	Edad del componente en el periodo $m$ tras el mantenimiento $m-1$
$f_m(t)$	Función de degradación en el periodo $m$ tras el mantenimiento $m-1$
$\alpha$	Factor de envejecimiento lineal
$\varepsilon_S$	Efectividad del mantenimiento asociados a los fallos en espera
$p_1$	Factor de degradación asociado a los fallos a la demanda
$\varepsilon_D$	Efectividad del mantenimiento asociados a los fallos en demanda
$T$	Intervalo de pruebas de vigilancia
$M$	Periodo de mantenimiento preventivo
$m$	Número de mantenimiento preventivo
$t_m$	Tiempo cronológico en que se produce el mantenimiento preventivo $m$
$H_m(t)$	Función de riesgo acumulada en el periodo $m$ tras el mantenimiento $m-1$
$D_m(t)$	Probabilidad de fallo a la demanda acumulada en el periodo $m$ tras el mantenimiento $m-1$
$L(.)$	Función de verosimilitud
$x$	Vector de parámetros desconocidos
$L_1(x)$	Función de verosimilitud para fallos en espera
$L_2(x)$	Función de verosimilitud para fallos en demanda
$r_{p,m}$	Número de fallos en espera del componente $p$ durante el periodo de mantenimiento $m$
$t_{p,m,i}$	Instantes de tiempo durante el periodo de mantenimiento $m$ en el que sucede el fallo $i$ del componente $p$
$t_{p,m}$	Tiempo cronológico de los $m$ -mantenimientos sobre el componente $p$
$P$	Número de componentes $p$ idénticos
$t_p^*$	Tiempo de censura
$M_p$	Número de mantenimientos preventivos realizados durante el periodo de observación $t_p^*$
$H_{Mp+1}(t_p^*)$	Función de riesgo acumulada en el tiempo de censura $t_p^*$
$D_{Mp+1}(t_p^*)$	Probabilidad de fallo a la demanda acumulada en el tiempo de censura $t_p^*$

$\sigma$	Desviación típica
$u_R$	Indisponibilidad media debida a la falta de fiabilidad durante la vida útil del componente
$u_{R,S}$	Indisponibilidad media debida a la falta de fiabilidad relacionada con los fallos en espera durante la vida útil del componente
$u_{R,D}$	Indisponibilidad media debida a la falta de fiabilidad relacionada con los fallos en demanda durante la vida útil del componente
$u_R$	Indisponibilidad media debida a la falta de fiabilidad para la vida útil del componente
$u_T$	Indisponibilidad media debida a las pruebas de vigilancia
$u_M$	Indisponibilidad mediad debida al mantenimiento preventivo
$u_C$	Indisponibilidad mediad debida al mantenimiento correctivo
$u_O$	Indisponibilidad mediad debida al reemplazamiento del componente
$\varphi$	Tiempo fuera de servicio medio debido a las pruebas de vigilancia
$\delta$	Tiempo fuera de servicio medio debido al mantenimiento preventivo
$\mu$	Tiempo fuera de servicio medio debido al mantenimiento correctivo

### Capítulo 5: Aplicación de un modelo RAM dependiente del tiempo para la Toma de Decisiones Informada en el Riesgo

$u_R^D$	Indisponibilidad debida a la falta de fiabilidad asociada con los fallos ocultos detectados en las pruebas de vigilancia
$u_R^{UD}$	Indisponibilidad debida a la falta de fiabilidad asociada con los fallos ocultos que no son detectados en las pruebas de vigilancia pero si en las pruebas funcionales
$u_R^{UU}$	Indisponibilidad debida a la falta de fiabilidad asociada con los fallos ocultos que no son detectados por ninguna de las dos pruebas
$\lambda_0$	Tasa de fallos en espera residual
$\rho_0$	Probabilidad de fallo a la demanda residual
$\lambda_m(t)$	Tasa de fallos en espera dependiente del tiempo en el periodo $m$ tras el mantenimiento $m-1$
$\rho_m(t)$	Probabilidad de fallo a la demanda dependiente del tiempo en el periodo $m$ tras el mantenimiento $m-1$



$\lambda$	Máximo valor que alcanza la tasa de fallos en espera media entre dos pruebas para un tiempo de referencia
$\rho$	Máximo valor que alcanza la probabilidad de fallo a la demanda media entre dos pruebas para un tiempo de referencia
$\eta_S$	Eficiencia de las pruebas de vigilancia para detectar fallos en espera
$\eta_D$	Eficiencia de las pruebas de vigilancia para detectar fallos a la demanda
$\eta_R$	Eficiencia de las pruebas funcionales para detectar fallos en espera
$\lambda^D$	Fracción de la tasa de fallos detectada por la pruebas de vigilancia
$\lambda^{UD}$	Fracción de la tasa de fallos detectada por la prueba funcional
$\lambda^{UU}$	Fracción de la tasa de fallos no detectada por ninguna de las dos pruebas
$\rho^D$	Probabilidad de fallo a la demanda asociada con los fallos detectados por las pruebas de vigilancia
$\rho^U$	Probabilidad de fallo a la demanda asociada con los fallos no detectados por las pruebas de vigilancia
$TR$	Tiempo de referencia
$T$	Intervalo de pruebas de vigilancia
$M$	Periodo de mantenimiento preventivo
$RI$	Intervalo entre pruebas funcionales
$RP$	Vida útil del componente
$u_R$	Indisponibilidad debida a la falta de fiabilidad dependiente del tiempo
$u_T$	Indisponibilidad media debida a las pruebas de vigilancia
$u_M$	Indisponibilidad media debida al mantenimiento preventivo
$u_C$	Indisponibilidad media debida al mantenimiento correctivo
$u_O$	Indisponibilidad media debida al reemplazamiento del componente
$u_{MT}$	Indisponibilidad media debida a los tiempos fuera de servicio
$u_{RT}$	Suma de las contribuciones a la indisponibilidad debidas a la falta de fiabilidad y a las pruebas de vigilancia
$\varphi$	Tiempo fuera de servicio medio debido a las pruebas de vigilancia
$\delta$	Tiempo fuera de servicio medio debido al mantenimiento preventivo
$\mu$	Tiempo fuera de servicio medio debido al mantenimiento correctivo

$\theta$	Tiempo fuera de servicio medio debido a los reemplazamientos
$R$	Riesgo anual
$r$	Riesgo simple
$\Delta FDN$	Cambio en la Frecuencia de Daño al Núcleo
$FDN_a$	Frecuencia de Daño al Núcleo después del cambio
$FDN_b$	Frecuencia de Daño al Núcleo antes del cambio
$ICPDN$	Incremento Condicional de la Probabilidad de Daño al Núcleo
$u_i^b(t=0)$	Indisponibilidad inicial del componente $i$ antes del cambio
$u_i^a(t)$	Indisponibilidad del componente $i$ dependiente del tiempo después del cambio y proyectado para un horizonte de tiempo $t$
$B_i$	Birnbaum del componente $i$
$d_i$	Tiempo indisponible que permanece el componente $i$ para efectuar una prueba o una actividad de mantenimiento
$R_{RT}^{lim}$	Valor límite de riesgo de la contribución de las pruebas de vigilancia y falta de fiabilidad
$u_{MT}^{lim}$	Valor límite de indisponibilidad debida a los tiempos fuera de servicio
$R_{MT}^{lim}$	Valor límite de riesgo debido a los tiempos fuera de servicio

### **Capítulo 6: Evaluación del impacto en la fiabilidad humana y el riesgo para cambios en las ETF**

$P_d$	Probabilidad de error en la fase de diagnóstico
$P_e$	Probabilidad de error en la fase de ejecución
$\Delta FDN$	Cambio en la Frecuencia de Daño al Núcleo
$FDN_a$	Frecuencia de Daño al Núcleo después del cambio
$FDN_b$	Frecuencia de Daño al Núcleo antes del cambio
$FDN_0$	Frecuencia de Daño al Núcleo cuando se conoce con certeza que el equipo no está indisponible debido a un mantenimiento
$FDN_1$	Frecuencia de Daño al Núcleo cuando se conoce con certeza que el equipo está indisponible debido a un mantenimiento
$d_M$	Tiempo de indisponibilidad anual permitido debido a un mantenimiento

$d_{M,a}$	Tiempo de indisponibilidad anual permitido debido a un mantenimiento después del cambio
$d_{M,b}$	Tiempo de indisponibilidad anual permitido debido a un mantenimiento antes del cambio
$ICPDN$	Incremento Condicional de la Probabilidad de Daño al Núcleo
$f_M$	Frecuencia anual con la que un equipo se encuentra fuera de servicio debido a un mantenimiento
$u_M$	Indisponibilidad anual del equipo
$T_{\text{límite}}$	Temperatura umbral para arrancar el tren de reserva del Sistema de Extracción del Calor Residual
$T_{SRR}$	Temperatura del Sistema de Refrigerante del Reactor
$\Delta PEH$	Cambio en la Probabilidad de Error Humano



# Capítulo 1

## Introducción

### 1.1. Motivación y antecedentes

Garantizar la seguridad de las centrales nucleares ha sido un objetivo fundamental en el desarrollo de la energía nuclear desde el inicio de su aplicación industrial para la producción de energía eléctrica. En los últimos años, tras el accidente nuclear de Fukushima, Japón, en el año 2011, volvió a centrarse la atención sobre las medidas a adoptar con el fin de minimizar los riesgos, garantizando el máximo nivel de seguridad.

En este contexto, las autoridades reguladoras nacionales competentes de cada estado miembro de la Unión Europea (UE) requirieron a los titulares de las instalaciones a efectuar las llamadas pruebas de resistencia, consistentes en una reevaluación de los márgenes de seguridad de las centrales nucleares. Los resultados obtenidos señalaron la necesidad de introducir mejoras en las estrategias de seguridad nuclear de los países participantes. Además, supuso la revisión por parte de la Comisión Europea del marco jurídico y reglamentario vigente en materia de seguridad de las instalaciones nucleares comunitarias, aprobando la Directiva 2014/87/Euratom Consejo de la Unión Europea, de 8 de julio de 2014, por la que se establece un marco comunitario para la seguridad nuclear de las instalaciones nucleares (European Commission, 2017a).

En paralelo a los cambios en materia de regulación, los esfuerzos en investigación nuclear a nivel europeo por parte de la Comunidad Europea de la Energía Atómica (Euratom) en su Programa de Investigación y Formación (2014-18), que complementa el Programa Marco de la Unión Europea de Investigación e Innovación Horizonte 2020, han priorizado reforzar la seguridad de las tecnologías de fisión (European Commission,

2013). Dicha prioridad se incluyó también, a partir del año 2015, en el Plan Estratégico de Tecnologías Energéticas (SET Plan), el cual constituye la referencia de las políticas en tecnologías energéticas en la Unión Europea desde su creación en 2007.

En los sucesivos planes de trabajo que han configurado los cinco años del programa Euratom vigente, se ha incidido, en la importancia de mejorar la fiabilidad de estructuras, sistemas y componentes (ESC) que cumplen funciones de seguridad y que, por sus características, están próximas al fin de su vida de diseño. Esto implica el desarrollo y estudio de diversas áreas, como el Análisis Probabilista de Seguridad, el análisis de incertidumbres o la identificación y comprensión de los mecanismos de degradación de dichas ESC (European Commission, 2015). Más recientemente, siguiendo el trabajo relativo a la gestión de accidentes severos, el último plan de trabajo ha puesto el foco en el análisis y evaluación de la fiabilidad humana, incluyendo también su estudio para accidentes base de diseño (European Commission, 2017b). Euratom destaca ambos elementos como esenciales en la mejora de la seguridad y fiabilidad de los reactores actuales de segunda y tercera generación.

A nivel nacional, el Consejo de Seguridad Nuclear (CSN) vela por el funcionamiento seguro de las instalaciones nucleares y radiactivas, estableciendo los principios, criterios y normativa que regulan la seguridad nuclear en el territorio nacional. Entre las diferentes normas técnicas en esta materia, la Instrucción Técnica, IS-26, establece los requisitos básicos de seguridad nuclear aplicables a las centrales nucleares (CSN, 2010b). Dicha instrucción designa al titular de la instalación como responsable en el cumplimiento del objetivo principal de seguridad, definiendo para ello una serie de requisitos en las distintas fases del ciclo de vida de la instalación. Entre los requisitos generales a tener en cuenta durante el ciclo de vida, destacan aspectos relativos al análisis de seguridad, al análisis de riesgos o a los factores humanos.

Actualmente, uno de los grandes retos del parque nuclear español es el de la Operación a Largo Plazo (OLP). La OLP es la “operación continuada de la instalación manteniendo un nivel de seguridad aceptable, más allá de la vida de diseño de la instalación, tras realizar una evaluación de seguridad que asegure que se mantienen los requisitos de seguridad aplicables a las ESC de la misma” (CSN, 2017a). La mayor parte de las 6 centrales que lo conforman están próximas a alcanzar el fin de su vida de diseño, fechado en 40 años. La voluntad de los titulares es prolongar la vida inicialmente prevista de las centrales existentes, lo cual supondrá nuevos requisitos adicionales a la Revisión Periódica de Seguridad (RPS) por parte del CSN. La RPS generalmente se realiza cada 10 años, e incluye una valoración en conjunto de la seguridad industrial, analizando los efectos acumulativos del envejecimiento de las ESC importantes para la seguridad, las modificaciones de diseño realizadas y las mejoras relacionadas con cambios normativos (CSN, 2017a). Entre los nuevos requerimientos, se contempla la realización de una serie de estudios de gestión del envejecimiento que garanticen la funcionalidad de las ESC relacionados con la seguridad, considerando el nuevo periodo de explotación. Además, se solicita la revisión de los análisis de seguridad, que incluye los análisis probabilistas

(APS) y determinista (ADS), en la que se evalúe si las conclusiones de estos análisis son válidas teniendo en cuenta el periodo de operación a largo plazo.

Relacionados con los requisitos arriba mencionados, el Plan de I+D del CSN 2016-2020 destaca como áreas de investigación prioritarias en el ámbito de metodologías de análisis de seguridad, las siguientes (CSN, 2016b):

- Desarrollo y validación de metodologías de análisis de seguridad realistas. Técnicas de cuantificación de márgenes de seguridad y de sus incertidumbres, combinando métodos probabilistas y deterministas.
- Desarrollo de nuevas capacidades y actualización de los modelos de APS.
- Factores humanos y organizativos. Actualización de los análisis de fiabilidad humana (AFH) en los APS.
- Comportamiento humano y factores humanos y organizativos, en condiciones accidentales.
- Gestión informada por el riesgo. Aplicaciones de análisis probabilistas de seguridad.

Estas líneas de investigación están estrechamente relacionadas con las aportaciones realizadas en esta tesis. Ello demuestra la vigencia presente y futura del trabajo desarrollado y expuesto en este documento.

Las aportaciones que conforman esta tesis doctoral se integran en la línea de investigación financiada por el Ministerio de Economía y Empresa en el proyecto ENE2016-80401-R, “Armonización de requisitos de vigilancia y mantenimiento en centrales nucleares con información en el riesgo” y la ayuda para contratos predoctorales para la formación de doctores BES-2014-067602.

## 1.2. Objetivos y organización del trabajo

A partir del conocimiento sobre la gestión de envejecimiento mediante las actividades de mantenimiento y requisitos de vigilancia de las centrales, así como del actual estado del arte de modelos RAM (*Reliability, Availability and Maintainability*; fiabilidad, disponibilidad y mantenibilidad) para componentes de seguridad, modelos de fiabilidad humana, y uso del APS en la Toma de Decisiones Informada en el Riesgo, la presente tesis aborda dos cuestiones fundamentales.

Por un lado, la necesidad de definir un modelo RAM dependiente del tiempo para componentes de seguridad, ajustado con datos de planta y con un nivel de detalle suficiente como para evaluar el impacto del envejecimiento y de las actividades de vigilancia y mantenimiento en la edad real del mismo.

Por otro lado, demostrar la utilidad del modelo RAM dependiente del tiempo y las aportaciones al modelado y cuantificación de la probabilidad de error humano (PEH) mediante el uso conjunto del ADS y el APS, en el contexto de la Toma de Decisiones Informada en el riesgo (TDIR).

En este contexto, los objetivos concretos de la presente tesis son los siguientes.

El desarrollo de un modelo RAM para componentes de seguridad que incorpore el efecto explícito del envejecimiento y las actividades mantenimiento y requisitos de vigilancia sobre la edad real del componente. Se define en detalle un nuevo modelo de fiabilidad e indisponibilidad para la probabilidad de fallo a la demanda de un componente de seguridad, que evalúa de forma explícita los efectos del estrés causado por las demandas, la efectividad del mantenimiento y la eficiencia de las pruebas.

En segundo lugar, la estimación de los parámetros para los modelos de tasa de fallos en espera y la probabilidad de fallo a la demanda dependientes del tiempo de componentes de seguridad. Se obtienen los parámetros mediante técnicas de estimación frecuentistas o clásicas, a partir de datos reales de planta, seleccionando el modelo de mantenimiento imperfecto cuyo comportamiento mejor se ajusta al histórico dado.

Seguidamente, la validación del modelo RAM desarrollado, en el contexto de la TDIR. Se formula un modelo de riesgo dependiente de la edad a partir del modelo RAM, que permite comparar los resultados de diversas estrategias de requisitos de vigilancia y mantenimiento, con los criterios definidos para cambios en las Especificaciones Técnicas de Funcionamiento (ETF) y en la Regla de Mantenimiento (RM). Este modelo permite seleccionar la estrategia más adecuada en términos de indisponibilidad y riesgo para la planta.

Finalmente, el desarrollo de una metodología de evaluación del impacto en el riesgo para cambios en el tiempo de indisponibilidad permitido (*Completion Time*, CT) de un componente de seguridad, incluido en las ETF, usando un modelo de APS refinado mediante códigos termohidráulicos *best-estimate* (BE) y técnicas de AFH. El uso de códigos BE permite obtener nuevos escenarios accidentales no contemplados en el APS original. Así mismo, permite modelar y cuantificar con mayor precisión las PEH para las acciones involucradas en las secuencias accidentales. Se evalúan los cambios en la PEH y el impacto en el riesgo del cambio en el CT, incluyendo el tratamiento de incertidumbres de parámetro y de modelo.

La tesis se ha dividido en ocho capítulos, incluyendo este primero de introducción y el último relativo a las referencias bibliográficas empleadas en la elaboración de la misma.

En el segundo capítulo, “Estado del arte”, se expone una revisión bibliográfica de los aspectos más importantes objeto de estudio de esta tesis, como son el marco normativo de la investigación, los modelos RAM que consideran la degradación, los modelos de APS junto a las técnicas de análisis de fiabilidad humana y los fundamentos de la toma de decisiones informada en fiabilidad y riesgo.



En el tercer capítulo, “Modelo de indisponibilidad en demanda dependiente del tiempo”, se desarrolla un nuevo modelo de fiabilidad e indisponibilidad para la probabilidad de fallo a la demanda dependiente del tiempo para un componente de seguridad, en el cual se considera de forma explícita el estrés de las demandas, la efectividad de mantenimiento y la eficiencia de las pruebas.

En el cuarto capítulo, “Estimación de parámetros de un modelo de fiabilidad dependiente del tiempo”, se estiman los parámetros de un modelo RAM dependiente de la edad para un componente de seguridad, empleando datos reales de equipos instalados en una central nuclear, que tiene en cuenta la contribución debida al modo de fallo en espera y al modo de fallo en demanda. Se estudia la influencia en la indisponibilidad de los requisitos de vigilancia y las actividades de mantenimiento de ambas contribuciones respecto al total.

En el quinto capítulo, “Aplicación de un modelo RAM dependiente del tiempo para la Toma de Decisiones Informada en el Riesgo”, se define un modelo del riesgo dependiente de la edad partiendo del modelo RAM previamente desarrollado en el Capítulo 4. Este modelo de riesgo facilita la toma de decisiones relativa a la selección de estrategias de requisitos de vigilancia y mantenimiento de equipos de seguridad.

En el sexto capítulo, “Evaluación del impacto en la fiabilidad humana y el riesgo para cambios en las ETF”, se evalúa el impacto en la fiabilidad humana y el riesgo de cambios en las acciones humanas y el tiempo de indisponibilidad permitido de un componente de seguridad. A partir del uso de un código termohidráulico BE, se hallan nuevos escenarios accidentales en el modelo APS disponible y se cuantifican con mayor exactitud las PEH de las acciones humanas envueltas en el transcurso de la secuencia accidental. Mediante la comparación con los criterios de la normativa reguladora, se analiza el impacto en el riesgo de los cambios propuestos en el APS.

En el séptimo capítulo, se señalan las conclusiones más relevantes. Partiendo de las ideas iniciales que motivaron la investigación llevada a cabo, se subrayan los objetivos específicos cubiertos a lo largo del trabajo realizado. Adicionalmente, se delimitan las líneas futuras de investigación que se derivan de los resultados obtenidos. Para finalizar, se enumeran las publicaciones y participaciones en congresos producto de la tesis doctoral.



# Capítulo 2

## Estado del arte

### 2.1. Marco normativo

En este apartado se esboza el marco normativo nacional e internacional bajo el cual se engloba la investigación desarrollada en esta tesis. En primer lugar, se aborda la Revisión Periódica de Seguridad (RPS) en el contexto de la Operación a Largo Plazo (OLP), la cual confiere un papel esencial a la gestión del envejecimiento de estructuras, sistemas y componentes (ESC) importantes para la seguridad. A continuación, se expondrá el papel de las Especificaciones Técnicas de Funcionamiento (ETF) y la Regla de Mantenimiento (RM) como principales herramientas para garantizar la fiabilidad y disponibilidad de estas ESC. Por último, como parte esencial del Análisis Probabilista de Seguridad (APS), se describen los últimos avances en el modelado de la fiabilidad humana.

#### 2.1.1. Revisión Periódica de Seguridad y gestión del envejecimiento

La Instrucción IS-26, del Consejo de Seguridad Nuclear, sobre requisitos básicos de seguridad nuclear aplicables a las instalaciones nucleares, obliga al titular de toda instalación nuclear a establecer, implantar, evaluar y mejorar de forma continua las condiciones de seguridad nuclear y protección radiológica de su instalación (CSN, 2010b). La evaluación continua de la seguridad incluye, entre otros aspectos, el Plan de Gestión de Vida (PGV). Las actividades de gestión de vida útil, incluyen “la vigilancia de los mecanismos de envejecimiento y degradación de las estructuras, sistemas y componentes relacionados con la seguridad y el estado de los mismos, identificando las nuevas actividades de inspección, vigilancia y mantenimiento incorporadas para detectar dichos mecanismos y controlar sus efectos” (CSN, 2010b).

Además, la misma Instrucción IS-26, señala la necesidad de que el titular realice una RPS, cuyo objetivo es evaluar globalmente el comportamiento de la instalación durante el periodo considerado, con un máximo de 10 años, analizando de forma sistemática todos los aspectos de seguridad nuclear y protección radiológica. Como señala la Guía de Seguridad GS 1.10 (Rev. 2), sobre revisiones periódicas de la seguridad de las centrales nucleares, esta complementa la evaluación continua a través del análisis de los efectos acumulados del envejecimiento de las ESC importantes para la seguridad, el efecto en conjunto de las modificaciones de diseño realizadas y las mejoras en normas y estándares, con el fin de extender la operación a un nuevo periodo. La RPS pretende identificar posibles cambios, que mantengan o incrementen la seguridad de la central, garantizando unos niveles lo suficientemente elevados hasta la siguiente RPS o el final de la operación (CSN, 2017a).

Como se ha señalado en la introducción, la edad de la mayor parte de las centrales nucleares españolas es cercana a la determinada por su vida de diseño. La voluntad de los titulares es prolongar la vida inicialmente prevista de las instalaciones, lo cual supondrá nuevos requerimientos adicionales a la RPS por parte del CSN. Entre los requerimientos adicionales para autorizar la OLP de la central, se encuentra la presentación de documentación relativa a (CSN, 2017a):

- Plan Integrado de Evaluación y Gestión del Envejecimiento (PIE-GE), que debe contener los Estudios de Gestión del Envejecimiento (*Ageing Management Reviews*, AMR) y los Análisis de Envejecimiento en Función del Tiempo (*Time Limited Aging Analyses*, TLAA).
- Propuesta de suplemento del Estudio de Seguridad que debe incluir los estudios y análisis que justifican la operación a largo plazo de la central.
- Propuesta de revisión de las ETF que debe incluir los cambios necesarios para mantener las condiciones seguras de operación durante la operación a largo plazo de la central.

Por otro lado, la Instrucción IS-22, sobre gestión del envejecimiento y operación a largo plazo de centrales nucleares, regula la gestión del envejecimiento de los componentes de las centrales nucleares, sobre la base de la experiencia en los Estados Unidos en la aplicación de los requisitos del 10 CFR 54 *License Renewal Rule* promulgados por la Comisión Reguladora Nuclear de Estados Unidos (*Nuclear Regulatory Commission*, NRC) (USNRC, 1995a). El alcance de la instrucción técnica se limita a los componentes pasivos, es decir, a aquellos cuyo funcionamiento no depende de un factor externo, como puede ser un accionamiento, y carece de partes con movimiento. La IS-22 exige al titular de la central, una vez concedido el permiso de explotación a largo plazo, realizar las actividades necesarias de gestión del envejecimiento de las ESC de la central. Estas se incluyen en el denominado Plan de Gestión de Envejecimiento a Largo Plazo (PGE-LP), hasta el cese definitivo de la explotación.

Tanto el PGV y el PGE-LP se fundamentan esencialmente en los Programas de Gestión del Envejecimiento (PGE). Estos no son más que un enfoque del mantenimiento a largo plazo para cumplir unos requisitos reguladores, los cuales integran tareas de mantenimiento que en la mayoría de los casos ya forman parte del programa de mantenimiento de la central. Los PGE incluyen actividades de mantenimiento preventivo y correctivo, pruebas periódicas y vigilancias de las ETF, programas de inspección en servicio, programas de estudio de mecanismos de degradación, etc.

La gestión del envejecimiento de componentes activos, implica principalmente gestionar los niveles de fiabilidad e indisponibilidad de los mismos. Ambos se regulan de forma directa mediante las Especificaciones Técnicas de Funcionamiento y la Regla de Mantenimiento. Los Apartados 2.1.2 y 2.1.3 presentan el papel de ambos elementos, como puntales de la gestión indirecta del envejecimiento.

### ***2.1.2. Especificaciones Técnicas de Funcionamiento***

Como se ha mencionado anteriormente, entre los requerimientos adicionales del CSN a los titulares de las centrales para obtener el permiso de OLP, se incluye también la propuesta de revisión de las ETF (CSN, 2017a).

La seguridad de las centrales nucleares depende esencialmente de las ETF, las cuales “constituyen el conjunto de requisitos mínimos que garantizan la operación segura de una central nuclear”, como define la Instrucción IS-32 del CSN, sobre Especificaciones Técnicas de Funcionamiento de centrales nucleares (CSN, 2011). Las ETF son desarrolladas por el titular de la central como parte de la base de licencia, a partir de los análisis recogidos en su Estudio de Seguridad, estableciendo las condiciones de funcionamiento necesarias para evitar situaciones accidentales, así como mitigar sus consecuencias cuando estos no puedan evitarse. Estas definen los requisitos aplicables a las ESC relacionados con la seguridad y/o que sean significativos para el riesgo, de manera que garanticen su funcionamiento previsto en el Estudio de Seguridad en cualquier situación operacional, al igual que en cada uno de los transitorios y accidentes contemplados en su base de diseño (CSN, 2011).

Originalmente, las ETF fueron definidas a partir de los análisis deterministas y el juicio de expertos, caracterizándose por su alto grado de conservadurismo. Actualmente, el APS supone una herramienta fundamental en la implantación y modificación de las ETF. En particular, en los apartados relativos a cambios en las Condiciones Límites de Operación (CLO) y los Requisitos de Vigilancia (RV) (IAEA, 1993; Samanta, Kim, Mankamo, & Vesely, 1994).

Las CLO pretenden asegurar que las ESC relacionado con la seguridad, las cuales se encuentran normalmente en espera, estén disponibles en el momento en que se produzca una demanda real del equipo. Estas definen la mínima capacidad funcional que se requiere para la operación segura de ESC en los modos de operación aplicables, incluyendo límites de operación y número de equipos operables (CSN, 2011). Las CLO fijan las acciones a desarrollar sobre el componente y el tiempo de indisponibilidad permitido

(CT) en el cual se debe de restaurar el equipo a condiciones operativas. Algunas de las actividades que se realizan durante el tiempo de indisponibilidad se corresponden al mantenimiento correctivo, el mantenimiento preventivo y las pruebas.

Los RV definen las pruebas, calibraciones e inspecciones que aplican a ESC, especificando la frecuencia de ejecución con el fin de garantizar la operabilidad de los mismos dentro de las CLO (CSN, 2011). Durante el tiempo que se encuentran las ESC relacionadas con la seguridad en espera, pueden generarse indisponibilidades debidas a fallos, que se manifestarán en el momento en que se produzca una demanda sobre el equipo. Para prevenirlas, se determinará el intervalo de pruebas de vigilancia, definido como el máximo intervalo de tiempo permitido entre el desarrollo de pruebas de vigilancia consecutivas de un determinado componente o sistema.

### ***2.1.3. Regla de Mantenimiento***

Además de las ETF, las prácticas de mantenimiento resultan esenciales para asegurar que las ESC de una central nuclear son capaces de cumplir con su función prevista. Mantenimiento es “la combinación de todas las acciones técnicas y de gestión destinadas a mantener o restaurar un elemento en un estado que le permita funcionar como lo requerido” (IEC, 2015). En otras palabras, la misión del mantenimiento es asegurar, mantener o restaurar las capacidades operacionales de los componentes o sistemas, compensando la degradación que el tiempo y el uso provocan en los mismos.

Se distinguen dos tipos de mantenimiento principales: el mantenimiento correctivo y el mantenimiento preventivo. El mantenimiento correctivo devuelve a un equipo fallado o degradado a un estado que le permite llevar a cabo su función. Por otro lado, el mantenimiento preventivo incrementa la fiabilidad de los equipos no fallados antes de que pueda tener lugar una avería. Pese a que un equipo esté sujeto a ambos tipos de mantenimiento, puede degradarse más allá de su edad cronológica, en función de sus condiciones de trabajo operacionales y ambientales, así como de la efectividad del mantenimiento recibido. Con el fin de monitorizar la evolución de los mecanismos de degradación, además de actuar a través del lanzamiento de actividades correctivas en los casos que corresponda, se implantan distintos tipos de pruebas, como las de vigilancia y las funcionales.

En 1999 entró en vigor la Regla de Mantenimiento en las centrales nucleares españolas (CSN, 2016a), cuyo propósito es medir la eficacia de las prácticas de mantenimiento llevadas a cabo durante el periodo de explotación. Esta se remitía esencialmente a la normativa americana, 10 CFR 50.65 (USNRC, 1991a). Con el objeto de regular el requerimiento por parte del CSN de un sistema de vigilancia de la eficacia de las prácticas de mantenimiento en centrales nucleares, el CSN emitió en 2007 la Instrucción IS-15 (CSN, 2007b), cuya primera revisión se publicó en el año 2016, recogiendo la experiencia derivada de su aplicación práctica, así como la evolución de la normativa internacional en el transcurso de esos años.

Anteriormente a la publicación del 10 CFR 50.65, las ETF determinaban las operaciones de planta. Estas dictaban que equipos debían estar normalmente en funcionamiento, cuanto tiempo debían estar fuera de servicio y las medidas compensatorias y las pruebas de vigilancia que demostraban que los equipos estaban listos para actuar. Su objetivo principal sigue siendo garantizar la disponibilidad y fiabilidad de los equipos necesarios para prevenir, o dado el caso, mitigar accidentes. Compartiendo la misma meta, la RM conforma una metodología para verificar el cumplimiento de los programas de mantenimiento. Al igual que para las ETF, su alcance comprende los componentes activos, esto es, las ESC relacionados con la seguridad y aquellas no relacionadas con la seguridad que son utilizadas para mitigar accidentes o en procedimientos de operación de emergencia (CSN, 2016a).

Para alcanzar su propósito, la RM obliga a la monitorización de una serie de parámetros de las distintas ESC, los cuales se toman como criterios de comportamiento entre los que se encuentran los siguientes (CSN, 2016a):

- Disponibilidad de la función de seguridad del tramo, tren o sistema.
- Fiabilidad de la función del tramo, tren o sistema.
- Condición del sistema o estructura.
- Comportamiento a nivel de planta.

Estos parámetros, definidos como criterios de comportamiento, deben ser suficientemente sensibles como para detectar comportamientos degradados, manteniendo al mismo tiempo un balance entre fiabilidad e indisponibilidad, tanto desde el punto de vista determinista como de riesgo.

La RM representa el punto de partida de una regulación significativa para la evolución de las ETF. La NRC, en la línea de la postura adoptada para fomentar las aplicaciones del APS en materia reguladora (USNRC, 1995b), impulsó una serie de iniciativas para la mejora de las ETF. Aprovechando las sinergias en el uso conjunto de las ETF y la RM, se emprendió el camino hacia las llamadas *Risk Management Technical Specifications* (RMTS) (Hess, 2009), cuya base se estableció con las ETF informadas en el riesgo reguladas por la Guía Reguladora RG 1.177 (USNRC, 1998c).

#### **2.1.4. Análisis de Fiabilidad Humana**

El factor humano influye de forma sustancial en los niveles de fiabilidad y seguridad de los equipos y sistemas complejos. Por este motivo, su análisis sistemático mediante el Análisis de Fiabilidad Humana (AFH) resulta una parte crítica del APS. Dada la continua importancia del APS en materia reguladora, es fundamental aumentar la confianza en los resultados del mismo, y, por ende, de los obtenidos del AFH.

En España, el organismo regulador señala, en la Instrucción IS-25, sobre criterios y requisitos sobre la realización de los análisis probabilistas de seguridad y sus aplicaciones a las centrales nucleares, al titular de la instalación como responsable en “basar los APS

en modelos realistas de la respuesta de la planta y tener en cuenta las acciones humanas” (CSN, 2010a). De este modo, no obliga ni recomienda la utilización de ningún método o técnica particular, apuntando también que “los análisis de fiabilidad humana deberán realizarse teniendo en cuenta los factores que pueden influir en el comportamiento humano en todos los estados de la planta” (CSN, 2010a).

La NRC ha llevado a cabo diversas iniciativas para evaluar cuestiones relacionadas con la calidad del APS, las cuales se reflejaron documentalmente en la Guía Reguladora RG 1.200. Esta proporciona un enfoque adecuado para determinar la adecuación técnica de los resultados del APS en el contexto de la Toma de Decisiones Informada en el Riesgo (USNRC, 2009). No obstante, la guía reguladora presenta unos criterios generales, necesitando un análisis específico de determinadas áreas del APS.

Los problemas asociados con la calidad de los AFH empleados en los APS están relacionados esencialmente con las dos críticas más frecuentes a los mismos: la falta de coherencia entre los distintos puntos de vista de los expertos al evaluar la conducta humana y las diferentes hipótesis y supuestos que adoptan las diferentes técnicas, responsables de la gran variabilidad presente en los resultados (Kolaczowshi, Forester, Lois, & Cooper, 2006). Con el propósito de poder evaluar en base a unos determinados criterios la amalgama de técnicas existentes, la NRC publica en el año 2005 una guía de buenas prácticas para implementar los AFH (Kolaczowshi, Forester, Lois, & Cooper, 2005), para posteriormente, en el año 2016, publicar una comparación de los principales métodos empleados partiendo de criterios señalados en la misma (Kolaczowshi et al., 2006).

Sin embargo, los esfuerzos por parte de la NRC en este campo no han cesado, siendo la investigación en técnicas y datos para el AFH parte fundamental de las iniciativas reguladoras informadas en el riesgo para reactores en operación (USNRC, 2006). Como principal resultado, destaca el trabajo conjunto realizado entre el Instituto de Investigación de Energía Eléctrica (*Electronic Power Research Institute*, EPRI) y la NRC, descrito en el NUREG-2199 (J Xing et al., 2017). El primer volumen describe un nuevo método de AFH aplicable al APS a potencia para sucesos internos, que recibe el nombre de *Integrated Human Event Analysis System* (IDHEAS), y cuya base se centra en informes previos en los que se establece la base cognitiva del modelo (Whaley et al., 2016) y la metodología general del IDHEAS (Jing Xing & Chang, 2016). Los objetivos principales de esta nueva técnica son reducir la variabilidad entre los distintos analistas del AFH, mejorar la transparencia y la trazabilidad de los procesos del AFH y basarlo en el estado del arte de las áreas relativas a la cognición y comportamiento humanos.

En la actualidad, como se ha mencionado en la introducción, la actualización de los análisis de fiabilidad humana en los APS supone una línea prioritaria en el Plan de I+D del CSN 2016-2020 (CSN, 2016b). Concretamente el desarrollo de modelos avanzados para el cálculo de la probabilidad de fallo de acciones humanas en tareas de mantenimiento y de operación en sala de control.



## 2.2. Análisis Probabilista de Seguridad

El Análisis Probabilista de Seguridad (APS) de una central nuclear es una técnica de análisis de riesgos que permite estimar cuantitativamente el riesgo de una instalación. Este riesgo se define tradicionalmente como la probabilidad de un accidente multiplicado por las consecuencias que se derivan del mismo. Dicho de otra manera, el APS determina que puede ir mal, como de probable es, y cuáles son sus consecuencias (Kaplan & Garrick, 1981). Para ello parte de un modelado de la instalación en el que se desglosan las posibles secuencia de acontecimientos que pueden conducir a un accidente, y para cada una de esas secuencias, las posibles combinaciones de sucesos básicos o elementales que las pueden causar (CSN, 2010a). Las consecuencias en el ámbito nuclear se definen como el daño al público externo a la central.

El uso de técnicas de análisis de riesgos probabilistas se origina en los años 60 en la industria aeroespacial americana (Keller & Modarres, 2005a). La expansión de la industria nuclear norteamericana, con el consecuente aumento del tamaño de los reactores, supuso un empuje esencial al desarrollo de las metodologías de análisis de riesgo y análisis de fiabilidad desarrolladas hasta la fecha (Chelson, 1971). A comienzos de los 70, el organismo regulador americano predecesor de la NRC, la *United States Atomic Energy Commission* (AEC) impulsó una iniciativa para desarrollar una metodología probabilista que evaluará de forma completa el riesgo de accidentes en las centrales nucleares. Esta iniciativa culminaría con la publicación del Estudio sobre la Seguridad de los Reactores (WASH-1400) (USNRC, 1975). Bajo la dirección técnica del catedrático del *Massachusetts Institute of Technology*, Norman Rasmussen, se fundaron las bases del APS a partir del uso combinado del análisis de árboles de sucesos (*Event Tree*, ET) y árboles de fallos (*Fault Tree*, FT). Los árboles de sucesos caracterizan las relaciones entre éxito y fallo de sistemas con funciones críticas de seguridad, mientras que los árboles de fallos se emplean para calcular la probabilidad de fallo de dichos sistemas a partir de los datos de probabilidad de fallo de los componentes (Figura 2.1). Este enfoque ha resultado idóneo para el análisis de accidentes en reactores nucleares, cuya seguridad se cimienta en sistemas de seguridad en espera múltiples y redundantes (Keller & Modarres, 2005b).

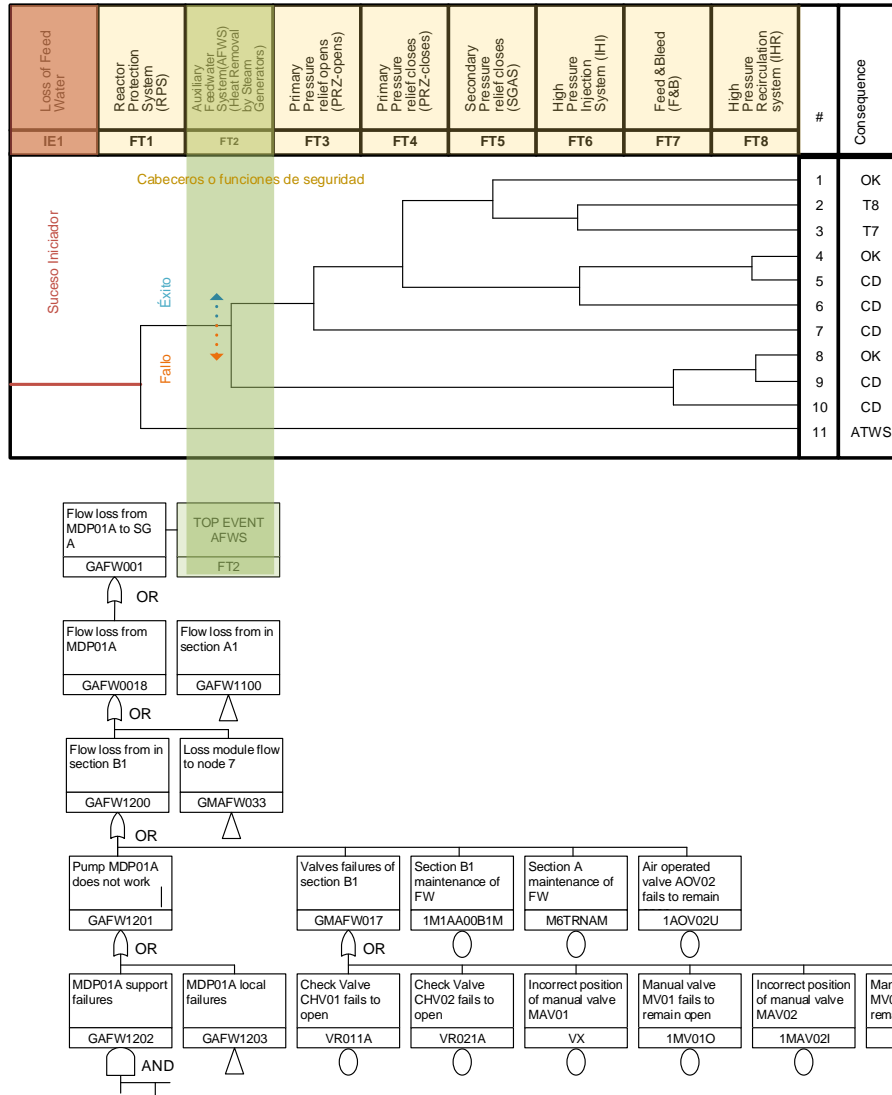


Figura 2.1 Ejemplo de árbol de eventos y árbol de fallos de un APS

El accidente de Three Mile Island (TMI), en el año 1979, puso de manifiesto algunas de los riesgos apuntados por el también llamado Informe Rasmussen, como la importancia de la actuación de los operadores, desencadenantes del siniestro ocurrido en la central estadounidense. Tras los sucesos de TMI, la NRC emprendió actividades dirigidas a la

mejora de la metodología APS, incluyendo un programa de investigación para el estudio de la evolución de los accidentes severos (USNRC, 1990). El paso definitivo en el desarrollo y mejora del APS en el ámbito de la seguridad nuclear y el análisis de riesgos se produciría en el año 1995 (USNRC, 1995b), con la adopción por parte de la NRC de una política para fomentar las aplicaciones del APS en materia reguladora, como complemento al tradicional enfoque determinista, dando lugar a la regulación informada en el riesgo (IAEA, 2005).

En el año 1986, siguiendo la estela de los programas del organismo regulador norteamericano, fue aprobado por el CSN el Programa integrado de realización y utilización de los análisis probabilistas de seguridad (CSN, 1986), cuyo primer objetivo fue la inclusión por parte de los propietarios de esta metodología en los estudios de seguridad de cada central, con el propósito de que su alcance fuera común y completo en todos ellos. Con la revisión del mismo en el año 1998, se persiguió alcanzar el segundo gran objetivo señalado en el título del programa, consistente en la utilización de los APS en aplicaciones que implicaran un beneficio para la seguridad.

El APS empleado en la industria nuclear distingue tres niveles:

- Nivel 1: estima la frecuencia de los accidentes que causan daño al núcleo, la suma de los cuales se conoce comúnmente como Frecuencia de Daño al Núcleo (FDN).
- Nivel 2: partiendo de los accidentes que causan daño al núcleo identificados en el Nivel 1, se estima la frecuencia de liberación de material radiactivo al exterior para cada secuencia. La suma de estas se conoce como Frecuencia de Grandes Liberaciones Tempranas (FGLT).
- Nivel 3: partiendo de las secuencias accidentales con liberación de material radiactivo al exterior extraídas del Nivel 2, se estiman las consecuencias en términos de daño al público y al medio ambiente.

Cada uno de los niveles del APS está relacionados con una barrera o nivel de protección, ligándolos así al concepto de defensa en profundidad. Los niveles se desarrollan de forma secuencial, tal y como se muestra en la Figura 2.2.

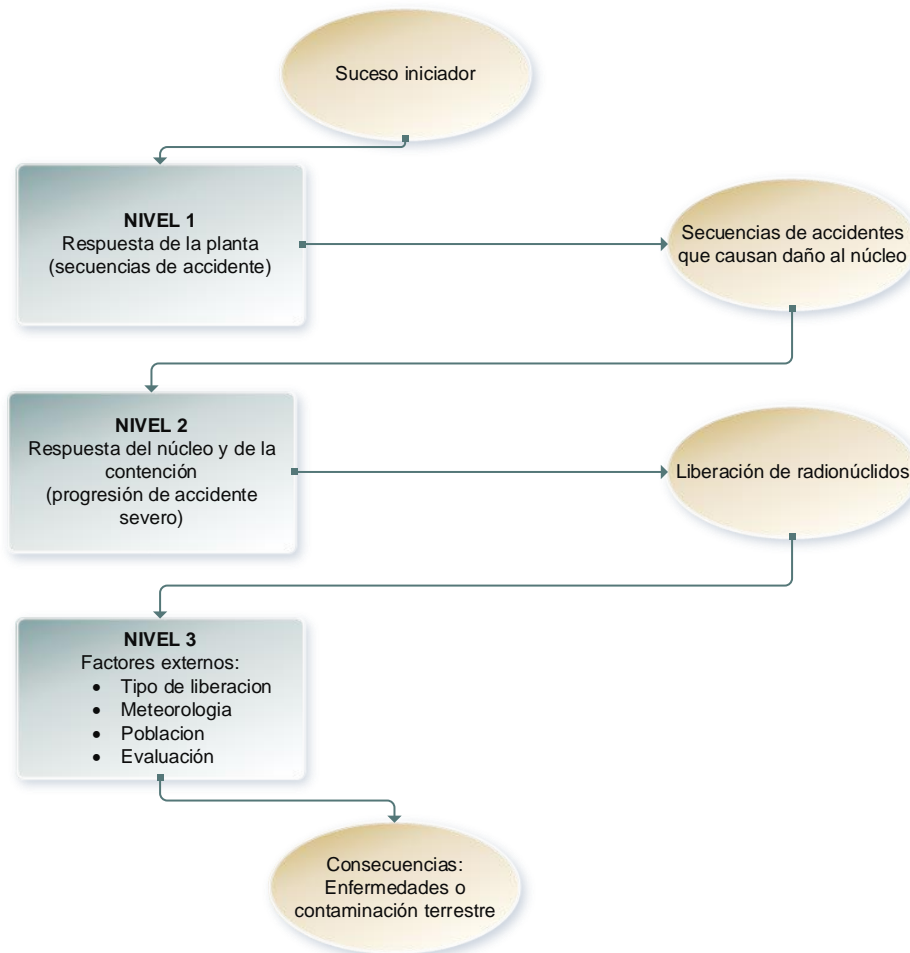


Figura 2.2 Niveles del APS<sup>1</sup>

Así mismo, también se distingue entre el APS a plena potencia y el APS en otros modos, en función de si los sucesos iniciadores contemplados en cada estudio tienen lugar en el modo de operación del reactor a plena potencia, o bien la central se encuentra aumentando o disminuyendo potencia. En caso de que no se especifique, en el texto las siglas APS se refieren al Análisis Probabilista de Seguridad a plena potencia.

<sup>1</sup> Fuente: (Díaz Bayona, 2018)

Actualmente, todas las centrales nucleares españolas disponen de un APS Nivel 1 y Nivel 2. La tendencia en estos últimos años se centra en la aplicación progresiva por parte de los propietarios y del CSN de las nuevas ideas implantadas por la NRC sobre regulación informada en riesgo, adaptando las guías y procedimientos al contexto español (CSN, 2007a, 2010a).

Los principales organismos reguladores sobre la energía atómica, nacionales e internacionales, han elaborado guías detalladas sobre la realización de APS para las centrales nucleares, como es el caso de la Organización Internacional de la Energía Atómica (*International Atomic Energy Agency*, IAEA) (IAEA, 1992, 2010b). Además, existe abundante bibliografía sobre el desarrollo en detalle de las distintas etapas que integran un APS (Kumamoto & Henley, 1996; Modarres, 2008). Debido al alcance de la investigación emprendida en esta tesis, se describe de forma breve las principales tareas de un APS de Nivel 1.

En primer lugar, se identifican y agrupan los sucesos iniciadores que pueden desencadenar un accidente. Posteriormente, se analizan las distintas secuencias accidentales, mediante la elaboración de los correspondientes árboles de sucesos para cada uno de los iniciadores. A continuación, se estudian los diferentes sistemas de seguridad que intervienen en la progresión de los árboles de sucesos, a través de la elaboración de sus respectivos árboles de fallos. La probabilidad de fallo o éxito de dichos sistemas se corresponde a la combinación de probabilidades de sucesos elementales o básicos, los cuales pueden corresponderse a un fallo independiente de un componente físico de la planta (válvula, bomba, etc.), a un fallo de causa común de un grupo de componentes o a un suceso de origen humano. La obtención de estas probabilidades, que son función del modelo de fiabilidad del componente o humana, y, por consiguiente, de la estimación de parámetros de los mismos, forma parte de la etapa de análisis de datos. En ella también se incluye la estimación de la frecuencia de los sucesos iniciadores. Una vez obtenidos todos estos datos, se procede a la cuantificación de la FDN total de la planta. Por último, se realizan análisis de los resultados, entre los que se incluyen los análisis de importancia, sensibilidad e incertidumbres.

Estos análisis permiten detectar e identificar las secuencias de accidentes más probables y los fallos de equipos o humanos que más contribuyen al riesgo. La información obtenida mediante los mismos permite introducir mejoras en el diseño o elaborar procedimientos para evitarlos, mejorar la formación en aquellos aspectos que más contribuyen al riesgo, establecer la frecuencia de las pruebas para los componentes más importantes, etc.

Los APS de las centrales nucleares españolas se actualizan, a día de hoy, cada 5 años, incorporando en los modelos, datos, etc. del conjunto de modificaciones y experiencias operativas significativas ocurridas en la planta desde la actualización previa, las que pudieran afectar al APS (CSN, 2017b). Esto impide realizar un seguimiento continuo de la repercusión en la seguridad de aspectos tales como el envejecimiento o la degradación de los componentes en función del tiempo y la política de mantenimiento y pruebas pro-

gramadas, limitándose a ofrecer una imagen estática para todo el periodo siguiente, mediante la asunción de tasas de fallo constantes para esos 5 años. Este perjuicio se volverá más relevante durante la OLP, donde los efectos del envejecimiento deberán ser evaluados y sometidos a un estricto seguimiento (IAEA, 2014)

Diversos autores han señalado la utilidad del APS en la evaluación de los efectos del envejecimiento sobre el riesgo de la planta (Kančev & Čepin, 2012; Martón, Sánchez, & Martorell, 2015; Nitoi & Rodionov, 2012; Volkanovski, 2012). En trabajos previos del Grupo de Medioambiente y Seguridad Industrial (MEDASEGI), adscrito al Departamento de Ingeniería Química y Nuclear de la Universitat Politècnica de València, se ha señalado la importancia de la inclusión de modelos de fiabilidad e indisponibilidad de componentes de seguridad dependientes del tiempo, que a su vez incluyeran el efecto de los programas de mantenimiento y pruebas y su correspondiente efectividad (Martón, 2014; A. I. Sanchez, 2000). Por otro lado también es extensa la experiencia del mismo en el uso del APS para aplicaciones informadas en el riesgo, más específicamente para cambios en las ETF (S. Martorell, Martón, Villamizar, Sánchez, & Carlos, 2014; S. Martorell, Villamizar, et al., 2014).

### **2.2.1. Modelos RAM dependientes de la edad**

El análisis de fiabilidad, disponibilidad y mantenibilidad, o en sus siglas anglosajonas, el análisis RAM (*reliability, availability and maintainability*), estudia tres parámetros esenciales en todo componente, sistema o estructura. Estos parámetros se pueden definir de la siguiente manera (IEC, 2015):

- La fiabilidad es la capacidad de un elemento para actuar sin fallo, durante un intervalo de tiempo dado, bajo unas condiciones dadas. Las condiciones dadas incluyen aspectos que afectan a la fiabilidad, como son el modo de operación, las condiciones ambientales, el nivel de estrés y el mantenimiento.
- La mantenibilidad es la capacidad de un elemento, bajo determinadas condiciones de uso, para conservar o ser restaurado a, un estado en el que pueda realizar la función requerida, cuando el mantenimiento se realiza bajo determinadas condiciones, usando procedimientos y recursos establecidos.
- La disponibilidad es la capacidad de un elemento para actuar cuando sea requerido. La disponibilidad depende de la fiabilidad, la mantenibilidad y del mantenimiento.

El objetivo de un análisis RAM, en cualquier ESC relacionado con la seguridad de una central nuclear, es minimizar la indisponibilidad del componente debida a fallos o requerimientos de mantenimiento e inspección para garantizar su funcionamiento en el caso de que sea solicitado.

El APS de una central nuclear considera normalmente un modelo de fiabilidad genérico para los componentes de seguridad, que está compuesto de al menos dos contribuciones asociadas con los modos de fallo en demanda y en espera. Estas son la probabilidad de

fallo a la demanda y la tasa de fallos en espera, respectivamente. Habitualmente, a ambos se les atribuye un valor contante en el APS, los cuales no tienen en cuenta la degradación del componente a causa del estrés por demandas y el envejecimiento (Atwood, Cronval, Patrik, & Rodionov, 2007). Estos parámetros son definidos como funciones de densidad de probabilidad, ajustados a partir de una función de distribución de probabilidad a priori (exponencial, log-normal, Weibull, etc.), dependiendo de cada componente en particular. Generalmente, se emplea el enfoque Bayesiano para combinar funciones de densidad de probabilidad con datos particulares de cada componente (Cadini & Gioietta, 2016; Cheng CY, 2005; Guure & Ibrahim, 2012; Guure, Ibrahim, & Ahmed, 2012).

Sin embargo, ambos modos de fallo suelen estar afectados tanto por el estrés de las demandas como por el envejecimiento, los cuales conducen a la degradación del componente hasta que en última instancia se produce su fallo. Las actividades de pruebas y mantenimiento se realizan con el fin de controlar la degradación y, consiguientemente, la fiabilidad y la indisponibilidad del mismo. No obstante, estas actividades tienen efectos positivos y negativos.

Los modelos RAM analíticos persiguen establecer de forma explícita la relación que existe entre los criterios RAM y las variables de interés correspondiente a la toma de decisiones. Los primeros avances en modelos de fiabilidad dependientes del tiempo nacieron al abrigo del programa de Investigación sobre el Envejecimiento de las Centrales Nucleares NPAR (*Nuclear Plant-Ageing Research*) de la NRC (USNRC, 1991b), dirigido a comprender los procesos de envejecimiento de las centrales, sus efectos potenciales sobre la seguridad, e investigar métodos para detectarlo y remediarlo. En su fase inicial, se desarrolló un modelo de envejecimiento lineal para la tasa de fallos en espera a nivel de componente (Vesely & Wolford, 1988). En el procedimiento de inclusión de los modelos dependientes de la edad en el APS ya se señalaba la influencia del mantenimiento y los intervalos de reemplazamiento (Vesely, Kurth, & Scalzo, 1990; Wolford, Atwood, & Roesener, 1992).

Posteriormente, Kim, Samanta, Martorell, & Vesely (1992) y Kim, Martorell, Vesely, & Samanta (1994) establecieron una base consistente sobre los efectos positivos y negativos derivados de las pruebas que se realizan a los componentes de seguridad, tanto para el modo de fallo en demanda como para el modo de fallo en espera. No obstante, este modelo no tenía en cuenta los efectos positivos del mantenimiento en función de su efectividad para gestionar la degradación del componente, fruto del estrés inducido por las demandas y el envejecimiento.

En lo que respecta al modo de fallo en espera, Sebastian Martorell, Sanchez, & Serradell (1999) propusieron un modelo dependiente de la edad en exclusiva para la tasa de fallos en espera. El modelo consideraba las condiciones ambientales y de trabajo, los efectos del envejecimiento en los componentes y, por último, los efectos positivos y negativos de las actividades de mantenimiento, mediante la adopción de modelos de mantenimiento imperfecto. Diversos autores han desarrollado modelos de indisponibilidad partiendo de estas variables, con el fin de optimizar la estrategia de pruebas y mantenimiento

teniendo en cuenta el envejecimiento (Kančev & Čepin, 2011; Martón, Martorell, Mullor, Sánchez, & Martorell, 2016; A. Sanchez, Carlos, Martorell, & Villanueva, 2009; Vaurio, 2009). Martón et al. (2015) propone un modelo de indisponibilidad para componentes relacionados con la seguridad asociado con los fallos en espera, el cual relaciona de forma explícita los efectos del envejecimiento, la efectividad del mantenimiento y la eficiencia de las pruebas. Estos modelos, no obstante, no recogen de forma explícita la degradación resultante del estrés inducido por las demandas.

Con relación al modo de fallo en demanda, su probabilidad en un componente de seguridad está afectada principalmente por el estrés de las demandas, entre las cuales se encuentran las demandas reales, las pruebas y otro tipo de demandas. El estrés debido a las demandas ha sido modelado como un proceso estocástico por saltos en Caballé, Castro, Pérez, & Lanza-Gutiérrez (2015); Choi, Lee, & Yang, 2010; Yang, Ma, Peng, Zhai, & Zhao (2017) y Zhang et al. (2016), sin tener en cuenta la degradación debida a las pruebas. Estos estudios consideran que se producen shocks aleatorios de acuerdo a un proceso de Poisson no homogéneo, que conduce de forma inmediata al fallo del componente. En Torres-Echeverría, Martorell, & Thompson (2009, 2011) se desarrolla un modelo que evalúa los efectos de la estrategia de pruebas en la probabilidad de fallo a la demanda para la instrumentación de sistemas de seguridad. Por último, Shin, Jeon, & Kang (2015) propone recientemente un modelo dependiente de la edad que considera entre otros factores, el efecto del “estrés por pruebas” y los efectos del mantenimiento.

### **2.2.2. Modelado de la PEH**

Las acciones humanas son una parte esencial de la operación y mantenimiento de las centrales nucleares, tanto en operación normal como en situaciones accidentales. Los errores humanos constituyen una de las principales contribuciones al riesgo de la central (USNRC, 1975), siendo posibles sucesos iniciadores de accidentes y jugando un papel fundamental en la mitigación de sus consecuencias. Los accidentes de TMI en 1979 o Chernóbil (1986) son dos ejemplos de la importancia de las acciones y decisiones humanas. Ambos casos señalaron la necesidad de plantear un estudio sistemático de la fiabilidad humana

El Análisis de Fiabilidad Humana (AFH) se lleva a cabo como parte del APS de una central nuclear para determinar cómo afecta la actuación humana a la seguridad de la planta de una forma estructurada, que permita identificar acciones humanas erróneas y estimar sistemáticamente la probabilidad de error de las mismas usando datos, modelos o juicio de expertos (ASME, 2000). Estas probabilidades reciben el nombre de Probabilidades de Error Humano (PEH).

El nacimiento de las técnicas de AFH se remonta a finales de los años 60. Desde mediados de los 80, varias metodologías han sido desarrolladas, las cuales se pueden dividir en dos categorías principales: los métodos de primera y de segunda generación (Di Pasquale, Iannone, Miranda, & Riemma, 2013). En la actualidad, se están desarrollando



métodos llamados de tercera generación, entendidos como una evolución de las generaciones anteriores (Bell & Holroyd, 2009).

Los métodos de primera generación están fuertemente influenciados por el punto de vista del APS. Otorgan al comportamiento humano un carácter esencialmente mecanicista, estableciendo una analogía entre el fallo humano y el fallo de un componente mecánico o eléctrico. Estos métodos atomizan las tareas a desempeñar por las personas en actividades humanas elementales, de las cuales se puede evaluar su fiabilidad ajustando su valor en función de la interdependencia entre ellas, o a través de una serie de factores como pueden ser el tiempo, el diseño de equipos, el estrés, etc. Estos factores, se conocen con el nombre de factores de influencia o *Performance Shaping Factors* (PSF). El modelo cognitivo adoptado por las técnicas de primera generación procede del modelo de J. Rasmussen (Rasmussen, 1983), el cual clasifica la conducta humana en tres niveles de funcionamiento: el nivel basado en habilidades, el nivel basado en reglas y el nivel basado en conocimientos.

Entre los métodos de primera generación destaca, por encima de todos ellos, el método *Technique for Human Error Rate Prediction* o método THERP (Swain & Guttmann, 1983). Su capacidad para integrarse en un análisis probabilista de riesgos, así como su extensa base de datos relativa a PEH procedente de la experiencia operacional y el juicio de expertos, lo constituyen como un referente entre las técnicas de AFH. Debido a la laboriosidad que requiere la cuantificación de las PEH, por el alto grado de detalle que exige su metodología, se desarrolló posteriormente una versión abreviada conocida como *Accident Sequence Evaluation Program* (ASEP) (Swain, 1987). Ambos métodos se sirven del *Time Reliability Correlation* (TRC) (Hall, Fragola, & Wreathall, 1982) para el cálculo de la PEH en la fase cognitiva, cuyo factor de influencia determinante es el tiempo disponible para realizar la acción.

También pertenece a esta generación el método *Success Likelihood Index Method* (SLIM) (Embrey, Humphreys, Rosa, Kirwan, & Rea, 1984), cuyo enfoque se basa en la estimación mediante juicio de expertos de las PEH. Además, el EPRI publicó el *Systematic Human Action Reliability Procedure* (SHARP) (Hannaman & Spurgin, 1984). El método SHARP no es una técnica en sí misma, sino un marco metodológico que se sirve de otras herramientas o técnicas para seleccionar y analizar acciones humanas relevantes para la seguridad de la planta y cuantificar su probabilidad de error humano. Supone un marco estructurado de trabajo que permite incorporar las interacciones humanas en el APS.

Los métodos de segunda generación, se aplicaron por primera vez en los años 90, utilizando un modelo cognitivo más acorde a los avances de la psicología sobre el estado del arte de los modelos de comportamiento humano (Di Pasquale et al., 2013). La descripción de los errores se aleja de la tradicional dicotomía omisión –comisión, dando especial importancia a los errores cognitivos y el impacto en ellos de los PSF. Además, consideran aspectos dinámicos en la interacción hombre-máquina, pudiendo ser usados como base para el desarrollo de simuladores para el operador (De Felice & Petrillo, 2018).

Algunas de las técnicas más representativas de esta segunda generación, y con una mayor repercusión en el ámbito nuclear son el *Standardized Plant Analysis Risk–Human Reliability Analysis Method* (SPAR-H) (Gertman, Blackman, Marble, Byers, & Smith, 2005), el *Cognitive Reliability and Error Analysis Method* (CREAM) (Hollnagel, 1998) y el *A Technique for Human Error Analysis* (ATHEANA) (Barriere et al., 2000).

En la actualidad, a partir de las limitaciones y defectos de los métodos de primera y segunda generación, nuevos métodos se están desarrollando con la catalogación de métodos de tercera generación. Dos de los métodos pertenecientes a esta última generación son *Nuclear Action Reliability Assessment* (NARA) y *Simulator for Human Error Probability Analysis* (SHERPA).

A nivel operativo, los documentos de guía de buenas prácticas en el campo del AFH desarrollados por la NRC, el NUREG-1792 (Kolaczkwshi et al., 2005) y el NUREG-1842 (Kolaczkwshi et al., 2006), permiten una mezcla de técnicas de diferentes generaciones para efectuar el AFH de los APS. En el Capítulo 6 se muestra un ejemplo de uso de distintas técnicas para estimar probabilidades de error humano.

### **2.3. Toma de decisiones informada en fiabilidad y riesgo**

Inicialmente, los enfoques deterministas fueron la referencia fundamental en la toma de decisiones en materia de seguridad de las centrales nucleares (Apostolakis, Cunningham, Lui, Pangburn, & Reckley, 2012; Nuclear Energy Agency, 2005; Zio & Pedroni, 2012). Los análisis deterministas de seguridad (ADS) se basaban en la asunción de hipótesis conservadoras en el modelado de las secuencias accidentales “creíbles”, las cuales eran seleccionadas por un juicio de expertos, experimentos e información operativa disponible hasta la fecha. Se analizaba para cada una de ellas el “escenario más desfavorable”, asumiendo que si las consecuencias derivadas del caso más desfavorable cumplían unos determinados criterios de aceptación, el resto de los casos los cumplirían igualmente (Zio & Pedroni, 2012). Esta metodología, nacida al abrigo del principio de “defensa en profundidad”, sirvió para establecer amplios márgenes de seguridad en el diseño de los primeros reactores a potencia, tratando de soliviantar la incertidumbre derivada de la falta de experiencia operativa, así como las limitaciones de los análisis de seguridad relativas a la estimación de probabilidades de los accidentes y sus consecuencias (Nourbakhsh, Apostolakis, & Powers, 2018).

La información en el riesgo en las normas de seguridad de esta primera etapa se ceñía a un plano cualitativo, tratando de diseñar la capacidad de los sistemas de seguridad de la planta en función de los accidentes base de diseño que comportarán consecuencias más graves para la seguridad y salud de las personas. No sería hasta el año 1975, con la publicación del Estudio sobre la Seguridad de las Reactores (WASH 1400) (USNRC, 1975), cuando se establecería el marco de aplicación de la metodología probabilista a la seguridad de los reactores nucleares. El WASH 1400 analizó dos reactores de agua ligera, un reactor de agua a presión (*Pressurized Water Reactor*, PWR) y un reactor de

agua en ebullición Una de las conclusiones principales del estudio fue la contribución mayoritaria al riesgo para las personas de aquellos accidentes caracterizados por una baja frecuencia y grandes consecuencias, tales como la fusión del núcleo o el fallo de la contención (Nourbakhsh et al., 2018). También se señaló en el estudio la importancia para la seguridad de los errores humanos, los fallos de causa común o los sistemas soporte.

El accidente de TMI, puso de manifiesto las carencias del enfoque determinista tradicional, señalando la necesidad de incluir evaluaciones del riesgo, capaces de detectar vulnerabilidades no identificadas hasta la fecha. Las políticas adoptadas por la NRC se dirigieron a incorporar la evaluación de riesgos en los procesos de toma de decisiones. Los esfuerzos realizados en esta dirección culminarían con la promulgación por parte de la NRC de una política para aumentar las aplicaciones del APS en materia reguladora, hasta el punto que el estado del arte lo permita, de forma que complemente el enfoque determinista (USNRC, 1995b). No obstante, esta política promovía, pero no requería, el incremento en el uso de estas técnicas. La ausencia de criterios en la toma de decisiones complicaba la implementación de dichas políticas.

En 1998, la Guía Reguladora RG 1.174 supuso un hito en la integración de la evaluación de riesgo en el proceso de toma de decisiones (USNRC, 1998a). Esta guía reguladora establece los principios del proceso de Toma de Decisiones Informada en el Riesgo (TDIR) de forma detallada (véase Figura 2.3). Específicamente, describe la aplicación del APS para la evaluación del impacto en el riesgo de cambios en la base de licencia de una central nuclear. Por primera vez, una normativa recoge las métricas de riesgo a tener en cuenta; Frecuencia de Daño al Núcleo (FDN) y Frecuencia de Grandes Liberaciones Tempranas (FGLT); y su variación en función del cambio propuesto, así como los criterios de aceptación de las mismas (véase Figura 2.4 y Figura 2.5). La RG 1.174 es la base de la llamada regulación informada en riesgo, cuyo desarrollo se extiende a partir de ese mismo año (USNRC, 1998b, 1998c, 1998d).



Figura 2.3 Principios básicos de las aplicaciones de APS<sup>2</sup>

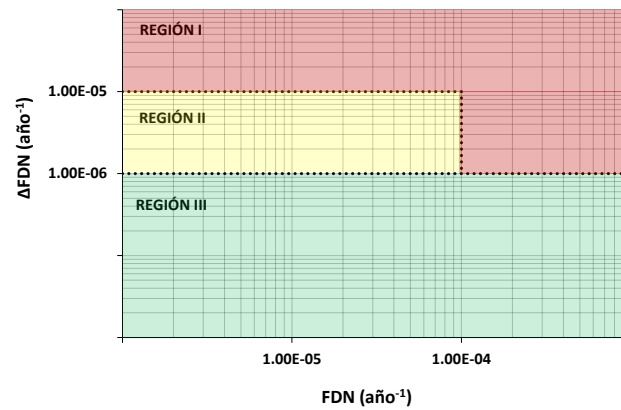
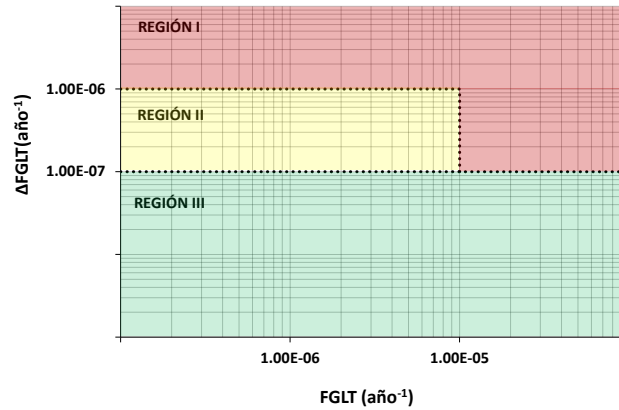


Figura 2.4 Criterios de aceptación para FDN

<sup>2</sup> Fuente: (CSN, 2007a)



**Figura 2.5** Criterios de aceptación para *FGLT*

A nivel nacional, las centrales y el CSN han adaptado las ideas implantadas por la NRC sobre regulación informada en riesgo, adaptando las guías y procedimientos a la realidad española. En este contexto se enmarca la publicación en el año 2007 de la Guía de Seguridad GS 1.14 (CSN, 2007a), donde se trasladan los principios de la TDIR, las métricas de riesgo y los criterios de aceptación descritos en la RG 1.174.

El enfoque de la TDIR vino acompañado, desde la aprobación en el año 1995 de la política sobre el uso de APS, de la necesidad de identificar y analizar todas las fuentes de incertidumbre con el fin de entender el impacto en el riesgo de las mismas. En este contexto, el EPRI y la NRC elaboraron sendas guías para la identificación, tratamiento y análisis de las incertidumbres (Drouin et al., 2009; EPRI, 2012). Trabajos anteriores del grupo de investigación, dentro del cual se ha desarrollado la presente tesis, muestran ejemplos en la aplicación de las directrices específicas en el tratamiento de incertidumbres para cambios en ETF (S. Martorell, Martón, et al., 2014; S. Martorell, Villamizar, et al., 2014). El Capítulo 6 se sirve de estas directrices para la evaluación del impacto en la fiabilidad humana y en el riesgo de un cambio en una ETF.



# Capítulo 3

## Modelo de indisponibilidad en demanda dependiente del tiempo

El presente capítulo delimita un modelo físico para componentes de seguridad que incorpora el efecto explícito del envejecimiento y las actividades de pruebas y mantenimiento sobre la edad real del componente. Partiendo del modelo de tasa de fallos en espera propuesto en Martón et al. (2015), se desarrolla un modelo para evaluar la probabilidad de fallo a la demanda de un componente de seguridad en función de la edad del equipo. Este modelo considera de forma explícita el efecto del estrés debido a las demandas, la efectividad del mantenimiento y la eficiencia de las pruebas. Se presentan diversos estudios de sensibilidad relativos a los diferentes parámetros que recoge el modelo. Este capítulo amplía el trabajo presentado en el artículo de P. Martorell, Martón, Sánchez, & Martorell (2017).

### 3.1. Modelo físico para un componente de seguridad

La Toma de Decisiones Informada en el Riesgo, en el contexto de los modelos RAM con degradación, requiere un modelo físico para los componentes de seguridad que reúna el suficiente grado de detalle como para evaluar de forma explícita el impacto del envejecimiento. Esto permitirá el desarrollo y definición de un modelo RAM dependiente del tiempo, así como modelos de riesgo que tengan en cuenta estos efectos. La Figura 3.1 proporciona una perspectiva general del modelo físico propuesto en esta tesis para componente de seguridad, como es el caso de motoválvulas (*motor operated valves*, MOV), motobombas (*motor driven pumps*, MDP) o generadores diésel (*diesel generators*, DG).

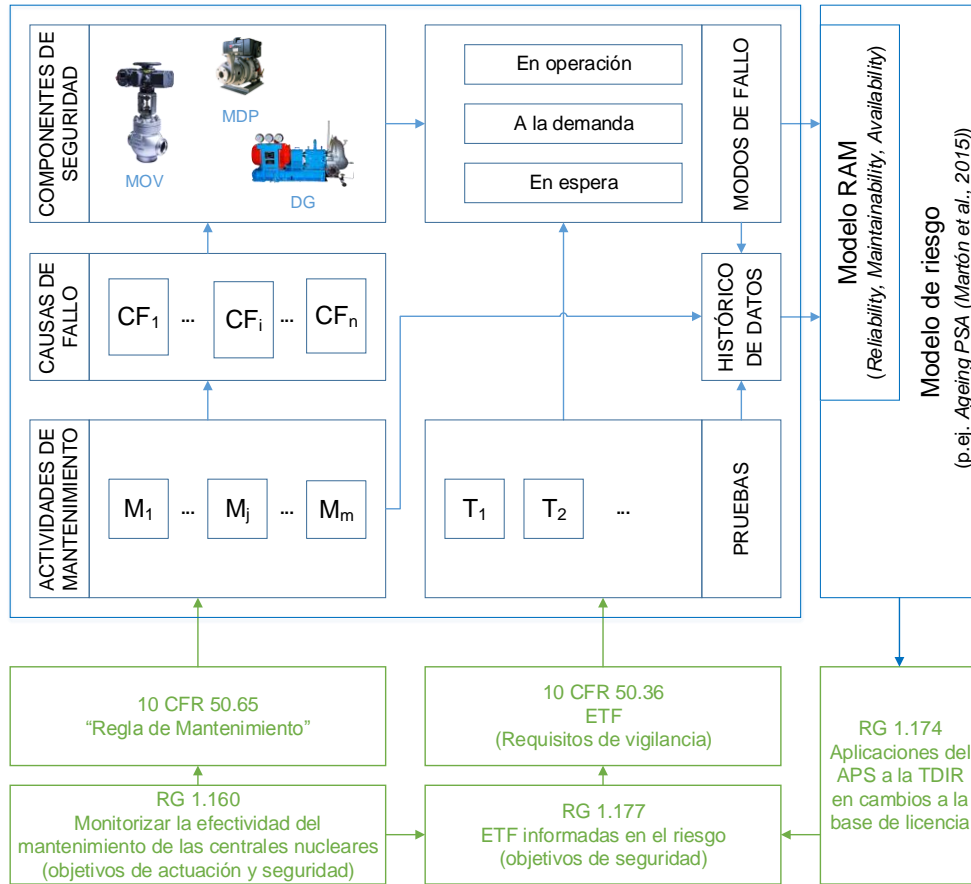


Figura 3.1 Modelo físico del funcionamiento de un componente de seguridad

El modelo físico asume que los componentes de seguridad normalmente se mantienen a la espera de una demanda, para entrar en operación y efectuar una función de seguridad en caso de una situación accidental de la central nuclear. Por consiguiente, los tres modos de fallo de un componente de seguridad que han de ser considerados son los fallos en espera, los fallos a la demanda y los fallos en operación. Como los equipos están normalmente en espera, pueden tener lugar fallos ocultos mientras el equipo permanece en ese estado. Por este motivo, los posibles tiempos fuera de servicio que podrían originar deben ser controlados con las pruebas de vigilancia ( $T_1, T_2, \dots$ ), como establecen las ETF. Las pruebas de vigilancia, sin embargo, constituyen una demanda real sobre el equipo, lo cual influye en el aumento de la probabilidad de fallo a la demanda. Además, las pruebas funcionales requieren actuar sobre el equipo y someterlo a unas condiciones



equivalentes a las solicitadas en un escenario accidental. Esto puede degradar el funcionamiento del equipo, es decir, aumentar la probabilidad de ocurrencia de cualquiera de los tres tipos de fallo.

La probabilidad de ocurrencia de un fallo para cualquiera de sus tres modos está ligado también a la edad del equipo, que es consecuencia directa del envejecimiento en función de sus causas de fallo dominantes ( $CF_1, CF_2, \dots$ ) o mecanismos de fallo que intervienen. Las actividades de mantenimiento ( $M_1, M_2, \dots$ ) se llevan a cabo con el fin de mantener las causas de fallo dominantes bajo control, retrasando la evolución de la edad del componente hasta el estado más nuevo posible. La RM impone los requisitos para la monitorización de la efectividad de dichas actividades.

La Figura 3.1 muestra una generalización del modelo particular adoptado para motoválvulas y motobombas en el caso de aplicación incluido en Martón et al. (2016). Como ejemplo, en el artículo, se descompone la MOV en dos subcomponentes: el actuador eléctrico y el cuerpo mecánico. Cada subcomponente está expuesto a un grupo distinto de causas de fallo o mecanismos de degradación que son controlado a través de actividades de mantenimiento eléctrico y mecánico, respectivamente. Se asume que los mecanismos de degradación y las actividades de mantenimiento solo afectan al modo de fallo en espera del equipo. Así, el efecto de estos no se tiene en cuenta para ni para el modo de fallo a la demanda, ni en operación. Además, solo se considera una prueba de vigilancia para controlar el tiempo fuera de servicio del componente como consecuencia de los fallos ocultos mientras el equipo se encuentra en espera.

La implementación de los requerimientos que establecen las ETF y la RM para una central nuclear permiten recoger un amplio historial de datos en relación a fallos, pruebas de vigilancia, pruebas funcionales y actividades de mantenimiento preventivo y correctivo. Todo este historial puede emplearse para ajustar el modelo RAM dependiente de la edad para cada componente de seguridad en particular, en función del modelo físico adoptado. Sin embargo, el nivel de detalle del modelo físico será seleccionado minuciosamente en función de la cantidad de datos que contenga el histórico. Puede darse el caso que, ante la ausencia de suficientes datos, sea imposible ajustar modelos RAM detallados que contengan un alto número de parámetros, obligando de esta forma a simplificar el modelo.

Volviendo al caso de aplicación expuesto en Martón et al. (2016), se selecciona un modelo de mantenimiento imperfecto para formular la tasa de fallos en espera de cada subcomponente que integra el componente de seguridad, considerando de forma explícita el efecto del envejecimiento, la eficiencia de las pruebas y la efectividad del mantenimiento. A partir del histórico de datos, se selecciona el modelo de fiabilidad y mantenibilidad más apropiado, así como los parámetros que mejor representan el comportamiento histórico del componente, a partir de la metodología expuesta por S. Martorell, Martorell, Sanchez, Mullor, & Martón (2017). Sin embargo, en consonancia con el modelo físico aquí adoptado, se asume que la probabilidad de fallo en demanda es constante. Además, no se considera la tasa de fallos en operación.

El modelo físico simplificado mostrado en la Figura 3.2 será adoptado de aquí en adelante. Este modelo asume que el impacto del envejecimiento, de las pruebas y el mantenimiento afecta a los modos de fallo en espera y en demanda de los componentes de seguridad, mientras que la tasa de fallos en operación permanece constante en su valor inicial.

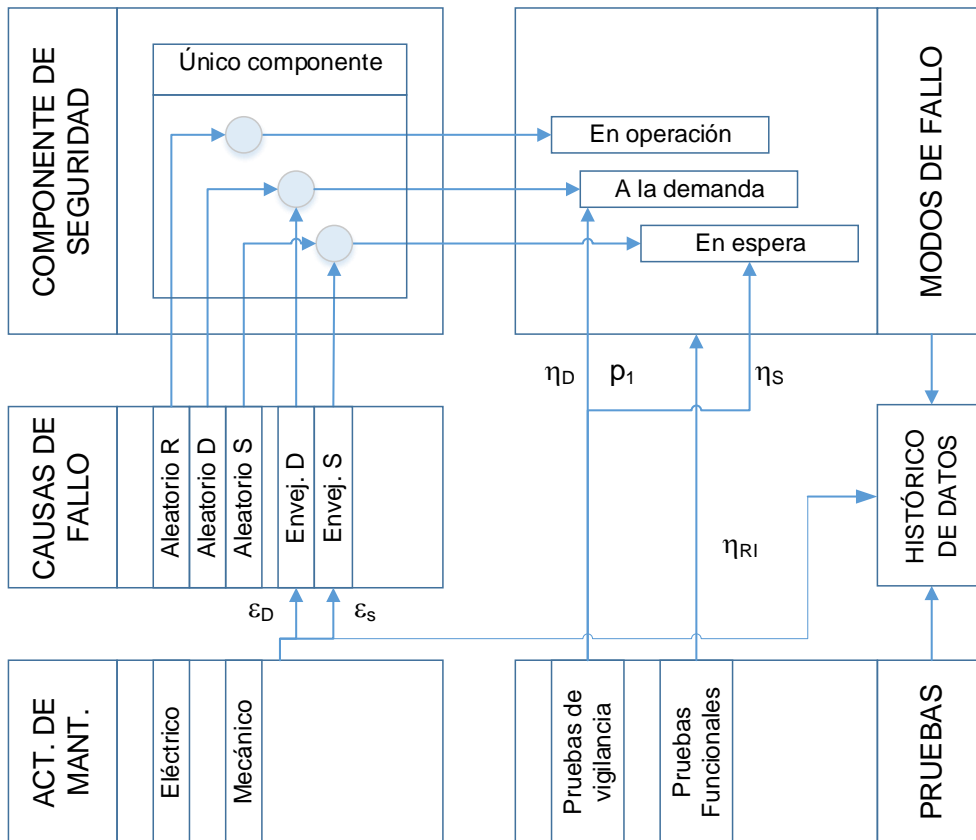


Figura 3.2 Modelo físico simplificado del funcionamiento de un componente de seguridad

### 3.2. Modelo de indisponibilidad básico para un componente de seguridad

El Análisis Probabilista de Seguridad (APS) de una central nuclear considera normalmente un modelo de fiabilidad genérico para los componentes de seguridad, que está compuesto de al menos dos contribuciones asociadas con cada uno de los modos de fallo;

la probabilidad de fallo a la demanda y la tasa de fallos en espera. Habitualmente, a ambos se les atribuye un valor contante en el APS,  $\rho_0$  y  $\lambda_0$ , respectivamente.

Sin embargo, ambos modos de fallo suelen estar afectados tanto por el estrés de las demandas como por el envejecimiento, los cuales conducen a la degradación del componente hasta que en última instancia se produce su fallo. Las actividades de pruebas y mantenimiento se realizan con el fin de controlar la degradación y, consiguientemente, la fiabilidad y la indisponibilidad del mismo. No obstante, estas actividades tienen efectos positivos y negativos.

Los primeros estudios documentados en Kim et al. (1992, 1994) han proporcionado una base consistente sobre los efectos positivos y negativos derivados de las pruebas que se realizan a estos componente, tanto para el modo de fallo en demanda como para el modo de fallo en espera. En Kim et al. (1992) se establecen los cimientos para considerar el envejecimiento y los efectos positivos y negativos de probar los componentes en la probabilidad de fallo a la demanda y la tasa de fallos en espera, definiendo un modelo de indisponibilidad para componentes de seguridad más realista. Más tarde, en Kim et al. (1994), se propone una simplificación del anterior modelo de indisponibilidad, el cual se formula de la siguiente manera:

$$u_R(n, t') = \rho(n) + \int_{nT}^{nT+t'} \lambda(n, u) du \quad t' \in [0, T]t \quad (3.1)$$

Siendo la contribución debida a fallos a la demanda:

$$\rho(n) = \rho_0 + \rho_0 p_1 n \quad (3.2)$$

Y la contribución debida a fallos en espera:

$$\lambda(n, u) = \lambda_0 + \lambda_0 p_2 n + \alpha v \quad v \in [0, nT + t'] \quad (3.3)$$

Donde  $n$  es el número de pruebas realizadas en el equipo en el tiempo cronológico  $t$ ,  $T$  es el intervalo de pruebas;  $t'$  es el tiempo transcurrido desde la última prueba,  $v$  es el tiempo transcurrido desde el último reemplazo;  $\rho_0$  es la probabilidad de fallo a la demanda residual;  $p_1$  es el factor de degradación asociado a los fallos a la demanda;  $p_2$  es el factor de degradación asociado a los fallos en espera;  $\lambda_0$  es la tasa de fallos en espera residual y  $\alpha$  es el factor de envejecimiento.

Las Ecuaciones (3.1) a (3.3) representan el modelo de indisponibilidad de un componente de seguridad considerando ambos modos de fallo, esto es, en demanda y en espera, y al mismo tiempo, integra la degradación del componente a consecuencia del estrés inducido por las pruebas y el envejecimiento lineal.

Sin embargo, este modelo no tiene en cuenta otros aspectos positivos y negativos derivados de la política de mantenimiento y pruebas, como son:

- La degradación debida al estrés de las demandas a las que es sometido el equipo dejando de lado las pruebas, como, por ejemplo, las demandas reales.
- El efecto positivo de la efectividad del mantenimiento para gestionar la degradación debida al estrés de las pruebas y el envejecimiento.
- El efecto negativo de la ineficiencia de las pruebas para detectar fallos.

En este contexto, el presente capítulo propone un nuevo modelo para la probabilidad de fallo a la demanda de un componente de seguridad, basado en el modelo de tasa de fallos en espera propuesto en Martón et al. (2015), que evalúa explícitamente los efectos del estrés causado por las demandas, la efectividad del mantenimiento y la eficiencia de las pruebas.

### **3.3. Modelo de la probabilidad de fallo a la demanda considerando el estrés causado por las demandas, la efectividad del mantenimiento y la eficiencia de las pruebas**

#### **3.3.1. Probabilidad de fallo a la demanda considerando el estrés causado por las demandas**

Teniendo en cuenta las contribuciones señaladas en la Ecuación (3.2), la probabilidad de fallo a la demanda de un componente, el cual se encuentra normalmente en espera y preparado para ejecutar una función de seguridad a la demanda, depende del número de demandas que haya satisfecho el componente. Habitualmente, estas demandas no están solo asociadas con las pruebas de vigilancia o funcionales, sino que también incluyen aquellas no planeadas por incidentes operacionales y pruebas realizadas tras la reparación del componente.

Una demanda operacional se define como un arranque manual o automático de un componente que no estaba previamente programada, como en el caso de las pruebas. La frecuencia de demandas no planeadas puede estimarse a partir de la experiencia operacional de una instalación como el número de demandas no planeadas dividida por el tiempo de operación (en años). Por ejemplo, para las turbobombas del sistema de inyección de alta presión y el sistema de refrigeración del núcleo del reactor aislado de una central nuclear se ha registrado una demanda por 2.5 reactores-año.

Las demandas asociadas con pruebas de vigilancia y funcionales son normalmente impuestas por las ETF, las cuales solicitan una demanda completa o una simulación del arranque automático de los componentes de seguridad. De este modo, como ejemplo, la frecuencia típica de una prueba funcional puede ser de 18 meses, lo cual suele equivaler al periodo de recarga (0.66 al año), mientras que para las pruebas de vigilancia los valores típicos suelen ser una por semana (52 al año), una al mes (12 al año), una por trimestre

(4 al año), etc., dependiendo de la importancia de la función de seguridad del componente.

El estrés causado por las pruebas no es, por lo tanto, la única contribución relevante al estrés causado por las demandas, especialmente para aquellos componentes que poseen una baja frecuencia de pruebas. No obstante, los componentes más importantes de una instalación suelen ser sometidos a un mayor número de pruebas de vigilancia, luego el estrés causado por las pruebas será probablemente la contribución más significativa al estrés total. Consecuentemente, la probabilidad de fallo a la demanda dependiente del tiempo dada en la Ecuación (3.2), puede ser reformulada en términos de una función de degradación dependiente del tiempo,  $f(t)$ , como sigue:

$$\rho(t) = \rho_0 + \rho_0 f(t) \quad (3.4)$$

Actualmente, el modelado de la probabilidad de fallo a la demanda en el APS puede simplificarse como  $\rho(t) = \rho_0$ , ya que no tiene en cuenta explícitamente el efecto de la degradación asociada al estrés por demanda. No obstante, estos efectos son limitados de forma implícita actualizando el APS de forma regular, como obliga la actual legislación en muchos países, como es el caso de España (CSN, 2017b). Asumiendo que el factor de degradación es el mismo para todo tipo de demandas e igual a  $p_1$ ,  $f(t)$  puede ser formulada como sigue:

$$f(t) = p_1 n(t) \quad (3.5)$$

Donde  $n(t)$  debe incluir el número de pruebas de vigilancia, de pruebas funcionales, de demandas operacionales, de pruebas tras mantenimiento preventivo y tras mantenimiento correctivo hasta el tiempo  $t$ .

Cuando solo se considera el estrés causado por las pruebas de vigilancia, la probabilidad de fallo a la demanda se representa a través de la Ecuación (3.4), mientras que la Ecuación (3.5) se simplifica para  $n(t) = \lfloor t/T \rfloor$ , donde  $T$  representa el intervalo de pruebas de vigilancia y  $\lfloor \cdot \rfloor$  es la función de parte entera que a cada número real asigna el número entero más próximo por defecto, es decir, el mayor número entero igual o menor que ese número real  $t/T$ . Esta simplificación se adopta en los siguientes apartados sin perder generalidad, con el fin de simplificar la introducción y formulación de los efectos positivos y negativos de los mantenimientos y las pruebas.

### 3.3.2. Probabilidad de fallo a la demanda considerando la efectividad del mantenimiento

Para introducir los efectos positivos del mantenimiento preventivo sobre la degradación debida al estrés causado por las demandas, se consideran dos modelos de mantenimiento imperfecto: el modelo *Proportional Age Setback* (PAS) y el modelo *Proportional Age Reduction* (PAR) (Sebastian Martorell et al., 1999; A. Sanchez et al., 2009).

### 3.3.2.1 Modelo PAS

El modelo PAS asume que cada actividad de mantenimiento reduce proporcionalmente la degradación del componente existente inmediatamente antes de llevar a cabo dicha actividad de mantenimiento, donde  $\varepsilon$  representa la efectividad del mantenimiento que oscila en el intervalo  $[0,1]$ . Si  $\varepsilon=0$ , el modelo PAS se simplifica a un modelo *Bad As Old* (BAO), en el que no influye la degradación acumulada hasta el momento. Por otro lado, si  $\varepsilon=1$ , el modelo se simplifica a un modelo *Good As New* (GAN), en el que el mantenimiento reduce la degradación del componente completamente, siendo su estado igual al inicial.

Por lo tanto, considerando la función de degradación  $f(\cdot)$  dependiente del número de pruebas de vigilancia, como se describe en la Ecuación (3.5), la función de degradación justo antes y después de llevar a cabo la primera actividad de mantenimiento,  $f_1^-$  y  $f_1^+$  respectivamente, puede ser formulada de la siguiente manera:

$$f_1^- = p_1 \left\lfloor \frac{t_1}{T} \right\rfloor \quad (3.6)$$

$$f_1^+ = p_1 (1 - \varepsilon) \left\lfloor \frac{t_1}{T} \right\rfloor \quad (3.7)$$

Siendo  $\varepsilon$  la efectividad del mantenimiento,  $T$  el intervalo de pruebas y  $\lfloor x \rfloor$  la función de parte entera que a cada número real  $x$  asigna el número entero más próximo por defecto. De esta forma, en las Ecuaciones (3.6) y (3.7), el término  $\lfloor t_1/T \rfloor$  representa el número de pruebas realizadas en el componente hasta la primera actividad de mantenimiento, que se realiza en el tiempo cronológico  $t_1$ .

Posteriormente, la función de degradación puede ser formulada justo antes y después de la segunda actividad de mantenimiento, que transcurre en el tiempo cronológico  $t_2$ , como sigue:

$$f_2^- = p_1 (1 - \varepsilon) \left\lfloor \frac{t_1}{T} \right\rfloor + p_1 \left\lfloor \frac{(t_2 - t_1)}{T} \right\rfloor \quad (3.8)$$

$$f_2^+ = p_1 (1 - \varepsilon) \left[ (1 - \varepsilon) \left\lfloor \frac{t_1}{T} \right\rfloor + \left\lfloor \frac{(t_2 - t_1)}{T} \right\rfloor \right] \quad (3.9)$$

De forma general, la función de degradación tras la actividad de mantenimiento  $m$  se formula de la siguiente manera:

$$\begin{aligned}
 f_m^+ &= p_1 \left\{ (1-\varepsilon)^m \left\lfloor \frac{t_1}{T} \right\rfloor + (1-\varepsilon)^{m-1} \left\lfloor \frac{(t_2 - t_1)}{T} \right\rfloor + \dots + (1-\varepsilon) \left\lfloor \frac{(t_m - t_{m-1})}{T} \right\rfloor \right\} \\
 &= p_1 \left\{ \sum_{k=1}^m (1-\varepsilon)^k \left\lfloor \frac{t_{m-k+1} - t_{m-k}}{T} \right\rfloor \right\}
 \end{aligned} \tag{3.10}$$

Ahora, asumiendo que las actividades de mantenimiento preventivo se realizan de forma regular con un intervalo de mantenimiento  $M$ , la Ecuación (3.10) se simplifica como:

$$f_m^+ = p_1 \frac{M}{T} \sum_{k=1}^m (1-\varepsilon)^k = p_1 \frac{M}{T} \sum_{k=0}^{m-1} (1-\varepsilon)^{k+1} = p_1 \frac{M}{T} (1-\varepsilon) \sum_{k=0}^{m-1} (1-\varepsilon)^k \tag{3.11}$$

El último término del lado derecho de la Ecuación (3.11) corresponde a la suma de una serie geométrica, donde el primer término de la serie es 1 y la razón  $(1-\varepsilon)$ . La ecuación se puede reformular de la siguiente manera:

$$f_m^+ = p_1 \frac{M}{T} (1-\varepsilon) \frac{1-(1-\varepsilon)^m}{1-(1-\varepsilon)} = p_1 \frac{M}{T} \frac{(1-\varepsilon)}{\varepsilon} (1-(1-\varepsilon)^m) \tag{3.12}$$

Y de forma similar se puede generalizar el valor de la función de degradación antes del mantenimiento  $m$  como:

$$f_m^- = p_1 \frac{M}{T} \frac{1-(1-\varepsilon)^m}{\varepsilon} \tag{3.13}$$

Las Ecuaciones (3.12) y (3.13) son funciones monótonas crecientes respecto a  $m$ , cuyo comportamiento asintótico queda definido por las siguientes expresiones:

$$f_a^+ = p_1 \frac{M}{T} \frac{(1-\varepsilon)}{\varepsilon} \tag{3.14}$$

$$f_a^- = p_1 \frac{M}{T} \frac{1}{\varepsilon} \tag{3.15}$$

Ahora, es posible extender la función de degradación dependiente del tiempo dada por la Ecuación (3.4), considerando el efecto de aplicar un mantenimiento imperfecto que sigue un modelo PAS. Luego, en el periodo número  $m$ , es decir, aquel que se sitúa entre el mantenimiento  $m-1$  y  $m$ , la evolución de la función de degradación del componente se puede representar como:

$$f_m(t) = f_{m-1}^+ + p_1 \left[ \frac{t - t_{m-1}}{T} \right] \quad t \geq t_{m-1} \quad (3.16)$$

A través de la Ecuación (3.4), la probabilidad de fallo a la demanda dependiente del tiempo que evalúa el estrés causado por las demandas y el efecto de las  $m-1$  actividades de mantenimiento realizadas, puede formularse para el periodo  $m$  como sigue:

$$\rho_m(t) = \rho_0 + \rho_0 f_m(t) \quad t \geq t_{m-1} \quad (3.17)$$

La Ecuación (3.17) puede particularizarse para  $t=t_m$ , inmediatamente después de realizarse el mantenimiento  $m$ , mediante las Ecuaciones (3.16) y (3.12). De esta forma, se expresa la probabilidad de fallo a la demanda tras el mantenimiento  $m$ :

$$\rho_m^+ = \rho_0 + \rho_0 p_1 \frac{M(1-\varepsilon)}{T\varepsilon} (1 - (1-\varepsilon)^m) \quad (3.18)$$

La Ecuación (3.18) puede ser reformulada como:

$$\rho_m^+ = \rho_0 + \Delta\rho_m^+ \quad (3.19)$$

Donde  $\Delta\rho_m^+$  representa el incremento en la probabilidad de fallo del componente, como consecuencia de la degradación acumulada debida a las demandas hasta la actividad de mantenimiento  $m$ , la cual se expresa para el modelo PAS como:

$$\Delta\rho_m^+ = \rho_0 p_1 \frac{M(1-\varepsilon)}{T\varepsilon} (1 - (1-\varepsilon)^m) \quad (3.20)$$

La Ecuación (3.20) representa una función monótona creciente de  $m$ , la cual tiene un comportamiento asintótico descrito por:

$$\Delta\rho_a^+ = \rho_0 p_1 \frac{M(1-\varepsilon)}{T\varepsilon} \quad (3.21)$$

Así, la probabilidad de fallo a la demanda entre dos actividades de mantenimiento consecutivas  $m-1$  y  $m$ ,  $\rho_m$ , puede ser formulada a través de la siguiente expresión:

$$\rho_m = \frac{1}{t_m - t_{m-1}} \int_{t_{m-1}}^{t_m} \rho_m(t) dt \quad (3.22)$$

Sustituyendo las Ecuaciones (3.17) y (3.16) en la Ecuación (3.22) y empleando la Ecuación (3.12), la probabilidad de fallo a la demanda entre dos actividades de mantenimiento consecutivas,  $m-1$  y  $m$ , viene dada por:



$$\rho_m = \rho_0 + \rho_0 p_1 \frac{M}{T} \left( \frac{1}{2} + \frac{(1-\varepsilon)}{\varepsilon} \left( 1 - (1-\varepsilon)^{m-1} \right) \right) \quad (3.23)$$

Cuando un componente se encuentra fuertemente degradado o en condiciones de fallo, debe ser reemplazado o restituido efectivamente como nuevo, llevarlo a un estado GAN. La Ecuación (3.24) muestra como la sustitución o renovación del componente a través del mantenimiento se considera en el modelo de degradación debida a las demandas del componente (Kim et al., 1992; A. Sanchez et al., 2009), mediante el cálculo de la probabilidad de fallo a la demanda media para la vida del componente,  $\rho_{m^*}$ , como sigue

$$\rho_{m^*} = \frac{1}{m^*} \int_0^{m^*} \rho_m dm \quad (3.24)$$

Donde  $m^* = (RP - M)$ , siendo  $RP$  la vida del componente. En un caso real,  $RP$  puede variar. En este caso, se puede adoptar un valor  $RP$  promedio (Vesely et al., 1990).

Sustituyendo la Ecuación (3.23) en la Ecuación (3.24) se alcanza la siguiente expresión, que describe la probabilidad de fallo a la demanda media para la vida del componente:

$$\begin{aligned} \rho_{m^*} &= \rho_0 + \rho_0 p_1 \frac{M}{T} \left( \frac{1}{2} + \frac{1}{m^*} \frac{(1-\varepsilon)}{\varepsilon} \int_0^{m^*} \left\{ 1 - (1-\varepsilon)^{m-1} \right\} dm \right) = \\ &= \rho_0 + \rho_0 p_1 \frac{M}{T} \left( \frac{1}{2} + \frac{(1-\varepsilon)}{\varepsilon} - \frac{(1-\varepsilon)^{m^*} - 1}{\varepsilon m^* \ln(1-\varepsilon)} \right) \end{aligned} \quad (3.25)$$

La Ecuación (3.25) puede ser reformulada como:

$$\rho_{m^*} = \rho_0 + \Delta\rho_{m^*} \quad (3.26)$$

Donde  $\Delta\rho_{m^*}$  representa el incremento medio en la probabilidad de fallo del componente, como consecuencia de la degradación acumulada debida a las demandas durante la vida del componente, el cual viene dado por:

$$\Delta\rho_{m^*} = \rho_0 p_1 \frac{M}{T} \left( \frac{1}{2} + \frac{(1-\varepsilon)}{\varepsilon} - \frac{(1-\varepsilon)^{m^*} - 1}{\varepsilon m^* \ln(1-\varepsilon)} \right) \quad (3.27)$$

La Ecuación (3.27) representa una función monótona creciente de  $m$ , la cual tiene un comportamiento asintótico descrito por:

$$\Delta\rho_{a^*} = \frac{1}{2} \rho_0 p_1 \frac{M}{T} \frac{(2-\varepsilon)}{\varepsilon} \quad (3.28)$$

### 3.3.2.2 Modelo PAR

El modelo PAR asume que tras cada actividad de mantenimiento, se reduce de forma proporcional al factor  $\varepsilon$  la degradación sufrida solo tras el último mantenimiento, mientras que la degradación acumulada previa no se ve alterada, siendo  $\varepsilon$  la efectividad del mantenimiento que oscila entre 0 y 1. De nuevo, se puede considerar que si  $\varepsilon=0$ , el modelo PAR se reduce a un modelo BAO, mientras que si  $\varepsilon=1$ , se reduce a un modelo GAN.

El valor de la función de degradación  $f(\cdot)$  para el modelo PAR se puede desarrollar análogamente al del modelo PAS del apartado previo. El valor de la función de degradación inmediatamente antes y después del primer mantenimiento está dado por las Ecuaciones (3.6) y (3.7), respectivamente. Para la segunda actividad de mantenimiento, la expresión de la función de degradación justo antes y después del mismo,  $f_2^-$  y  $f_2^+$  respectivamente, se formulan así:

$$f_2^- = p_1(1-\varepsilon)\left[\frac{t_1}{T}\right] + p_1\left[\frac{(t_2-t_1)}{T}\right] \quad (3.29)$$

$$f_2^+ = p_1(1-\varepsilon)\left[\frac{t_1}{T}\right] + p_1(1-\varepsilon)\left[\frac{(t_2-t_1)}{T}\right] \quad (3.30)$$

De forma general, la función de degradación tras la actividad de mantenimiento  $m$  se formula de la siguiente manera:

$$f_m^+ = p_1(1-\varepsilon)\left[\frac{t_m}{T}\right] \quad (3.31)$$

Asumiendo que las actividades de mantenimiento preventivo se realizan de forma regular con un intervalo de mantenimiento  $M$ , la Ecuación (3.31) representa una función monótona creciente respecto a  $m$  tal que:

$$f_m^+ = p_1 \frac{M}{T} (1-\varepsilon)m \quad (3.32)$$

y de forma similar

$$f_m^- = p_1 \frac{M}{T} ((1-\varepsilon)(m-1)+1) \quad (3.33)$$

Análogamente al desarrollo realizado para el modelo PAS, la Ecuación (3.17) puede particularizarse para  $t=t_m$ , inmediatamente después de realizarse el mantenimiento  $m$ , mediante las Ecuaciones (3.16) y (3.32). De esta forma, se expresa la probabilidad de fallo dependiente del tiempo,  $\rho_m$ , tras el mantenimiento  $m$ :

$$\rho_m^+ = \rho_0 + \rho_0 p_1 \frac{M}{T} (1 - \varepsilon) m \quad (3.34)$$

Así mismo, la Ecuación (3.34) puede reformularse de la siguiente manera:

$$\rho_m^+ = \rho_0 + \Delta\rho_m^+ \quad (3.35)$$

Donde  $\Delta\rho_m^+$  representa el incremento en la probabilidad de fallo del componente, como consecuencia de la degradación acumulada debida a las demandas hasta la actividad de mantenimiento  $m$ , la cual se expresa para el modelo PAR como:

$$\Delta\rho_m^+ = \rho_0 p_1 \frac{M}{T} (1 - \varepsilon) m \quad (3.36)$$

La probabilidad de fallo a la demanda media entre dos actividades de mantenimiento consecutivas  $m-1$  y  $m$ ,  $\rho_m$ , puede ser formulada a partir de la Ecuación (3.22). Sustituyendo las Ecuaciones (3.17) y (3.16), además de la Ecuación (3.32) para el modelo PAR, se alcanza la siguiente expresión:

$$\rho_m = \rho_0 + \rho_0 p_1 \frac{M}{T} \left( \frac{1}{2} + (1 - \varepsilon)(m - 1) \right) \quad (3.37)$$

La probabilidad de fallo a la demanda media a lo largo de la vida del componente,  $\rho_{m^*}$ , puede ser formulada a través de las Ecuaciones (3.24) y (3.37) de la siguiente forma:

$$\rho_{m^*} = \rho_0 + \frac{1}{2} \rho_0 p_1 \frac{M}{T} \left( 1 + (1 - \varepsilon)(m^* - 2) \right) \quad (3.38)$$

La Ecuación (3.38) puede ser reformulada como:

$$\rho_{m^*} = \rho_0 + \Delta\rho_{m^*} \quad (3.39)$$

Donde  $\Delta\rho_{m^*}$  representa el incremento medio en la probabilidad de fallo del componente como consecuencia de la degradación acumulada debida a las demandas durante la vida del componente, el cual viene dado por:

$$\Delta\rho_{m^*} = \frac{1}{2} \rho_0 p_1 \frac{M}{T} \left( 1 + (1 - \varepsilon)(m^* - 2) \right) \quad (3.40)$$

### 3.3.3. Probabilidad de fallo a la demanda considerando la eficiencia de las pruebas

El principal objetivo de las pruebas de vigilancia es detectar fallos ocultos, de manera que el componente puede ser restituido mediante un mantenimiento correctivo a un estado operacional idéntico al que poseía antes de la realización de la prueba. Este estado

sigue el comportamiento del llamado *Bad As Old*. La eficiencia de las pruebas de vigilancia a la hora de detectar fallos puede ser medida a través de un parámetro que recibe el nombre de eficiencia de la prueba,  $\eta$  (Martón et al., 2015).

Por lo tanto, la consideración de la eficiencia de las pruebas divide la probabilidad de fallo a la demanda total en dos contribuciones, la detectada y la no detectada, tal que:

$$\rho_{m^*} = \eta\rho_{m^*}^D + (1-\eta)\rho_{m^*}^U = \rho_{m^*}^D + \rho_{m^*}^U \quad (3.41)$$

Donde  $\eta$  es la eficiencia de la prueba, que oscila en el intervalo [0,1]. En la Ecuación (3.41), el primer término representa la probabilidad de fallo a la demanda asociada con los fallos detectados por las pruebas  $\rho_{m^*}^D$ , mientras que el segundo representa la probabilidad de fallo a la demanda asociada con los fallos no detectados por las pruebas,  $\rho_{m^*}^U$ . Ambos términos pueden ser obtenidos a partir de la formulación de  $\rho_{m^*}$ , introducida en el Apartado 3.3.2, la cual depende del modelo de mantenimiento imperfecto adoptado, PAS y PAR.

### 3.4. Modelo de indisponibilidad para el modo de fallo en demanda

Las contribuciones a la indisponibilidad de un componente que se encuentran normalmente en espera se dividen en dos categorías:

- a) La indisponibilidad debida a fallos aleatorios, esto es, a la falta de fiabilidad.
- b) La indisponibilidad debida a los tiempos que está fuera de servicio derivados de la realización de pruebas y/o mantenimientos.

#### 3.4.1. Indisponibilidad debida a la falta de fiabilidad

La indisponibilidad debida a la falta de fiabilidad de un componente normalmente en espera se compone de distintos términos, como se introdujo en la Ecuación (3.1). No obstante, en este apartado se limitará el estudio a aquellas contribuciones relacionadas con la probabilidad de fallo a la demanda.

Partiendo de las Ecuaciones (3.1) y (3.2), la indisponibilidad debida a la falta de fiabilidad causada por las demandas es una función de la probabilidad de fallo a la demanda del componente en el periodo  $m$ , es decir, en el periodo entre los mantenimientos  $m-1$  y  $m$ . La evolución de la indisponibilidad debida a la falta de fiabilidad dependiente del tiempo puede ser representada como:

$$u_{R,m}(t) = \rho_m(t) \quad (3.42)$$

A partir de la Ecuación (3.22), se puede formular de manera sencilla la indisponibilidad media debida a la falta de fiabilidad para el periodo entre los mantenimientos  $m-1$  y  $m$  como sigue:

$$u_{R,m} = \rho_m \quad (3.43)$$

Donde  $\rho_m$  es la probabilidad de fallo a la demanda media entre las actividades de mantenimiento  $m-1$  y  $m$ , la cual viene dada por las Ecuaciones (3.23) o (3.37), bajo la hipótesis de que el comportamiento de las actividades de mantenimiento que se realizan asuman un modelo PAS o PAR, respectivamente.

A partir de la Ecuación (3.24) se puede formular de manera sencilla la indisponibilidad media debida a la falta de fiabilidad para la vida útil del componente como:

$$u_R = \rho_m^* \quad (3.44)$$

Donde  $\rho_m^*$  es la probabilidad de fallo a la demanda media para la vida del componente, la cual viene dada por las Ecuaciones (3.25) o (3.38), bajo la hipótesis de que el comportamiento de las actividades de mantenimiento que se realizan asuma un modelo PAS o PAR, respectivamente. En el caso del modelo PAS, las Ecuaciones (3.43) y (3.44) presentan un comportamiento asintótico, como quedó demostrado en el Apartado 3.3.2.1.

#### 3.4.1.1 Evaluación del doubling time

Como se puede observar en la Ecuación (3.42), la falta de fiabilidad de un componente que se encuentra normalmente en espera, que se prueba y se mantiene de forma periódica, aumentará a lo largo del tiempo cuanto más pruebas se le realicen, a pesar de las actividades de mantenimiento llevadas a cabo. El incremento global en la contribución debida a la falta de fiabilidad del componente puede ser representada mediante la definición de un *doubling time* de falta de fiabilidad del componente, como propone Kim et al. (1992). En general, el *doubling time* debe entenderse como el tiempo cronológico a partir del cual la indisponibilidad debida a la falta de fiabilidad dependiente del tiempo, dada por la Ecuación (3.42), alcanza  $u_{R,m}(t)=2\rho_0$ . Esta definición se adopta de aquí en adelante de acuerdo a Kim et al. (1992), con el fin de tener en cuenta el efecto del mantenimiento.

Se considera la evolución dependiente del tiempo de la indisponibilidad debida a la falta de fiabilidad del componente dada por la Ecuación (3.42), la cual representa una función monótona creciente de  $m$ . Particularizándola para los modelos PAS y PAR tras realizar la actividad de mantenimiento  $m$ , mediante las Ecuaciones (3.18) y (3.34), se alcanza respectivamente:

$$u_{R,m}(t=t_m) = \rho_m^+ = \begin{cases} \rho_0 + \rho_0 p_1 \frac{M}{T} \frac{(1-\varepsilon)}{\varepsilon} (1-(1-\varepsilon)^m) & \text{Modelo PAS} \\ \rho_0 + \rho_0 p_1 \frac{M}{T} (1-\varepsilon)m & \text{Modelo PAR} \end{cases} \quad (3.45)$$

La efectividad del mantenimiento reduce la contribución debida a la falta de fiabilidad en cada actividad de mantenimiento llevada a cabo. El *doubling time*,  $t_D$ , se define en este caso como aquel en el que tras realizarse la actividad de mantenimiento  $m_D$ , la contribución debida a la falta de fiabilidad se reduce, pero no lo suficiente como para que sea menor al que impone la condición del *doubling time*, es decir,  $2\rho_0$ . De esta forma, en la Ecuación (3.45) se alcanzará dicha condición cuando  $u_{R,m}(t_m) \geq 2\rho_0$ . Esto significa que el segundo término de la suma del lado derecho de la Ecuación (3.45) debe ser mayor o igual al primer término, esto es,  $\rho_0$ . El número de actividades de mantenimiento en el cual se alcanza el *doubling time* se verifica para los modelos PAS y PAR, respectivamente, a través de las siguientes expresiones:

$$m_D = \begin{cases} \frac{\ln\left(1 - \frac{T\varepsilon}{p_1 M(1-\varepsilon)}\right)}{\ln(1-\varepsilon)} & \text{Modelo PAS} \\ \frac{T}{p_1 M(1-\varepsilon)} & \text{Modelo PAR} \end{cases} \quad (3.46)$$

El *doubling time* de la indisponibilidad debida a la falta de fiabilidad del componente puede ser estimado usando la Ecuación (3.46) y la relación  $t_D = m_D M$ . Así,  $m_D$  representa la actividad de mantenimiento a partir de la cual la falta de fiabilidad del componente permanece por encima del doble de su falta de fiabilidad inicial. Este tiempo es un buen indicador para restituir un componente, bien sea a través de un reemplazo o de un mantenimiento completo, siendo así  $RP = m_D M$ .

### 3.4.1.2 Indisponibilidad media debida a la falta de fiabilidad a lo largo de la vida del componente

La indisponibilidad media debida a la falta de fiabilidad a lo largo de la vida del componente,  $u_R$ , viene dada por la Ecuación (3.44), la cual se particulariza de la siguiente manera para los modelos PAS y PAR, respectivamente:

$$u_R = \begin{cases} \rho_0 + \rho_0 p_1 \frac{M}{T} \left( \frac{1}{2} + \frac{(1-\varepsilon)}{\varepsilon} - \frac{(1-\varepsilon)^m - 1}{\varepsilon m^* \ln(1-\varepsilon)} \right) & \text{Modelo PAS} \\ \rho_0 + \frac{1}{2} \rho_0 p_1 \frac{M}{T} (1 + (1-\varepsilon)(m^* - 2)) & \text{Modelo PAR} \end{cases} \quad (3.47)$$

Donde  $m^* = (RP - M)$  y  $RP$  es la vida del componente.

### 3.4.2. Indisponibilidad debida a los tiempos fuera de servicio

De acuerdo a Martón et al. (2015), las contribuciones a la indisponibilidad debida a los tiempos fuera de servicio como consecuencia de las actividades de pruebas y mantenimientos se evalúan mediante las siguientes expresiones:

$$u_T = \frac{\varphi}{T} \quad (3.48)$$

$$u_M = \frac{\delta}{M} \quad (3.49)$$

$$u_C = \frac{1}{T} \rho_m^D \mu \quad (3.50)$$

$$u_O = \frac{\theta}{RP} \quad (3.51)$$

Donde  $u_T$  es la indisponibilidad debida a la realización de pruebas de vigilancia,  $u_M$  es la indisponibilidad debida a la realización de mantenimiento preventivo,  $u_C$  es la indisponibilidad debida a la realización de mantenimiento correctivo y  $u_O$  es la indisponibilidad debida a los reemplazamientos. Los parámetros a través de los cuales se definen dichas contribuciones son los siguientes:

- $\varphi$  es el tiempo fuera de servicio medio debido a las pruebas de vigilancia.
- $\delta$  es el tiempo fuera de servicio medio debido al mantenimiento preventivo.
- $\mu$  es el tiempo fuera de servicio medio debido al mantenimiento correctivo.
- $\theta$  es el tiempo fuera de servicio medio debido a los reemplazamientos

De esta forma, la indisponibilidad media de un componente puede ser formulada como la suma de todas las contribuciones introducidas anteriormente, es decir:

$$u = u_R + u_T + u_M + u_C + u_O \quad (3.52)$$

### 3.5. Estudio de la evolución de la fiabilidad e indisponibilidad de un componente aplicando el modelo de probabilidad de fallo a la demanda dependiente del tiempo

Este apartado muestra la aplicación de los modelos propuestos para una motoválvula (MOV) genérica de una central nuclear. La Tabla 3.1 muestra los datos relativos a la fiabilidad, el envejecimiento, las pruebas y el mantenimiento de la MOV (A. Sanchez et al., 2009; Shin et al., 2015).

**Tabla 3.1 Valor de los parámetros de la MOV para el caso base**

Parámetro	Valor
$\rho_0$ (-)	1.82E-03
$p_1$ (-)	0.073
$T$ (-)	2190
$M$ (h)	13140
$\varepsilon$ (-)	0.6
$\eta$ (-)	1
$\delta$ (h)	1
$\varphi$ (h)	1
$\mu$ (h)	2.6
$\theta$ (h)	6
$RP$ (h)	87600

### 3.5.1. Fiabilidad dependiente del tiempo: modelos PAS y PAR

En primer lugar, se ofrece una comparación del comportamiento entre los modelos PAS y PAR presentados en el Apartado 3.3.2. La Figura 3.3 muestra la evolución de la probabilidad de fallo a la demanda en función del tiempo para ambos modelos. En la figura, es posible observar el comportamiento asintótico del modelo PAS frente al incremento lineal del modelo PAR. Como consecuencia, la probabilidad de fallo a la demanda solo alcanza la condición del *doubling time* descrita en el Apartado 3.4.1.1, la cual se representa con una línea de trazos verde en la Figura 3.3, para el modelo PAR. La línea a trazos negra representa el *doubling time*,  $t_D$ , el cual se asocia con la actividad de mantenimiento  $m_D$ , a partir de la cual el componente debería ser reemplazado, considerando la condición de alcance del *doubling time*.

Como se prevé en el modelo PAS, la probabilidad de fallo a la demanda del componente evoluciona con el tiempo mostrando un comportamiento asintótico. Por lo tanto, se puede asumir que, si se mantiene un intervalo de mantenimiento constante, se puede fijar la edad del componente a una constante o a un determinado nivel residual a largo plazo, y este dependerá de la efectividad del mantenimiento y del intervalo de pruebas y mantenimiento.



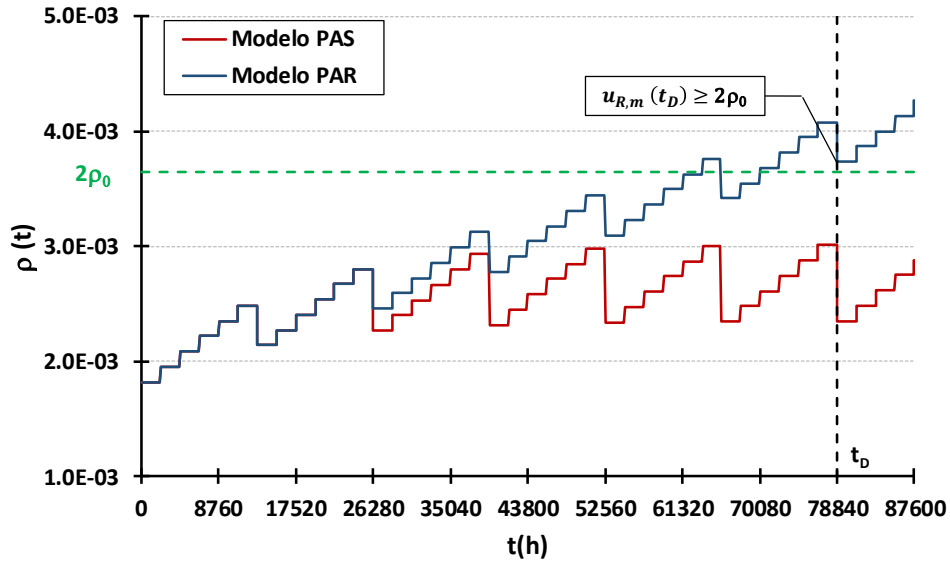


Figura 3.3  $\rho(t)$  del componente para los modelos de mantenimiento imperfecto PAS y PAR

### 3.5.2. Sensibilidad de $\rho(t)$ para el intervalo de mantenimiento

La Figura 3.4 y la Figura 3.5 muestran el resultado de realizar un análisis de sensibilidad de  $\rho(t)$  para distintos periodos de mantenimiento,  $M$ , para los modelos PAS y PAR, respectivamente. Para el modelo PAS, se observa que, para una efectividad del mantenimiento constante,  $\varepsilon=0.6$ , si el periodo de mantenimiento  $M$  se extiende, el comportamiento asintótico se alcanza más tarde, luego  $\rho(t)$  aumenta. Así, para  $M=18$  meses, el valor asintótico  $\rho_m^+$  tiende a un valor de  $2.35E-03$ , alcanzado tras 52560 horas de funcionamiento. Para el resto de casos estudiados, no se aprecia la adopción del mencionado comportamiento asintótico, que con certeza se alcanzará posteriormente. La probabilidad de fallo a la demanda sí que alcanza el doble de su valor original en los mismos. Este valor se alcanza más tempranamente si se extiende el periodo de mantenimiento, como lo demuestra el hecho de que para  $M=3$  años y  $M=5$  años se alcance a las 45000h y a las 30000h respectivamente. Por otro lado, en el modelo PAR se alcanzan los tiempos del *doubling time* en 8000h, 45000h, y 60000h para  $M=18$  meses,  $M=3$  años y  $M=5$  años, respectivamente.

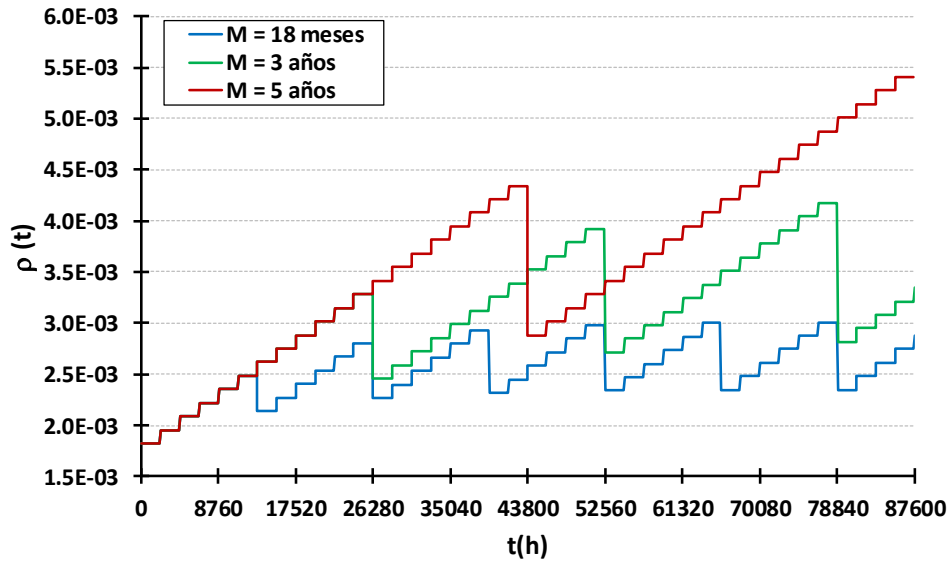


Figura 3.4  $\rho(t)$  del componente para diferentes periodos de mantenimiento del modelo PAS

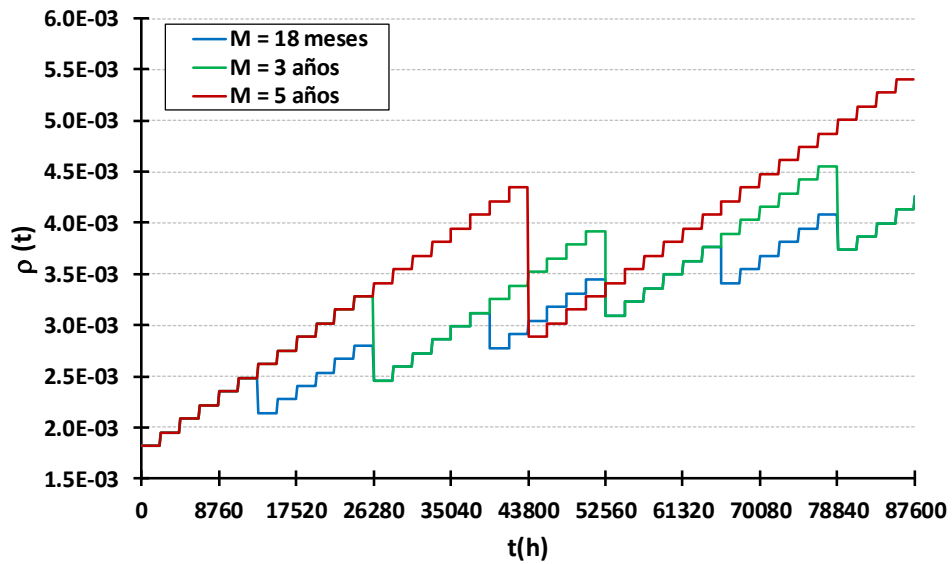


Figura 3.5  $\rho(t)$  del componente para diferentes periodos de mantenimiento del modelo PAR

### 3.5.3. Sensibilidad de $\rho(t)$ para la efectividad del mantenimiento

La Figura 3.6 y la Figura 3.7 muestran el resultado de realizar un análisis de sensibilidad de  $\rho(t)$  en función de distintos valores de la efectividad del mantenimiento para los modelos PAS y PAR, respectivamente. El intervalo de mantenimiento se mantiene constante en  $M=18$  meses. Para el modelo PAS se observa que, si la efectividad del mantenimiento aumenta, el comportamiento asintótico se alcanza más rápidamente. Este hecho es coherente con la función del mantenimiento como herramienta de mejora del estado del componente. De esta forma, para valores de  $\varepsilon=0.4$  el comportamiento asintótico no es alcanzado tras 10 años de funcionamiento del componente, mientras que para valores de  $\varepsilon=0.6$  y  $\varepsilon=0.8$ , la función  $\rho(t)$  tiende a  $\rho_a^+=2.35E-03$  y  $\rho_a^+=1.99E-03$ , respectivamente. El *doubling time* no se alcanza en ninguno de los casos planteados, aunque el caso más desfavorable se produce para una baja efectividad del mantenimiento. Por otro lado, como era previsible, para todos los casos estudiados con el modelo PAR se alcanza el *doubling time*. Se puede deducir que la pendiente y, por ende, el valor de  $\rho(t)$ , se suaviza en función del incremento de la efectividad del mantenimiento.

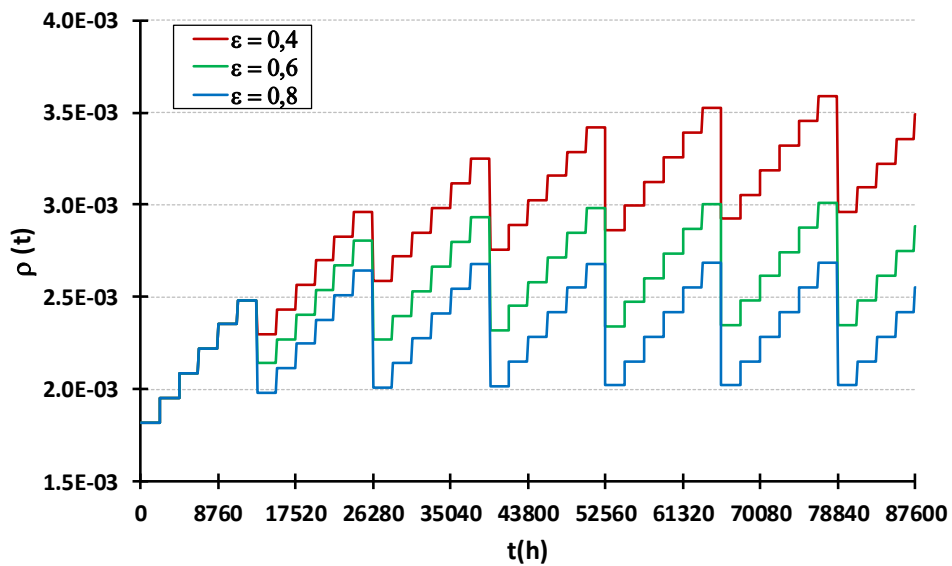


Figura 3.6  $\rho(t)$  del componente para diferentes efectividades del mantenimiento del modelo PAS

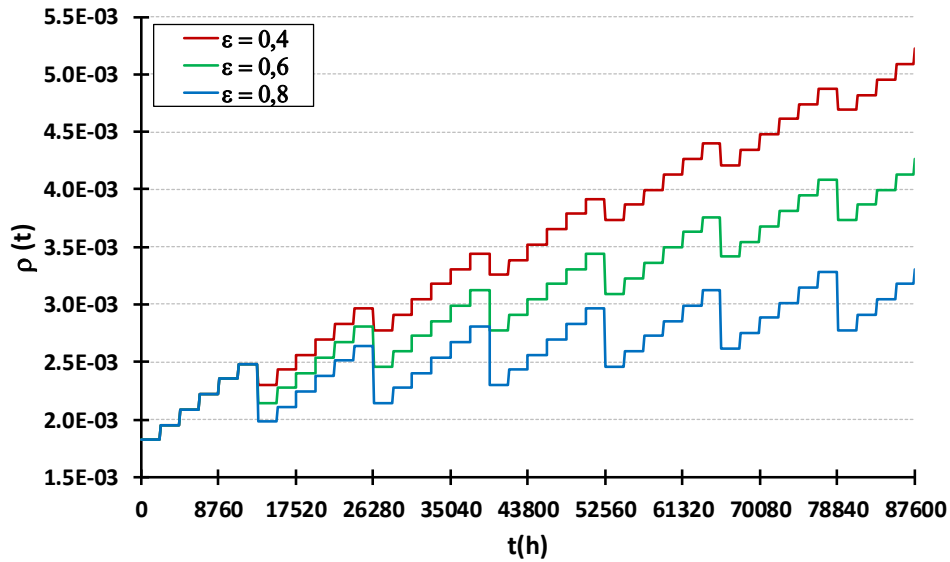


Figura 3.7  $\rho(t)$  del componente para diferentes efectividades del mantenimiento del modelo PAR

### 3.5.4. Sensibilidad de $\rho(t)$ para el intervalo de pruebas

La Figura 3.8 y la Figura 3.9 muestran el resultado de realizar un análisis de sensibilidad de  $\rho(t)$  en función de distintos intervalos de pruebas,  $T$ , para los modelos PAS y PAR, respectivamente. El intervalo de mantenimiento y la efectividad del mismo se mantienen constantes en  $M=18$  meses y  $\epsilon=0.6$  respectivamente. Para el modelo PAS se observa que el comportamiento asintótico es independiente de la periodicidad a la que se somete la motoválvula a las pruebas. En ambos modelos queda patente que la pendiente en la evolución de la probabilidad de fallo a la demanda aumenta cuando el intervalo de las pruebas decrece.

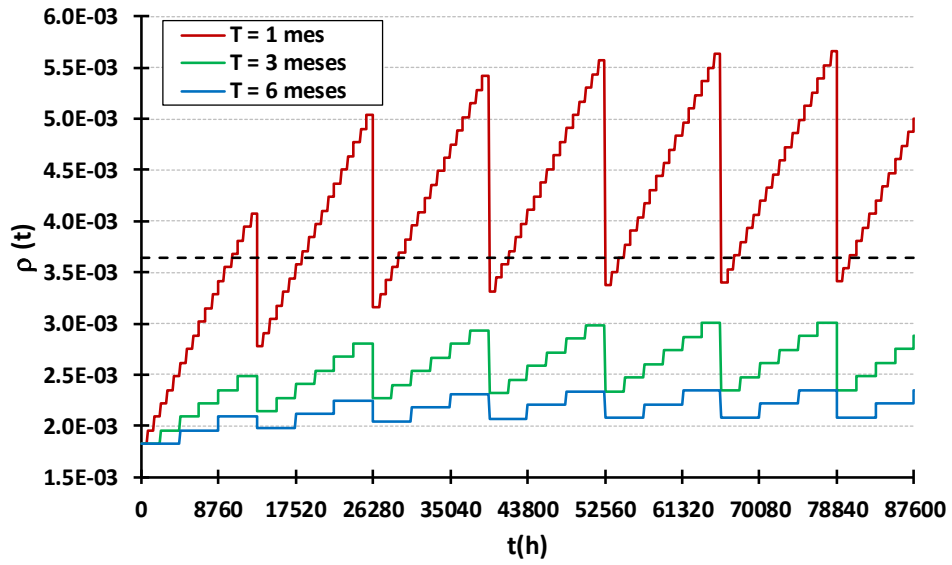


Figura 3.8  $\rho(t)$  del componente para diferentes intervalos de pruebas del modelo PAS

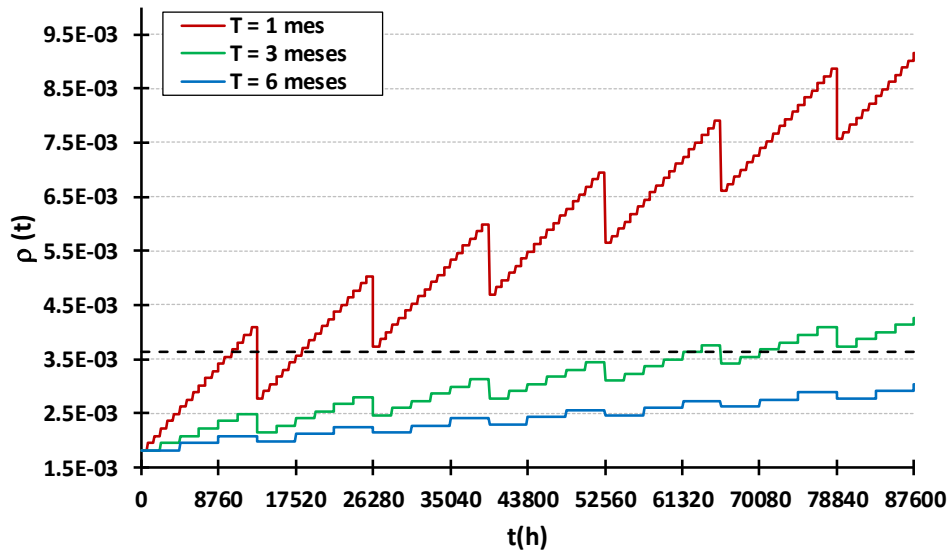
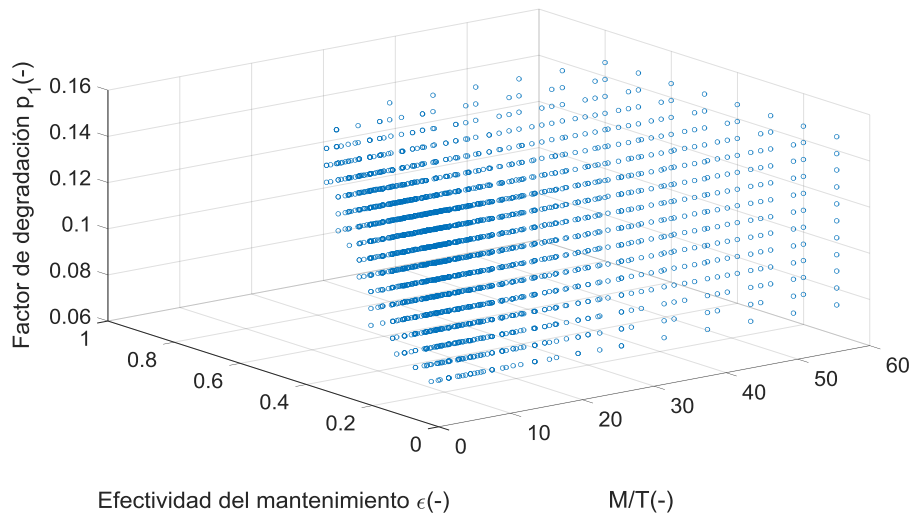


Figura 3.9  $\rho(t)$  del componente para diferentes intervalos de pruebas del modelo PAR

### 3.6. Sensibilidad del *doubling time* para el mantenimiento y el intervalo de pruebas

El siguiente estudio de sensibilidad analiza la relación entre los distintos parámetros relacionados con el mantenimiento y las pruebas en el *doubling time*,  $t_D$ , dada por la Ecuación (3.46).

El *doubling time* para la probabilidad de fallo a la demanda no se alcanza para el caso base bajo un modelo PAS, usando los datos de la Tabla 3.1 (véase Figura 3.3). Sin embargo, si se pueden alcanzar dependiendo de los valores que adopten los parámetros de mantenimiento y pruebas (véase Figura 3.4 y Figura 3.6). La Figura 3.10 muestra las distintas posibles combinaciones de  $M/T$ , factor de degradación por pruebas y efectividad del mantenimiento, para los que se alcanza dicho *doubling time*.



**Figura 3.10** Posibles combinaciones de  $p_1$ ,  $\epsilon$  y  $M/T$  para las que se alcanza el *doubling time* antes de 10 años

Por otro lado, el *doubling time* para la probabilidad de fallo a la demanda se alcanza para el caso base bajo un modelo PAR, usando los datos de la Tabla 3.1 (véase la Figura 3.3). La Figura 3.11 muestra como el *doubling time* varía en función de  $M$  y  $T$ , fijando  $p_1$  y  $\epsilon$  a sus valores iniciales. Se observa claramente una relación inversamente proporcional entre  $t_D$  y  $T$ , lo cual se deduce del análisis de la Ecuación (3.46) para el modelo PAR, donde no existe dependencia entre  $t_D$  y  $M$ .

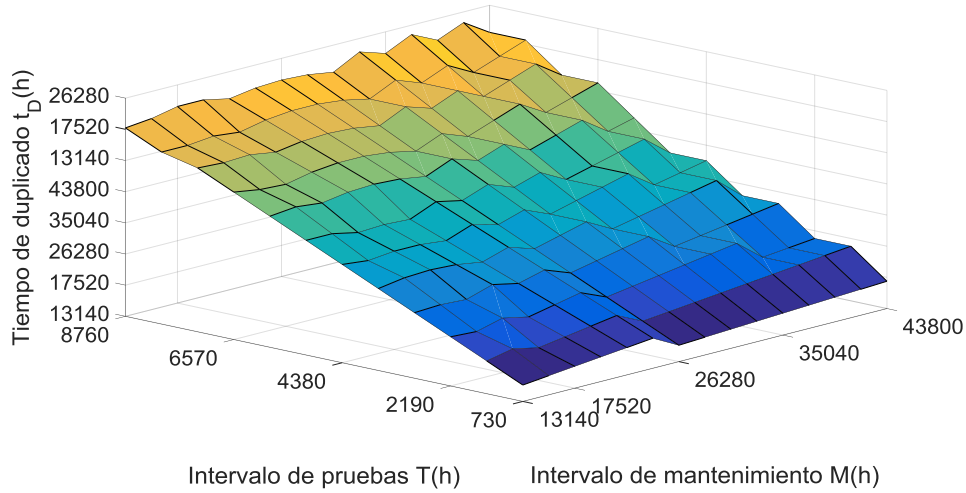
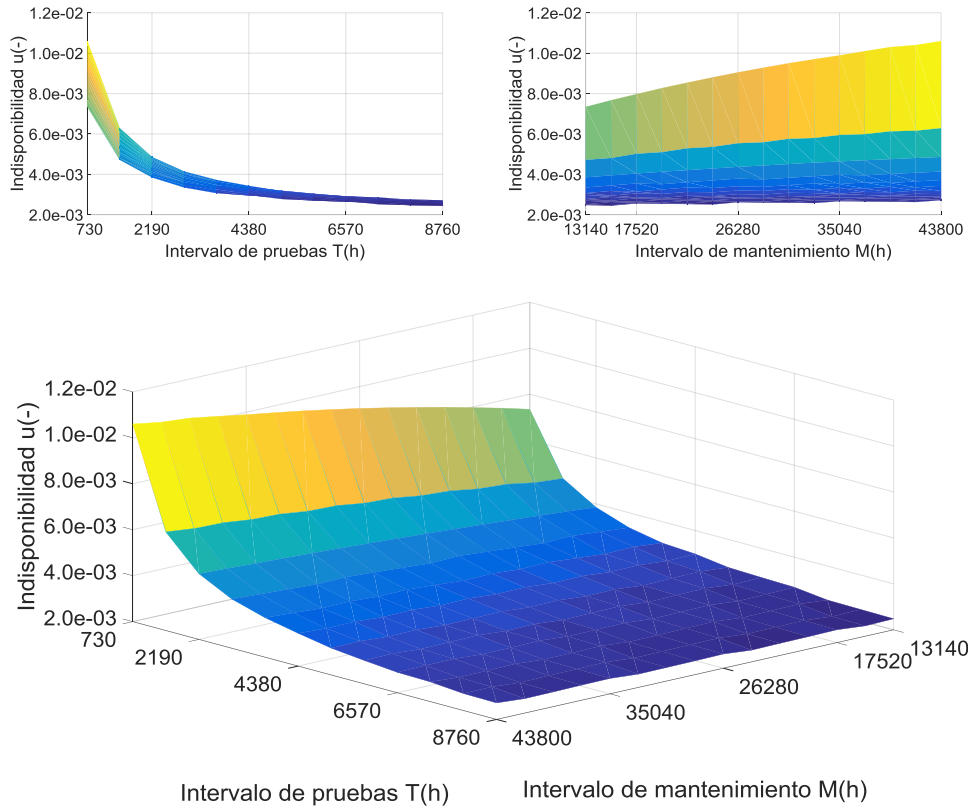


Figura 3.11  $t_D$  para diferentes intervalos de pruebas y mantenimientos del modelo PAR

### 3.7. Indisponibilidad media en función de los intervalos de pruebas y mantenimiento

El último estudio de sensibilidad relaciona la evolución de la indisponibilidad media total del componente, dada por la Ecuación (3.52), en función del par  $\{M, T\}$ , esto es, de los intervalos de mantenimiento y pruebas. Los valores de los parámetros  $p_1$ ,  $\varepsilon$  y  $\eta$  permanecen constantes en los valores que muestra la Tabla 3.1. En particular, la eficiencia de las pruebas,  $\eta$ , no tiene ninguna influencia en  $\rho(t)$ , pero afecta a la indisponibilidad del componente,  $u$ , como función de  $u_c$  (véase la Ecuación (3.50)).

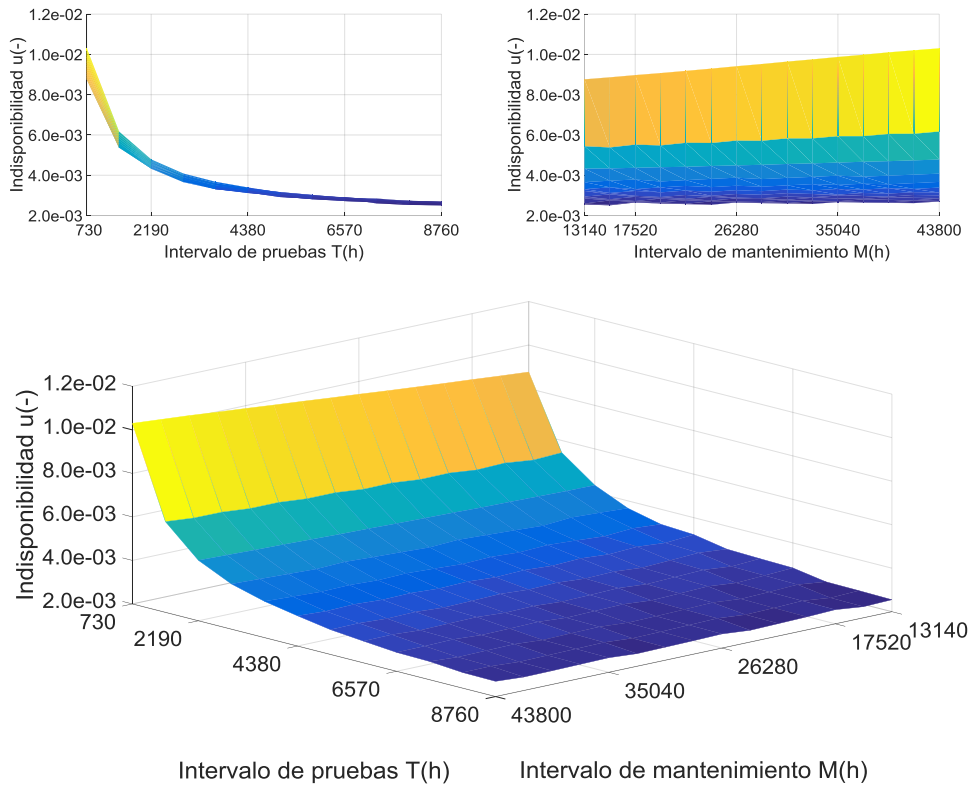
La Figura 3.12 muestra los resultados obtenidos para el modelo PAS. Los valores más altos de  $u$  se alcanzan para el mayor intervalo de mantenimiento y el menor de pruebas entre todos los considerados. La principal contribución a la indisponibilidad total del equipo,  $u$  (véase la Ecuación (3.52)), es la indisponibilidad media debida a la falta de fiabilidad dada por la Ecuación (3.47). Esto explica la relación inversamente proporcional entre  $u$  y  $T$ , para un modelo PAS, así como la relación directamente proporcional entre  $u$  y  $M$ .



**Figura 3.12 Indisponibilidad para diferentes intervalos de mantenimiento y pruebas adoptando un modelo PAS**

La Figura 3.13 muestra los resultados obtenidos adoptando un modelo PAR. Nuevamente, los valores más altos de  $u$  se alcanzan para el mayor y menor intervalo de mantenimiento y pruebas, respectivamente. La principal contribución a la indisponibilidad total del componente es la debida a la falta de fiabilidad dada por la Ecuación (3.47), la cual vuelve a explicar la relación inversamente proporcional entre  $u$  y  $T$ , mientras que existe una dependencia casi directamente proporcional entre  $u$  y  $M$ .





**Figura 3.13 Indisponibilidad para diferentes intervalos de mantenimiento y pruebas adoptando un modelo PAR**

Comparando los resultados de indisponibilidad mostrados en las Figura 3.12 y Figura 3.13, se puede observar que la indisponibilidad total alcanza valores más altos bajo la adopción de un modelo PAR, como consecuencia del comportamiento asintótico del modelo PAS. Por este motivo,  $u$  se incrementa más rápidamente para un modelo PAR que para un modelo PAS con los mismos valores de  $M$  y  $T$ . Dos muestras de ello se obtienen comparando para ambos modelos los valores alcanzados para el menor  $T$  y el mayor  $M$  o el mayor  $T$  y el menor  $M$ .



# Capítulo 4

## Estimación de parámetros de un modelo de fiabilidad dependiente del tiempo

Como se ha mencionado al comienzo del capítulo anterior, se distinguen tradicionalmente dos modos de fallo que contribuyen a la probabilidad de fallo de un componente de seguridad, estos son, el modo de fallo en espera y el modo de fallo en demanda.

Este capítulo aborda la estimación de parámetros del modelo de probabilidad de fallo a la demanda dependiente del tiempo. Mediante el método de Estimación de Máxima Verosimilitud, se estiman los parámetros del modelo relativos a la efectividad del mantenimiento para fallos a la demanda y el estrés debido a las pruebas. Se incluye la discusión y el ajuste del modelo que ofrece un comportamiento más realista, para el caso de aplicación de una motoválvula de una central nuclear.

El modelo de tasa de fallos en espera dependiente de la edad, y la estimación de los parámetros involucrados en el mismo se presentaron en Sebastian Martorell et al. (1999) y Mullor (2006), respectivamente. Para facilitar el seguimiento y desarrollo del capítulo, se incluye también de forma resumida las expresiones de este, y su correspondiente proceso de estimación.

### 4.1. Modelos de fiabilidad bajo mantenimiento imperfecto

Para modelar el modo de fallo en espera y el modo de fallo en demanda, se parte de los modelos desarrollados en Sebastian Martorell et al. (1999) y P. Martorell et al. (2017), para la tasa de fallos en espera y la probabilidad de fallo a la demanda, respectivamente. En los siguientes apartados, ambos modelos se describen de forma breve. Las expresiones que relacionan la estimación de parámetros con la selección del modelo se obtendrán asumiendo las siguientes hipótesis:

1. El mantenimiento preventivo programado en el tiempo depende de su efectividad. La efectividad se representa en el modelo de mantenimiento imperfecto mediante el parámetro  $\varepsilon$ , que oscila en el intervalo  $[0, 1]$ . El modelo de mantenimiento imperfecto adoptado puede ser *Proportional Age Setback* (PAS) o *Proportional Age Reduction* (PAR).
2. El mantenimiento correctivo realiza reparaciones mínimas. Es decir, estas reparaciones no mejoran la edad del equipo. Por lo tanto, para el mantenimiento correctivo se adopta un modelo *Bad As Old* (BAO).
3. Se escoge un modelo de envejecimiento lineal para modelar la tasa de fallos en espera.
4. El estrés causado por las pruebas es el único mecanismo de degradación considerado para modelar la probabilidad de fallo a la demanda.

#### 4.1.1. Modelo de fiabilidad para fallos en espera

En el contexto de los equipos de seguridad de las centrales nucleares, la función más usada frecuentemente en el análisis de la fiabilidad es la función de riesgo o tasa de fallos. La tasa de fallos de un equipo depende de su edad, la cual es función del tiempo cronológico transcurrido desde su instalación y la efectividad de las actividades de mantenimiento realizadas sobre el mismo. Así, un modelo de tasa de fallos dependiente del tiempo, en el periodo  $m$  tras el mantenimiento  $m-1$ , se expresa así (Sebastian Martorell et al., 1999):

$$\lambda_m(t) = \lambda(w_m(t)) + \lambda_0 \quad w_m(t) \geq w_{m-1}^+ \quad (4.1)$$

Donde  $\lambda_0$  es la tasa de fallos en espera o función de riesgo inicial del equipo y  $w_{m-1}^+$  es la edad del componente inmediatamente después de la actividad de mantenimiento  $m-1$ .

Adoptando un modelo lineal para la tasa de fallos, la expresión de la tasa de fallos dependiente de la edad tras el mantenimiento  $m-1$  puede expresarse como:

$$\lambda_m(t) = \alpha w_m(t) + \lambda_0 \quad w_m(t) \geq w_{m-1}^+ \quad (4.2)$$

Donde  $\alpha$  es el factor de envejecimiento lineal, y

$$w_m(t) = w_{m-1}^+ + (t - t_{m-1}) \quad t \geq t_{m-1} \quad (4.3)$$

siendo  $t_{m-1}$  el tiempo cronológico en el cual se realiza el mantenimiento  $m-1$  sobre el equipo.

La función de riesgo acumulada o función de supervivencia en el periodo después del mantenimiento  $m-1$ ,  $H_m(t)$ , se obtiene integrando la función de riesgo dada por la Ecuación (4.1), obteniendo la siguiente expresión:

$$H_m(t) = \frac{\alpha}{2} (w_m(t))^2 + \lambda_0 w_m(t) \quad (4.4)$$

La edad del componente inmediatamente después del mantenimiento  $m-1$ ,  $w_{m-1}^+$ , y, por lo tanto, la función de riesgo y la función de riesgo acumulada, dependen del modelo de mantenimiento imperfecto seleccionado, PAS o PAR. En los siguientes apartados, se presenta la particularización de estas ecuaciones.

#### 4.1.1.1 Modelo PAS

Adoptando un modelo PAS, la edad del equipo inmediatamente después del mantenimiento  $m-1$  viene dada por (Sebastian Martorell et al., 1999):

$$w_{m-1}^+ = t - \sum_{k=0}^{m-2} (1-\varepsilon)^k \varepsilon t_{m-k-1} \quad t \geq t_{m-1} \quad (4.5)$$

Sustituyendo las expresiones correspondientes a  $w_m(t)$  y  $w_{m-1}^+$ , dadas por las Ecuaciones (4.3) y (4.5), en la Ecuación (4.2), la función de riesgo dependiente de la edad se puede escribir de la siguiente forma:

$$\lambda_m(t) = \alpha \left[ t - \sum_{k=0}^{m-2} (1-\varepsilon)^k \varepsilon t_{m-k-1} \right] + \lambda_0 \quad t \geq t_{m-1} \quad (4.6)$$

De manera similar, sustituyendo las Ecuaciones (4.3) y (4.5) en la Ecuación (4.4), la función de riesgo acumulada dependiente de la edad para el periodo  $m$ ,  $H_m(t)$ , puede escribirse de la siguiente forma:

$$H_m(t) = \frac{\alpha}{2} \left[ t - \sum_{k=0}^{m-2} (1-\varepsilon)^k \varepsilon t_{m-k-1} \right]^2 + \lambda_0 \left[ t - \sum_{k=0}^{m-2} (1-\varepsilon)^k \varepsilon t_{m-k-1} \right] \quad (4.7)$$

#### 4.1.1.2 Modelo PAR

Adoptando un modelo PAR, la edad del equipo inmediatamente después del mantenimiento  $m-1$  viene dada por:

$$w_{m-1}^+ = t - \varepsilon t_{m-1} \quad t \geq t_{m-1} \quad (4.8)$$

De forma análoga al razonamiento descrito para el modelo PAS, pero reemplazando en este caso la Ecuación (4.5) por la Ecuación (4.8), es posible deducir las expresiones para la función de riesgo y la función de riesgo acumulada dependiente de la edad para el periodo  $m$ , para un modelo PAR de mantenimiento imperfecto:

$$\lambda_m(t) = \alpha (t - \varepsilon t_{m-1}) + \lambda_0 \quad t \geq t_{m-1} \quad (4.9)$$

$$H_m(t) = \frac{\alpha}{2}(t - \varepsilon t_{m-1})^2 + \lambda_0(t - \varepsilon t_{m-1}) \quad (4.10)$$

#### 4.1.2. Modelo de fiabilidad para fallos en demanda

Las Ecuaciones (3.17) y (3.16) del Capítulo 3 sirven para describir la probabilidad de fallo a la demanda dependiente del tiempo considerando el estrés causado por las demandas en el periodo  $m$ , tras el mantenimiento  $m-1$ ,  $\rho_m(t)$ .

$$\rho_m(t) = \rho_0 + \rho_0 \left( f_{m-1}^+ + p_1 \left[ \frac{t - t_{m-1}}{T} \right] \right) \quad t \geq t_{m-1} \quad (4.11)$$

La probabilidad de fallo a la demanda acumulada en el periodo  $m$ ,  $D_m(t)$ , puede obtenerse sumando la función de distribución acumulada en la actividad de mantenimiento  $m-1$  a las funciones de probabilidad en demanda para cada prueba realizada durante el periodo  $m$ . En general,  $D_m(t)$  no posee una expresión de forma cerrada.

En los siguientes apartados, se presenta la particularización de las expresiones de  $\rho_m(t)$  y  $D_m(t)$ , para los modelos PAS y PAR.

##### 4.1.2.1 Modelo PAS

Si se adopta un modelo PAS, la función de degradación tras el mantenimiento  $m-1$  puede formularse como:

$$f_{m-1}^+ = p_1 \left[ \frac{t_{m-1}}{T} \right] p_1 \sum_{i=1}^{m-2} (1 - \varepsilon)^i \quad (4.12)$$

Sustituyendo la Ecuación (4.12) en la Ecuación (4.11), la función de la probabilidad de fallo a la demanda para el periodo  $m$  puede expresarse como:

$$\rho_m(t) = \rho_0 \left( 1 + \left[ \frac{t_{m-1}}{T} \right] p_1 \sum_{i=1}^{m-2} (1 - \varepsilon)^i + \left[ \frac{t - t_{m-1}}{T} \right] p_1 \right) \quad t \geq t_{m-1} \quad (4.13)$$

La función de distribución de la probabilidad de fallo a la demanda acumulada en el periodo  $m$  tras la actividad de mantenimiento  $m-1$ ,  $D_m(t)$ , se obtiene mediante la suma de la función de distribución inmediatamente después del mantenimiento  $m-1$  y las funciones de probabilidad para cada prueba realizada entre el mantenimiento  $m-1$  y  $t$ , alcanzando así la siguiente expresión:

$$\begin{aligned}
 D_m(t) = & \rho_0 \left( 1 + \left\lfloor \frac{t_{m-1}}{T} \right\rfloor p_1 \left( \sum_{i=1}^{m-1} \left( \left( \left\lfloor \frac{t_{m-1}}{T} \right\rfloor + 1 \right) i + 1 \right) (1-\varepsilon)^{m+1-i} + \frac{(m+1) \left( \left\lfloor \frac{t_{m-1}}{T} \right\rfloor + 1 \right)}{2} \right) \right) \\
 & + \rho_0 \left( 1 + \left\lfloor \frac{t-t_{m-1}}{T} \right\rfloor \left\lfloor \frac{t_{m-1}}{T} \right\rfloor p_1 \sum_{i=1}^{m-1} (1-\varepsilon)^i + \frac{\left\lfloor \frac{t-t_{m-1}}{T} \right\rfloor \left( \left\lfloor \frac{t_{m-1}}{T} \right\rfloor + 1 \right)}{2} p_1 \right)
 \end{aligned} \tag{4.14}$$

#### 4.1.2.2 Modelo PAR

Adoptando un modelo PAR, la función de degradación inmediatamente después del mantenimiento  $m-1$  viene dada por:

$$f_{m-1}^+ = p_1 \left\lfloor \frac{t_{m-1}}{T} \right\rfloor p_1 (1-\varepsilon)(m-1) \tag{4.15}$$

Siguiendo un procedimiento análogo al descrito para el modelo PAS, la probabilidad de fallo a la demanda dependiente del tiempo se obtiene sustituyendo la Ecuación (4.15) en la Ecuación (4.11):

$$\rho_m(t) = \rho_0 \left( 1 + \left\lfloor \frac{t_{m-1}}{T} \right\rfloor p_1 (m-1)(1-\varepsilon) + \left\lfloor \frac{t-t_{m-1}}{T} \right\rfloor p_1 \right) \quad t \geq t_{m-1} \tag{4.16}$$

Por último, la probabilidad de fallo a la demanda acumulada dependiente del tiempo,  $D_m(t)$ , alcanza la siguiente expresión considerando un modelo PAR:

$$\begin{aligned}
 D_m(t) = & \rho_0 \left( 1 + (m-1) \frac{\left\lfloor \frac{t_{m-1}}{T} \right\rfloor \left( \left\lfloor \frac{t_{m-1}}{T} \right\rfloor + 1 \right)}{2} p_1 \right. \\
 & + \left. \left( \left( \left\lfloor \frac{t_{m-1}}{T} \right\rfloor + 1 \right) \frac{m(m-1)}{2} - \left\lfloor \frac{t_{m-1}}{T} \right\rfloor (m-1) \right) \left\lfloor \frac{t_{m-1}}{T} \right\rfloor p_1 (1-\varepsilon) \right) \\
 & + \rho_0 \left( 1 + \left\lfloor \frac{t-t_{m-1}}{T} \right\rfloor \left\lfloor \frac{t_{m-1}}{T} \right\rfloor (m-1) p_1 (1-\varepsilon) + \frac{\left\lfloor \frac{t-t_{m-1}}{T} \right\rfloor \left( \left\lfloor \frac{t-t_{m-1}}{T} \right\rfloor + 1 \right)}{2} p_1 \right)
 \end{aligned} \tag{4.17}$$

## 4.2. Metodología de estimación de parámetros y selección del modelo

En la literatura, es posible encontrar numerosos métodos de estimación de parámetros para modelos de fiabilidad, como el método de máxima verosimilitud, método de los momentos, estimadores bayesianos, etc. En este caso, se opta por el método de Estimación de Máxima Verosimilitud para estimar los parámetros de fiabilidad de los modelos presentados en el Apartado 4.1. Para un modelo dado y una serie de datos observados, la función de verosimilitud  $L$  es el producto de la probabilidad de los datos observados como función de los parámetros del modelo. Esto puede aplicarse a los modelos de fiabilidad y mantenimiento imperfecto para los fallos en espera y los fallos en demanda. Así, las funciones de verosimilitud para fallos en espera y fallos en demanda,  $L_1(\xi)$  y  $L_2(\xi)$ , respectivamente, pueden formularse de la siguiente manera:

$$L_1(\xi | \text{modelo, datos observados}) = \prod_{\text{fallos}} \lambda(t) \prod_{\text{mantenimientos}} \exp[-H(t)] \tag{4.18}$$

$$L_2(\xi | \text{modelo, datos observados}) = \prod_{\text{fallos}} \frac{\rho(t)}{1-D(t)} \prod_{\text{mantenimientos}} (1-D(t)) \tag{4.19}$$

El método de estimación máximo verosímil proporciona estimadores, llamados estimadores de máxima verosimilitud (EMV), de parámetros relacionados de los modelos de fiabilidad y mantenimiento. Las estimaciones máximo verosímiles de estos parámetros son aquellos valores que hacen lo más grande posible la función de verosimilitud, esto es, aquellos que maximizan la probabilidad de los datos observados. Puesto que el logaritmo es una función estrictamente creciente, la función de verosimilitud y su logaritmo



alcanzaran el máximo para los mismos valores de sus parámetros objetivo. Por motivos computacionales, es preferible maximizar el logaritmo de la función de verosimilitud. Maximizando las expresiones correspondientes a  $\log(L(\xi))$ , se obtienen los EMV de los parámetros objetivo. En este caso, el algoritmo empleado para este fin en cada uno de los modelos propuesto es el Nelder Mead Simplex (Lagarias, Reeds, Wright, & Wright, 1998; Nelder & Mead, 1965).

El método de estimación máximo verosímil proporciona, además de la estimación de los parámetros, información de su variabilidad a través de la matriz de información de Fisher. Cada elemento de esta matriz es el opuesto de la segunda derivada parcial de la función de log-verosimilitud evaluada posteriormente en los EMV del modelo de distribución correspondiente, que es, a su vez, el opuesto de su Hessiano. De esta forma, puede obtenerse la matriz de varianzas-covarianza para los parámetros estimados como la inversa de la matriz de información dividida por el tamaño de la muestra.

Concretamente, aprovechando el comportamiento asintótico de la estimación máximo verosímil, si la muestra es suficientemente grande, se puede obtener la desviación estándar de los parámetros de estimación como la raíz cuadrada de la diagonal principal de la matriz de varianzas-covarianza para inferir los intervalos de confianza de cada uno de los parámetros, así como la información que relaciona a los parámetros a través de su covarianza.

#### 4.2.1. Función de verosimilitud para fallos en espera, $L_1(\xi)$

Sea  $r_{p,m}$  el número de fallos en espera del componente  $p$  durante el periodo de mantenimiento  $m$ , los cuales suceden en los instantes  $\tau_{p,m,1}, \tau_{p,m,2}, \tau_{p,m,3}, \dots$ , sea  $t_{p,m}$  el tiempo cronológico de los  $m$ -mantenimientos sobre el componente  $p$ . La función de verosimilitud para  $P$  componentes idénticos de un equipo sometido a un mantenimiento preventivo imperfecto vienen dada por:

$$L_1(\xi) = \prod_{p=1}^P \left\{ \prod_{m=1}^{M_p+1} \left[ \prod_{j=1}^{r_{p,m}} \lambda_{p,m}(\tau_{p,m,j}) \exp \left( - \sum_{m=1}^{M_p} H_{p,m}(t_{p,m}) - H_{M_p+1}(t_p^*) \right) \right] \right\} \quad (4.20)$$

Donde  $\xi$  es el vector de parámetros desconocidos  $(\alpha, \varepsilon)$ . Para cada componente  $p$ ,  $M_p$  es el número de mantenimientos preventivos realizados durante el periodo de observación  $t_p^*$ , siendo  $\lambda_{p,m}(\tau)$  y  $H_{p,m}(t)$  la función de riesgo inducida y la función de riesgo acumulada en el periodo  $m$  respectivamente, y  $H_{M_p+1}(t_p^*)$  es la función de riesgo acumulada en el tiempo de censura  $t_p^*$ .

La función de log-verosimilitud viene dada por:

$$\log L_1(\xi) = \sum_{p=1}^P \left[ \sum_{m=1}^{M_p+1} \sum_{j=1}^{r_{p,m}} \log(\lambda_{p,m}(\tau_{p,m,j})) - \sum_{m=1}^{M_p} H_{p,m}(t_{p,m}) - H_{M_p+1}(t_p^*) \right] \quad (4.21)$$

La Ecuación (4.21) debe ser particularizada en función del modelo de mantenimiento imperfecto considerado. Por un lado, para el modelo PAS, las expresiones correspondientes a  $\lambda_{p,m}(\tau_{p,m,j})$ ,  $H_{p,m}(t_{p,m})$  y  $H_{M_{p+1}}(t_p^*)$  se obtienen a partir de la Ecuación (4.6), evaluada para los tiempos de fallo, y la Ecuación (4.7), evaluada para los tiempos de las actividades de mantenimiento y el tiempo de censura:

$$\lambda_{p,m}(\tau_{p,m,j}) = \alpha \left( \tau_{p,m,j} - \sum_{k=0}^{m-2} (1-\varepsilon)^k \varepsilon t_{p,m-k-1} \right) + \lambda_0 \quad (4.22)$$

$$H_{p,m}(t_{p,m}) = \frac{\alpha}{2} \left( t_{p,m} - \sum_{k=0}^{m-2} (1-\varepsilon)^k \varepsilon t_{p,m-k-1} \right)^2 + \lambda_0 \sum_{m=1}^{M_p} \left( t_{p,m} - \sum_{k=0}^{m-2} (1-\varepsilon)^k \varepsilon t_{p,m-k-1} \right) \quad (4.23)$$

$$H_{M_{p+1}}(t_p^*) = \frac{\alpha}{2} \left( t_p^* - \sum_{k=0}^{M_p-2} (1-\varepsilon)^k \varepsilon t_{p,m-k-1} \right)^2 + \lambda_0 \left( t_p^* - \sum_{k=0}^{M_p-2} (1-\varepsilon)^k \varepsilon t_{p,m-k-1} \right) \quad (4.24)$$

Por otro lado, para el modelo PAR, las expresiones correspondientes a la tasa de fallos  $\lambda_{p,m}(\tau_{p,m,j})$ , y las tasas de fallos acumuladas  $H_{p,m}(t_{p,m})$  y  $H_{M_{p+1}}(t_p^*)$ , se obtienen a partir de las Ecuaciones (4.9) y (4.10), resultando:

$$\lambda_{p,m}(\tau_{p,m,j}) = \alpha (\tau_{p,m,j} - \varepsilon t_{p,m-1}) + \lambda_0 \quad (4.25)$$

$$H_{p,m}(t_{p,m}) = \frac{\alpha}{2} (t_{p,m} - \varepsilon t_{p,m-1})^2 + \lambda_0 (t_{p,m} - \varepsilon t_{p,m-1}) \quad (4.26)$$

$$H_{M_{p+1}}(t_p^*) = \frac{\alpha}{2} (t_p^* - \varepsilon t_{p,M_p})^2 + \lambda_0 (t_p^* - \varepsilon t_{p,M_p}) \quad (4.27)$$

#### 4.2.2. Función de verosimilitud para fallos en demanda, $L_2(\xi)$

De la misma manera que en el apartado anterior, sea  $r_{p,m}$  el número de fallos en demanda del componente  $p$  durante el periodo de mantenimiento  $m$ , los cuales suceden en los instantes  $\tau_{p,m,1}$ ,  $\tau_{p,m,2}$ ,  $\tau_{p,m,3}$ , ..., sea  $t_{p,m}$  el tiempo cronológico de los  $m$ -mantenimientos sobre el componente  $p$ . La función de log-verosimilitud para  $P$  componentes idénticos de un equipo sometido a un mantenimiento preventivo imperfecto viene dada por:

$$\log L_2(\xi) = \sum_{p=1}^P \left[ \sum_{m=1}^{M_p+1} \sum_{j=1}^{r_{p,m}} \log \left( \frac{\rho_{p,m}(\tau_{p,m,j})}{1 - D_{p,m}(\tau_{p,m,j})} \right) + \sum_{m=1}^{M_p} \log \left( 1 - D_{p,m}(t_{p,m}) \right) + \log \left( 1 - D_{M_p+1}(t_p^*) \right) \right] \quad (4.28)$$

La función de probabilidad  $\rho_{p,m}(\tau_{p,m,j})$ , y las funciones de probabilidad acumuladas,  $D_{p,m}(t_{p,m})$  y  $D_{M_p+1}(t_p^*)$ , dependen del modelo de mantenimiento imperfecto escogido. En el caso del modelo PAS, estas funciones se obtienen sustituyendo las Ecuaciones (4.13) y (4.14) en la función de log-verosimilitud tal que:

$$\rho_{p,m+1}(\tau_{p,m+1,j}) = \rho_0 \left( 1 + \left\lfloor \frac{t_{p,m}}{T} \right\rfloor p_1 \sum_{i=1}^m (1-\varepsilon)^i + \left\lfloor \frac{\tau_{p,m+1,j} - t_{p,m}}{T} \right\rfloor p_1 \right) \quad (4.29)$$

$$D_{p,m+1}(t_{p,m+1}) = \rho_0 \left( 1 + \left\lfloor \frac{t_{p,m}}{T} \right\rfloor p_1 \left( \sum_{i=1}^m \left( \left( \left\lfloor \frac{t_{p,m}}{T} \right\rfloor + 1 \right) i + 1 \right) (1-\varepsilon)^{m+1-i} + \frac{(m+1) \left( \left\lfloor \frac{t_{p,m}}{T} \right\rfloor + 1 \right)}{2} \right) \right) \quad (4.30)$$

$$D_{p,m+1}(t_p^*) = D_{p,m}(t_{p,m}) + \rho_0 \left( 1 + \left\lfloor \frac{t_p^* - t_{p,m}}{T} \right\rfloor \left\lfloor \frac{t_{p,m}}{T} \right\rfloor p_1 \sum_{i=1}^m (1-\varepsilon)^i \right. \\ \left. + \frac{\left\lfloor \frac{t_p^* - t_{p,m}}{T} \right\rfloor \left( \left\lfloor \frac{t_p^* - t_{p,m}}{T} \right\rfloor + 1 \right)}{2} p_1 \right) \quad (4.31)$$

En el caso de un modelo PAR, las expresiones correspondientes a la probabilidad de fallo a la demanda y la probabilidad de fallo a la demanda acumulada se obtienen particularizando la Ecuación (4.16) en  $\tau_{p,m,j}$  y la Ecuación (4.17) en  $t_{p,m}$  y  $t_p^*$ .

$$\rho_{p,m+1}(\tau_{p,m+1,j}) = \rho_0 \left( 1 + m \left\lfloor \frac{t_{p,m}}{T} \right\rfloor p_1 (1-\varepsilon) + \left\lfloor \frac{\tau_{p,m+1,j} - t_{p,m}}{T} \right\rfloor p_1 \right) \quad (4.32)$$

$$D_{p,m+1}(t_{p,m+1}) = \rho_0 \left( 1 + m \frac{\left\lfloor \frac{t_{p,m}}{T} \right\rfloor \left( \left\lfloor \frac{t_{p,m}}{T} \right\rfloor + 1 \right)}{2} p_1 \right. \\ \left. + \left( \left( \left\lfloor \frac{t_{p,m}}{T} \right\rfloor + 1 \right) \frac{m(m+1)}{2} - \left\lfloor \frac{t_{p,m}}{T} \right\rfloor m \right) \left\lfloor \frac{t_{p,m}}{T} \right\rfloor p_1 (1-\varepsilon) \right) \quad (4.33)$$

$$D_{p,m+1,j}(\tau_{p,m+1,j}) = D_{p,m}(t_{p,m}) + \rho_0 \left( 1 + \left\lfloor \frac{\tau_{p,m+1,j} - t_{p,m}}{T} \right\rfloor \left\lfloor \frac{t_{p,m}}{T} \right\rfloor mp_1 (1 - \varepsilon) + \frac{\left\lfloor \frac{\tau_{p,m+1,j} - t_{p,m}}{T} \right\rfloor \left( \left\lfloor \frac{\tau_{p,m+1,j} - t_{p,m}}{T} \right\rfloor + 1 \right)}{2} p_1 \right) \quad (4.34)$$

### 4.3. Caso de aplicación

Este apartado comprende la estimación de los parámetros asociados con los modelos de fiabilidad presentados en el Apartado 4.1, para una motoválvula del Sistema de Agua de Alimentación Auxiliar (AAA) de un reactor PWR. Mediante la metodología presentada en el Apartado 4.2, se realiza la estimación de los parámetros y la selección del mejor modelo en función de los datos disponibles. Estas estimaciones se emplean para predecir la respuesta de la motoválvula en función de los intervalos de pruebas de vigilancia y mantenimiento preventivo. Específicamente, se evalúan de forma numérica y gráfica la indisponibilidad debida a la falta de fiabilidad para cada modo de fallo de la MOV y la indisponibilidad total de la MOV en función de los intervalos de pruebas y mantenimiento, teniendo en cuenta los tiempos fuera de servicio debidos a la aplicación de los requisitos de vigilancia y las actividades de mantenimiento, para un horizonte temporal de 10 años.

#### 4.3.1. Histórico de fallos, mantenimientos y pruebas

El histórico de fallos, mantenimientos y pruebas ha sido recopilado para dos motoválvulas idénticas de una central nuclear. Esta colección de datos contiene los fallos y el instante de tiempo en el que sucedieron, así como el número total de mantenimientos preventivos y pruebas de vigilancia registrados para un periodo de 27 años.

La Tabla 4.1 muestra los tiempos de fallo de las dos motoválvulas estudiadas, obtenidos a partir de los datos operacionales de planta. La segunda columna distingue a cuál de las motoválvulas corresponde el fallo. La tercera columna describe brevemente la causa de fallo de la válvula y, por último, la cuarta columna muestra para cada fallo la asignación al modo de fallo, teniendo en cuenta la información disponible de la causa de fallo.

Se han realizado un total de 432 pruebas de vigilancia y 17 mantenimientos preventivos en la MOV1, distribuidos uniformemente con una periodicidad de 22 y 572 días respectivamente a lo largo de un periodo de análisis de 27 años. Por otro lado, se han realizado un total de 424 pruebas de vigilancia y 18 mantenimientos preventivos en la MOV2,

distribuidos uniformemente con una periodicidad de 22 y 528 días respectivamente, a lo largo del mismo periodo.

**Tabla 4.1 Datos de fallos recopilados para dos motoválvulas idénticas de una central nuclear**

Tiempo de fallo [h]	Equipo	Causa de fallo	Modo de fallo
384	MOV2	Contactos del térmico del motor deteriorados	Espera
23472	MOV1	Fallo al abrir. Interruptor final de carrera falla	Demanda
24336	MOV1	Fallo al abrir. Interruptor final de carrera falla	Demanda
27024	MOV2	Fallo al abrir. Interruptor final de carrera falla	Demanda
56424	MOV1	Interruptor guardamotor quemado	Espera
94512	MOV1	Fallo al abrir. Interruptor final de carrera falla	Demanda
94584	MOV1	Fallo al abrir. Desajuste del estrangulador	Demanda

#### 4.3.2. Resultados de la estimación máximo verosímil

En este apartado se presentan los resultados de la estimación de la efectividad del mantenimiento y los parámetros de fiabilidad para los fallos en espera,  $\varepsilon_s$  y  $\alpha$ , y a la demanda,  $\varepsilon_D$  y  $p_I$ , respectivamente, asumiendo los modelos de mantenimiento imperfecto PAS y PAR, mediante los datos presentados en el apartado anterior. Posteriormente se selecciona el modelo que mejor se ajusta a cada modo de fallo.

La estimación máximo verosímil de los parámetros  $\varepsilon_s$ ,  $\alpha$ ,  $\varepsilon_D$  y  $p_I$  se obtiene maximizando las funciones de log-verosimilitud descritas en la Ecuación (4.21) para los fallos en espera y en la Ecuación (4.28) para los fallos a la demanda, mediante el algoritmo simplex de Nelder-Mead. La segunda y tercera columnas de la Tabla 4.2 recogen los EMV de los parámetros correspondientes al modelo de fiabilidad para fallos en espera;  $\varepsilon_s$  y  $\alpha$ , considerando un mantenimiento imperfecto tipo PAS y PAR. Así mismo, incluye el doble de la desviación típica,  $2\sigma$  para cada parámetro, el cual se obtiene a partir de la matriz de información de Fisher. La cuarta columna muestra el valor de las funciones de verosimilitud  $L$ . Análogamente, la Tabla 4.3 muestra la misma información para el caso del modelo de fiabilidad de los fallos en demanda, siendo en este caso los parámetros del modelo estimados  $\varepsilon_D$  y  $p_I$ .

**Tabla 4.2 EMV de los parámetros del modelo de fiabilidad para fallos en espera bajo modelos de mantenimiento imperfecto PAS y PAR**

	$\lambda_0[\text{h}^{-1}]$	$\varepsilon_s[-]$	$\alpha[\text{h}^{-2}]$	$L$
Modelo PAS	5.860E-06	0.716 ± 0.084	3.424E-10 ± 1.0798E-10	5.202E-10
Modelo PAR	5.860E-06	0.995 ± 0.012	5.793E-10 ± 1.757E-10	2.215E-10

**Tabla 4.3 EMV de los parámetros del modelo de fiabilidad para fallos en demanda bajo modelos de mantenimiento imperfecto PAS y PAR**

	$\rho_0[-]$	$\varepsilon_D[-]$	$p_1[-]$	L
Modelo PAS	6.420E-03	0.886 ± 0.084	5.415E-3 ± 1.127E-03	1.136E-18
Modelo PAR	6.420E-03	0.719 ± 0.100	1.141E-3 ± 1.999E-04	1.776E-20

El mejor modelo de fiabilidad para los fallos en espera y los fallos en demanda es, en ambos casos, aquel que asume un mantenimiento imperfecto tipo PAS, siendo el que proporciona un valor más alto para la función de verosimilitud. El resultado se muestra en la cuarta columna de la Tabla 4.2 y la Tabla 4.3. Por lo tanto, se seleccionan estos modelos para ambos modos de fallo, con el valor de los parámetros correspondiente a lo expuesto en ambas tablas.

#### 4.3.3. Indisponibilidad media debida a la falta de fiabilidad durante la vida útil del componente en función de los intervalos de pruebas y mantenimiento

La contribución media debida a la falta de fiabilidad a la indisponibilidad de un componente normalmente en espera durante su vida útil puede ser formulada de la siguiente forma (Martón et al., 2015; P. Martorell et al., 2017):

$$u_R = u_{R,S} + u_{R,D} \quad (4.35)$$

Donde  $u_{R,S}$  es la indisponibilidad debida a la falta de fiabilidad relacionada con los fallos en espera y  $u_{R,D}$  es la indisponibilidad debida a la falta de fiabilidad relacionada con los fallos en demanda.

Por un lado, adoptando el modelo PAS para representar el comportamiento del mantenimiento imperfecto para los fallos en espera, de acuerdo con el Apartado 4.3.2,  $u_{R,S}$  viene dada por la siguiente expresión (Martón et al., 2015):

$$u_{R,S} \approx \frac{1}{2} \left( \lambda_0 + \frac{1}{2} \alpha M \left( \frac{2 - \varepsilon_S}{\varepsilon_S} \right) \right) T \quad (4.36)$$

Por otro lado, adoptando el modelo PAS para representar el comportamiento del mantenimiento imperfecto para los fallos en demanda, de acuerdo con el Apartado 4.3.2,  $u_{R,D}$ , viene dada por la siguiente expresión (P. Martorell et al., 2017):

$$u_{R,D} = \rho_0 + \frac{1}{2} \rho_0 p_1 \frac{M}{T} \left( \frac{2 - \varepsilon_D}{\varepsilon_D} \right) \quad (4.37)$$

La Figura 4.1 muestra la evolución de  $u_{R,S}$  y  $u_{R,D}$  en función del intervalo de pruebas, considerando distintos intervalos de mantenimiento para un horizonte temporal de 10 años. Se observa como  $u_{R,S}$  aumenta de forma significativa para altos valores de  $T$  y  $M$ .

No obstante, el efecto del mantenimiento es positivo para ambas contribuciones. Además, un incremento del intervalo de las pruebas, es decir, valores bajos de  $T$ , tienen un impacto muy negativo en  $u_{R,D}$ .

Además, la Figura 4.1 representa los intervalos de confianza para los valores predichos en la Tabla 4.2 y Tabla 4.3 por las contribuciones debidas a la falta de fiabilidad  $u_{R,S}$  y  $u_{R,D}$ , para diferentes pares de  $T$  y  $M$ .

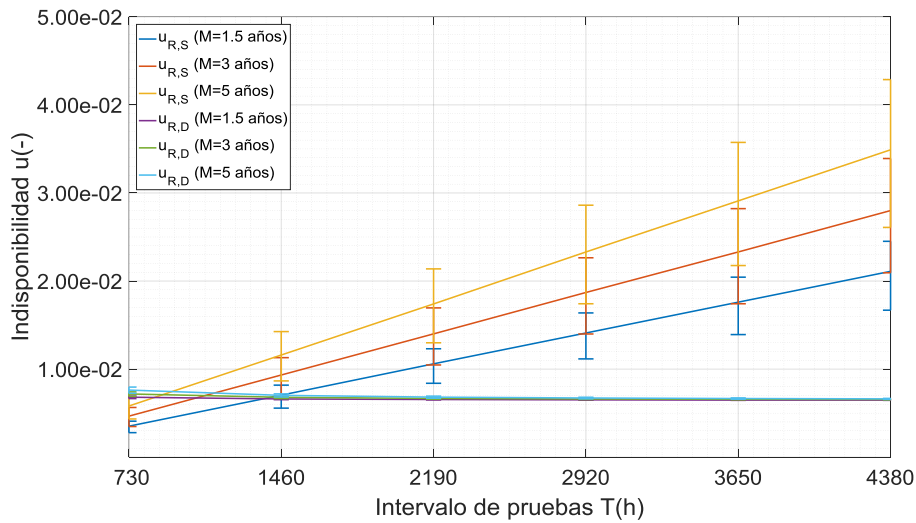


Figura 4.1  $u_{R,S}$  y  $u_{R,D}$  en función del intervalo de pruebas para distintos periodos de mantenimiento

#### 4.3.4. Indisponibilidad media total durante la vida útil del componente en función de los intervalos de pruebas y mantenimiento

Como se ha señalado en el Capítulo 3, la indisponibilidad media de un componente es la suma de la indisponibilidad debida a la falta de fiabilidad y la indisponibilidad debida a los tiempos fuera de servicio derivados de la ejecución de las pruebas y mantenimientos de las centrales nucleares, lo cual puede formularse como:

$$u = u_R + u_T + u_M + u_C + u_O \quad (4.38)$$

Para una mayor claridad, las últimas dos contribuciones,  $u_C$  y  $u_O$ , no se incluyen en el estudio de sensibilidad, pues ambas son despreciables en comparación con el tiempo de espera resultante de los mantenimientos preventivos y las pruebas de vigilancia. Por lo tanto, la indisponibilidad media del componente viene dada por:



$$u = u_{R,S} + u_{R,D} + u_T + u_M \quad (4.39)$$

La Figura 4.2 compara la evolución de  $u_{R,S}$  y la suma de  $u_{R,D}$ ,  $u_T$  y  $u_M$  en función del intervalo de pruebas, considerando diferentes intervalos de mantenimiento preventivo para un horizonte de reemplazamiento del componente de 10 años. El término  $u_{R,S}$  permite evaluar el beneficio de llevar a cabo pruebas y actividades de mantenimiento sobre la indisponibilidad total del componente, mientras que la suma de las contribuciones  $u_{R,D}$ ,  $u_T$ ,  $u_M$  representa su efecto negativo.

La Figura 4.2 muestra también los intervalos de confianza para los valores predichos de indisponibilidad de ambas contribuciones, para diferentes pares de  $T$  y  $M$ .

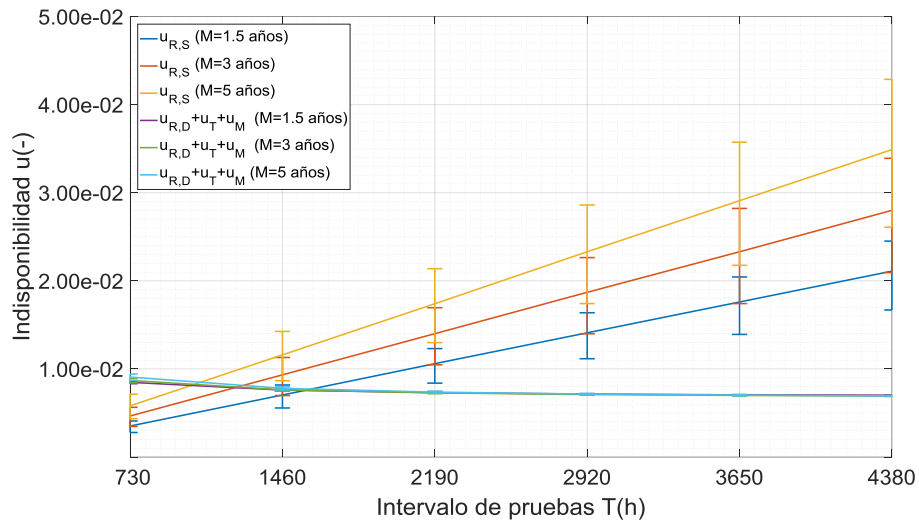


Figura 4.2  $u_{R,S}$  y  $u_{R,D}+u_T+u_M$  en función del intervalo de pruebas para distintos periodos de mantenimiento

Sustituyendo las Ecuaciones (4.36), (4.37), (3.48) y (3.49) en la Ecuación (4.39) se alcanza la siguiente formulación para la indisponibilidad total media del componente a lo largo de la vida útil del mismo:

$$u \approx \frac{1}{2} \left( \lambda_0 + \frac{1}{2} \alpha M \left( \frac{2 - \varepsilon_S}{\varepsilon_S} \right) \right) T + \rho_0 + \frac{1}{2} \rho_0 p_1 \frac{M}{T} \left( \frac{2 - \varepsilon_D}{\varepsilon_D} \right) + \frac{\varphi}{T} + \frac{\delta}{M} \quad (4.40)$$

El último estudio relaciona la indisponibilidad total del componente en función del par  $\{M, T\}$  para un horizonte temporal de reemplazamiento del componente de 10 años. Dicho estudio se representa gráficamente en la Figura 4.3. Los valores más altos de  $u$  se alcanzan para los mayores intervalos de pruebas y mantenimiento considerados  $\{43800h, 4380h\}$ . La contribución más determinante a la indisponibilidad total  $u$  (véase la Ecuación (4.40)), es la contribución debida a la falta de fiabilidad causada por los fallos en espera, como puede observarse en la Figura 4.2. Esto explica la relación de dependencia directamente proporcional entre  $u$  y  $T$  y  $M$ . No obstante, la suma de la contribución debida a la falta de fiabilidad causada por los fallos en demanda y los tiempos en espera causados por los mantenimientos y las pruebas es relevante para valores bajos de  $T$ . Este hecho puede apreciarse también en la Figura 4.2.

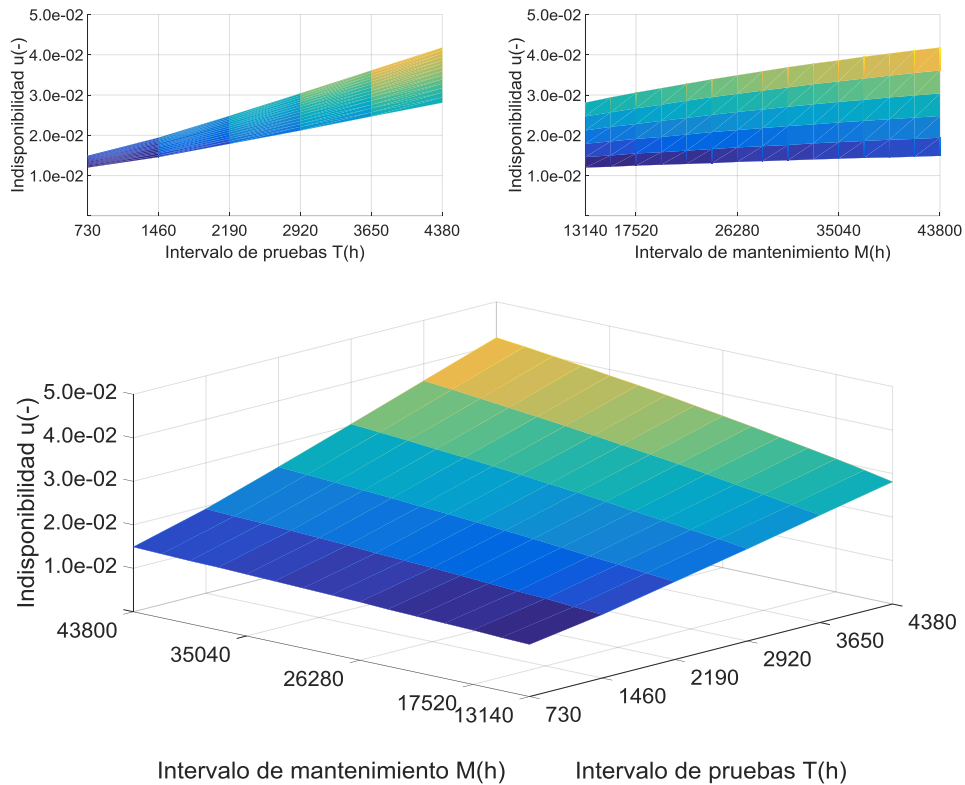


Figura 4.3 Indisponibilidad total para diferentes intervalos de mantenimiento y pruebas

# Capítulo 5

## Aplicación de un modelo RAM dependiente del tiempo para la Toma de Decisiones Informada en el Riesgo

Existe un creciente interés por parte de los organismos reguladores y los titulares de las instalaciones para investigar nuevos modelos y herramientas que realicen un control efectivo del riesgo, garantizando así la seguridad de las centrales nucleares. No obstante, estos modelos y herramientas deben ser consistentes con las ETF y la RM, cuyo objetivo es garantizar los niveles de fiabilidad y disponibilidad de las ESC de seguridad para prevenir, o en última instancia, mitigar las situaciones accidentales.

En 1998, la publicación de la Guía Reguladora RG 1.174 supuso un hito en la integración de la evaluación del riesgo en el proceso de toma de decisiones (USNRC, 1998a). Esta guía reguladora establece los principios del proceso de Toma de Decisiones Informada en el Riesgo (TDIR) de forma detallada (véase Figura 2.3). Específicamente, describe la aplicación del APS para la evaluación del impacto en el riesgo de cambios en la base de licencia de una central nuclear.

Tras la decisión por parte de la NRC de extender las aplicaciones del APS en actividades reguladoras de la industria nuclear (USNRC, 1995b), en la búsqueda de implantar mejoras en el establecimiento de las ETF, surgen las llamadas ETF informadas en el riesgo o *Risk Management Technical Specifications* (RMTS). Esta denominación deriva del objetivo de establecer ETF que refuercen la gestión proactiva del riesgo total que existe en la planta, con la configuración y las acciones que pueden ser necesarias para responder a nuevas condiciones operacionales. Estas mejoras están destinadas a mantener o mejorar la seguridad, al tiempo que reducen la carga innecesaria, asegurando que los requisitos de las ETF sean coherentes con otros requisitos reglamentarios informados en el riesgo solicitados por el regulador, como es el caso de la Regla de Mantenimiento.

En este marco, la NRC promovió un programa con diversas iniciativas que persiguen introducir mejoras en las ETF de los reactores de agua ligera, estableciendo grupos de trabajo en colaboración directa con los titulares de las centrales norteamericanas, conocidos como *Technical Specifications Task Force* (TSTF). En particular, la iniciativa RITS-5b (TSTF-425) (Nuclear Energy Institute, 2007) se ha desarrollado con el objetivo de permitir a los titulares de la instalación modificar las frecuencias de vigilancia mediante un enfoque informado en el riesgo, abriendo así el camino a explorar soluciones que permiten la sinergia entre requisitos de vigilancia flexibles y una RM dinámica. Este hecho cobra especial importancia en el panorama actual, donde numerosas centrales se acercan al fin de su vida de diseño. Las actividades de mantenimiento juegan un papel crucial en la gestión del envejecimiento, luego éstas deben ser replanteadas valorando el impacto en el riesgo del envejecimiento para el horizonte temporal definido por la OLP, ajustando las frecuencias de vigilancia en consonancia con estas.

El trabajo desarrollado en este capítulo sigue la línea trazada por el RITS-5b, teniendo en cuenta los efectos del envejecimiento y la RM. A partir del modelo RAM seleccionado en el capítulo anterior, cuyos parámetros de fiabilidad han sido estimados, se define un modelo de riesgo dependiente de la edad. Ambos modelos permitirán seleccionar la política de pruebas y mantenimiento más adecuada, evaluando el impacto en el riesgo y la indisponibilidad de componentes de seguridad. Se considerará la influencia del envejecimiento, las actividades de mantenimiento y las pruebas de vigilancia. Además, se consideran los criterios impuestos por cambios en las Especificaciones Técnicas de Funcionamiento y en la Regla de Mantenimiento como restricciones a las estrategias contempladas.

## 5.1. Modelo RAM dependiente de la edad

Para la formulación del modelo del caso de aplicación aquí presentado, se asume en primer lugar que los intervalos de pruebas de vigilancia y mantenimiento preventivo,  $T$  y  $M$ , respectivamente, son constantes en el horizonte temporal en el que se aplican. Además, se asume que  $M$  es múltiplo de  $T$ , algo habitual en el programa de mantenimiento de las centrales. Esta condición puede expresarse también de la siguiente manera:

$$\exists a \in \mathbb{N} : M_i = aT_j \quad i = 1, 2, \dots, n ; j = 1, 2, \dots, m \quad (5.1)$$

### 5.1.1. Modelo de indisponibilidad

Como se ha indicado en los capítulos precedentes, la indisponibilidad media de un componente es la suma de la indisponibilidad debida a la falta de fiabilidad,  $u_R$ , y la indisponibilidad debida a los tiempos fuera de servicio derivados de la ejecución de las pruebas y mantenimientos de las centrales nucleares,  $u_{MT}$ , lo cual puede formularse como:

$$u = u_R + u_{MT} \quad (5.2)$$

En los apartados siguientes se presenta la modelización de ambas contribuciones.

### 5.1.1.1 Indisponibilidad debida a la falta de fiabilidad

La indisponibilidad debida a la falta de fiabilidad media de un componente que se encuentra normalmente en espera, puede ser formulada como la suma de tres contribuciones distintas (Martón et al., 2015):

$$u_R = u_R^D + u_R^{UD} + u_R^{UU} \quad (5.3)$$

Donde  $u_R^D$  es la contribución debida a la falta de fiabilidad asociada con los fallos ocultos detectados en las pruebas de vigilancia,  $u_R^{UD}$  es la contribución debida a la falta de fiabilidad asociada con los fallos ocultos que no son detectados en las pruebas de vigilancia pero si en las pruebas funcionales y  $u_R^{UU}$  es la contribución debida a la falta de fiabilidad asociada con los fallos ocultos que no son detectados por ninguna de las dos pruebas. Estas contribuciones se definen a partir de parámetros relativos a la tasa de fallos en espera y a la probabilidad de fallo a la demanda, de la siguiente manera:

$$u_R^D \approx \rho^D + \frac{1}{2} \lambda^D T \quad (5.4)$$

$$u_R^{UD} \approx \frac{1}{2} \lambda^{UD} RI \quad (5.5)$$

$$u_R^{UU} \approx \frac{1}{2} \lambda^{UU} RP \quad (5.6)$$

Donde  $\rho^D$  es la probabilidad de fallo a la demanda asociada con los fallos detectados por las pruebas de vigilancia,  $\lambda^D$  es la fracción de la tasa de fallos detectada por la pruebas de vigilancia,  $T$  es el intervalo de las pruebas de vigilancia,  $\lambda^{UD}$  y  $\lambda^{UU}$ , son las contribuciones de los fallos detectados y no detectados tras la realización de la prueba funcional,  $RI$  es el intervalo de las pruebas funcionales y  $RP$  es la vida útil del componente.

Por un lado, las diferentes contribuciones de la tasa de fallos en espera;  $\lambda^D$ ,  $\lambda^{UD}$  y  $\lambda^{UU}$ , pueden ser obtenidas a partir de la tasa de fallos inducida del equipo,  $\lambda$ , ya que se verifica que (Martón et al., 2015):

$$\lambda = \lambda^D + \lambda^U \quad (5.7)$$

Donde:

$$\lambda^D = \eta_s \lambda \quad (5.8)$$

$$\lambda^U = (1 - \eta_s) \lambda \quad (5.9)$$

Donde  $\eta_S$  es la eficiencia de las pruebas de vigilancia para detectar fallos en espera.

Adicionalmente, asumiendo que la mayor parte de los equipos de seguridad son también objeto de pruebas funcionales, se puede dividir la tasa de fallos no detectada por las pruebas de vigilancia,  $\lambda^U$ , en dos nuevas contribuciones (Martón et al., 2015):

$$\lambda^U = \eta_R \lambda^U + (1 - \eta_R) \lambda^U = \lambda^{UD} + \lambda^{UU} \quad (5.10)$$

Donde  $\eta_R$  es la eficiencia de las pruebas funcionales.

Para el cálculo de la tasa de fallos en espera inducida,  $\lambda$ , a partir de la cual se calculan las contribuciones recién definidas, se debe tener en cuenta que los intervalos de pruebas en las centrales nucleares presentan periodos menores que aquellos en los que se realizan mantenimientos preventivos, tal como se muestra en la Ecuación (5.1). Por tanto, se considera conveniente calcular la tasa de fallos en espera media entre periodos de pruebas consecutivos, de forma que se tenga el indicador más fiable para el cálculo de la indisponibilidad en el horizonte temporal considerado.

La tasa de fallos en espera media entre dos pruebas de vigilancia consecutivas realizadas en los tiempos cronológicos  $t_{n-1}$  y  $t_n$ , se puede expresar en función de la tasa de fallos dependiente del tiempo,  $\lambda_m(t)$ , de la siguiente manera:

$$\lambda_n = \frac{1}{t_n - t_{n-1}} \int_{t_{n-1}}^{t_n} \lambda_m(t) dt \quad (5.11)$$

Assumiendo un modelo lineal para la distribución de tasa de fallos en espera, se substituyen las Ecuaciones (4.2) y (4.3) del Capítulo 4 en la Ecuación (5.11), para alcanzar el siguiente resultado:

$$\lambda_n = \lambda_{m-1}^+ + \frac{\alpha}{2}(t_{n-1} - t_m) + \frac{\alpha}{2}(t_n - t_m) \quad (5.12)$$

Donde  $\lambda_{m-1}^+$  es el valor de la tasa de fallos inmediatamente después de la actividad de mantenimiento  $m-1$ . Llamando  $TR$  al tiempo de referencia para el cual se evalúa la tasa de fallos dependiente de la edad, se adoptará como valor de  $\lambda$  el máximo valor que alcanza la tasa de fallos en espera media entre dos pruebas,  $\lambda_n$ , en todo el  $TR$ , lo cual se puede expresar de esta manera:

$$\lambda = \max \{ \lambda_n \} \quad n=1,2,\dots,N \quad \text{donde } N = TR/T \quad (5.13)$$

Por otro lado,  $\rho^D$  puede ser obtenida a partir de la probabilidad de fallo a la demanda media como (P. Martorell et al., 2017):

$$\rho = \rho^D \quad (5.14)$$

Ya que se asume que la eficiencia de las pruebas de vigilancia respecto a su capacidad para detectar fallos a la demanda,  $\eta_D$ , es 1.

La probabilidad de fallo a la demanda media entre dos pruebas de vigilancia consecutivas realizadas en los tiempos cronológicos  $t_{n-1}$  y  $t_n$ , se puede expresar en función de la probabilidad de fallo a la demanda dependiente del tiempo,  $\rho_m(t)$ , de la siguiente manera:

$$\rho_n = \frac{1}{t_n - t_{n-1}} \int_{t_{n-1}}^{t_n} \rho_m(t) dt \quad (5.15)$$

Como se señaló en el Capítulo 3, la probabilidad de fallo a la demanda en función del tiempo permanece constante entre dos pruebas consecutivas, luego se cumple que:

$$\rho_n = \rho_n(t) \quad (5.16)$$

Al igual que en el caso de la tasa de fallos en espera, se tomará como valor de referencia el máximo valor que alcanza la probabilidad de fallo a la demanda media entre dos pruebas,  $\rho_n$ , para todo  $TR$ , lo cual se puede expresar así:

$$\rho = \max \{ \rho_n \} \quad n = 1, 2, \dots, N \quad \text{donde } N = TR / T \quad (5.17)$$

Finalmente, una vez conocidos los valores de  $\rho^D$ ,  $\lambda^D$ ,  $\lambda^{UD}$  y  $\lambda^{UU}$ , se sustituyen las Ecuaciones (5.4), (5.5) y (5.6) en la Ecuación (5.3) para obtener la expresión de la indisponibilidad debida a la falta de fiabilidad media, en función de los parámetros de tasa de fallos en espera y probabilidad de fallo a la demanda:

$$u_R \approx \rho^D + \frac{1}{2} \lambda^D T + \frac{1}{2} \lambda^{UD} RI + \frac{1}{2} \lambda^{UU} \quad (5.18)$$

#### 5.1.1.2 Indisponibilidad debida a los tiempos fuera de servicio

Como se ha visto en el Capítulo 3, la indisponibilidad debida a los tiempos fuera de servicio de un componente que se encuentra normalmente en espera, puede ser formulada como la suma de hasta cuatro contribuciones (Martón et al., 2015):

$$u_{MT} = u_T + u_M + u_C + u_O \quad (5.19)$$

Cada uno de estos sumandos se evalúa de la siguiente manera (Martón et al., 2015; P. Martorell et al., 2017):

$$u_T = \frac{\varphi}{T} \quad (5.20)$$

$$u_M = \frac{\delta}{M} \quad (5.21)$$

$$u_C = \left( \lambda^D + \frac{1}{T} \rho^D \right) \mu \quad (5.22)$$

$$u_0 = \frac{\theta}{RP} \quad (5.23)$$

Conviene recordar del Apartado 3.4 del Capítulo 3, que  $u_T$  es la indisponibilidad debida a la realización de pruebas de vigilancia,  $u_M$  es la indisponibilidad debida a la realización de mantenimientos preventivos,  $u_C$  es la indisponibilidad debida a la realización de mantenimientos correctivos y  $u_0$  es la indisponibilidad debida a los reemplazamientos. Los parámetros a través de los cuales se definen dichas contribuciones son los siguientes:

- $\varphi$  es el tiempo fuera de servicio medio debido a las pruebas de vigilancia.
- $\delta$  es el tiempo fuera de servicio medio debido al mantenimiento preventivo.
- $\mu$  es el tiempo fuera de servicio medio debido al mantenimiento correctivo.
- $\theta$  es el tiempo fuera de servicio medio debido a los reemplazamientos.

Así, sustituyendo las Ecuaciones (5.20), (5.21), (5.22) y (5.23) en la Ecuación (5.19), se obtiene la expresión de la indisponibilidad media debida a los tiempos fuera de servicio:

$$u_{MT} = \frac{\varphi}{T} + \frac{\delta}{M} + \left( \lambda^D + \frac{1}{T} \rho^D \right) \mu + \frac{\theta}{L} \quad (5.24)$$

## 5.2. Modelo de riesgo dependiente de la edad

La TDIR requiere cuantificar la Frecuencia de Daño al Núcleo (FDN) como métrica de riesgo, a partir del APS Nivel 1 de la central nuclear. Los actuales modelos y datos del APS no contienen el suficiente nivel de detalle para el tipo de aplicación propuesta, así que primero se deberá adaptar el APS para que considere de forma explícita el impacto del envejecimiento, así como el de las pruebas de vigilancia y las actividades de mantenimiento, en el riesgo de la central.

De forma similar al modelo APS Extendido (APSE) presentado en Martón et al. (2015) y desarrollado en detalle en Martón (2014), se integra en el APS el modelo RAM dependiente de la edad para componentes de seguridad formulado en el Apartado 5.1. De esta manera, se podrá obtener la FDN en función de los parámetros relacionados con el envejecimiento de los equipos, la frecuencia de los requisitos de vigilancia, el periodo de las actividades de mantenimiento, y la eficiencia y efectividad correspondiente a los mismos.



Este modelo APSE incluye modelos para representar las contribuciones a la indisponibilidad producto de ambos modos de fallo y de los tiempos fuera de servicio. Las contribuciones de este modelo también permiten evaluar el comportamiento del equipo en términos RAM como función del envejecimiento, de la frecuencia de las pruebas y el mantenimiento, y de la efectividad asociada a los mismos. De esta forma, los modelos y datos del APSE permiten realizar predicciones en la fiabilidad e indisponibilidad de los componentes, y en la FDN de la central nuclear, para un horizonte temporal, pudiendo ser usado en la programación de la frecuencia de los requisitos de vigilancia y las actividades de mantenimiento.

### 5.2.1. Cambio en la contribución a la FDN anual

La RG 1.174 y la RG 1.177 establecen dos métricas de riesgo que son ineludibles para evaluar el impacto en el riesgo de cualquier cambio en la base de licencia de una central nuclear. Esas métricas hacen referencia al riesgo anual y al riesgo simple, que pueden ser evaluadas a través del APS adoptando, por ejemplo, el enfoque propuesto por S. Martorell, Martón, et al. (2014) y S. Martorell, Villamizar, et al. (2014). Estas métricas deben ser formuladas en términos de frecuencia de daño al núcleo y probabilidad de daño al núcleo, respectivamente.

El APS Nivel 1 puede utilizarse para formular la primera métrica de riesgo propuesta en RG 1.174, el cambio en la contribución a la FDN anual, la cual requiere evaluar la FDN antes y después del cambio para cuantificar la FDN dependiente del tiempo como sigue:

$$\Delta R = \Delta FDN(t) = FDN_a(t) - FDN_b(t=0) \quad (5.25)$$

Donde  $FDN_b$  es la FDN antes del cambio y  $FDN_a$  es la FDN dependiente de la edad después del cambio y proyectada a un horizonte temporal determinado  $t$ . La Ecuación (5.25) tiene en cuenta de forma simultánea el impacto en la FDN de los cambios en la frecuencia de los requisitos de vigilancia y las actividades de mantenimiento, así como el envejecimiento de los equipos entre la situación de partida ( $t=0$ ) y el tiempo cronológico  $t$ . Por esta razón, la ecuación permite proyectar el impacto en la FDN para una política de pruebas y mantenimiento determinada dado un horizonte temporal  $t$ .

La Ecuación (5.25) se puede simplificar para el caso de un único componente, asumiendo una dependencia lineal entre la indisponibilidad del componente,  $u$ , y FDN, como sigue:

$$\Delta R \approx \Delta R_i = [u_i^a(t) - u_i^b(t=0)] B_i \quad (5.26)$$

Donde  $u_i^b(t=0)$  es la indisponibilidad inicial del componente  $i$  antes del cambio y  $u_i^a(t)$  es la indisponibilidad del componente dependiente del tiempo después del cambio y proyectada para un horizonte de tiempo  $t$ . La indisponibilidad dependiente del tiempo del equipo  $i$  puede obtenerse a partir de la Ecuación (5.2). Además,  $B_i$  representa la medida

de importancia Birnbaum del equipo  $i$ , la cual se obtiene a partir del análisis de importancias del APS. El valor de  $B$  de un componente es independiente de su propia fiabilidad y solamente depende de la estructura del sistema. Es decir, esta medida evalúa como de importante es la posición que ocupa el componente dentro del sistema, permitiendo relacionar de forma sencilla la sensibilidad del riesgo frente a la variación de la probabilidad de ocurrencia de un suceso determinado.

A partir de la Ecuación (5.26), se deduce que la contribución a la FDN anual de la indisponibilidad de un solo componente puede ser aproximada, para un plan de pruebas de vigilancia y mantenimiento y teniendo en cuenta el envejecimiento durante el periodo  $t$ , como sigue:

$$R_i = FDN_i(t) \approx u_i(t) B_i \quad (5.27)$$

Las Ecuaciones (5.26) y (5.27) muestran la relación entre el modelo de riesgo dependiente de la edad y el modelo RAM dependiente de la edad. Sin embargo, la dependencia lineal asumida no siempre es cierta, y debe suponerse con cautela. En muchas ocasiones, FDN es una función polinómica cubica o cuadrática, por poner dos ejemplos. Esto es debido a que los intervalos de pruebas y mantenimiento no solo afectan a un único componente, sino que en general, son grupos de componentes los que se ven afectados por la variación de dichos intervalos.

### 5.2.2. Incremento Condicional de la Probabilidad de Daño al Núcleo

El APS Nivel 1 puede también emplearse para formular la segunda métrica de riesgo propuesta por la RG 1.177 relativa al riesgo simple, la cual requiere evaluar el Incremento Condicional de la Probabilidad de Daño al Núcleo (ICDPN), mediante la siguiente expresión:

$$r_i = ICPDN_i(t) \approx d_i B_i \quad (5.28)$$

Donde el nuevo parámetro  $d_i$  representa el tiempo que permanece el equipo  $i$  indisponible como consecuencia de la realización de una prueba o una actividad de mantenimiento, esto es, el tiempo fuera de servicio. El tiempo fuera de servicio de los componentes se limita en las ETF, concretamente, las condiciones límites de operación establecen el tiempo de indisponibilidad permitido (CT). Nuevamente aparece el término  $B_i$ , el Birnbaum del equipo  $i$ .  $B_i$  representa, al igual que en el apartado anterior, la medida de importancia Birnbaum del equipo  $i$ .

## 5.3. Toma de decisiones

Este apartado presenta diversos criterios a ser considerados en la toma de decisiones informada en criterios RAM y el riesgo, para cambios en los intervalos de las pruebas de vigilancia y los periodos de mantenimiento preventivo, tal y como son requeridos por la

regulación vigente en las centrales nucleares. Concretamente, los criterios derivan de la aplicación de las guías reguladoras RG 1.174 y RG 1.177 para cambios en las ETF y el 10 CFR 50.65, en su apartado correspondiente a la Regla de Mantenimiento. Estos criterios deben ser formulados en función del modelo RAM y el modelo de riesgo introducidos en los Apartados 5.1 y 5.2.

### 5.3.1. Criterios relativos a cambios en las ETF

Como se ha señalado en la Figura 2.3, la RG 1.174 identifica cinco principios básicos que deben seguir todas aquellas aplicaciones informadas en el riesgo. En el caso particular tratado en este capítulo, son de aplicación los principios número 4 y 5.

El principio 4 de la RG 1.174 establece que cuando los cambios propuestos den lugar a un incremento en el riesgo, los incrementos deben ser pequeños y no excederán los criterios de aceptación. Normalmente, el impacto global de los cambios efectuado es evaluado y comparado con los valores límite proporcionados por la RG 1.174 para las métricas FDN y FGLT. La primera se obtiene mediante el APS Nivel 1 mientras que la segunda requiere del APS Nivel 2.

Para cada cambio individual en los intervalos de pruebas, el cambio en FDN para los distintos APS Nivel 1 de la planta; sucesos internos, externos u otros modos, deben ser menores al criterio de aceptación, que se sitúa en valores de  $1.00E-06$ /año para la FDN. Este criterio puede ser formulado, por tanto, como:

$$\Delta R < 1.00E - 06 / \text{año} \quad (5.29)$$

Además, para cambios en las ETF, la RG 1.177 establece que la contribución al riesgo simple del tiempo fuera de servicio de un componente debería ser menor que el valor límite marcado para el ICPDN:

$$r_i < 5.00E - 07 \quad (5.30)$$

Como se expone en la RG 1.177, la contribución de las pruebas de vigilancia de un componente al riesgo debe evaluarse teniendo en cuenta las contribuciones debidas a la falta de fiabilidad representadas por la componente,  $u_R$ , la frecuencia de vigilancia,  $SF$ , que se define como la inversa de  $T$ , y la duración de las pruebas de vigilancia,  $\phi$ . Por lo tanto, existe un criterio adicional impuesto por la contribución de las pruebas de vigilancia al riesgo, que se define como:

$$R_{RT} \approx u_{RT,i} B_i < R_{RT}^{\text{lim}} \quad (5.31)$$

Donde  $u_{RT}$  es la suma de las contribuciones a la indisponibilidad debidas a la falta de fiabilidad,  $u_R$ , y a las pruebas de vigilancia,  $u_R$ , definidas por las Ecuaciones (5.18) y (5.20).  $R_{RT}^{\text{lim}}$  representa el valor límite de riesgo para la contribución de las pruebas de

vigilancia, el cual no viene fijado por el regulador, obteniéndose a partir de la experiencia operativa en planta.

### 5.3.2. Criterios relativos a cambios en la RM

El principio 5 de la RG 1.174 establece que el impacto del cambio propuesto debe vigilarse utilizando elementos de medida de prestaciones de la planta. Luego, se requiere una estrategia para efectuar la vigilancia que garantice que el cambio no está deteriorando el estado del equipo, por ejemplo, la fiabilidad y la disponibilidad del mismo. Para ciertos casos, existen estrategias de vigilancia requeridas por la Regla de Mantenimiento (RM) adecuadas para aquellos equipos cuya  $SF$  es controlada por los RV de las ETF. Los resultados del programa de vigilancia de la eficacia del mantenimiento deben ser periódicamente reevaluados, realizando los ajustes pertinentes a la frecuencia de las pruebas de vigilancia, además de a las actividades de mantenimiento.

El objetivo de la Regla de Mantenimiento (USNRC, 1991a, 2018) es requerir a los titulares de la instalación la medición de la eficacia de las prácticas de mantenimiento llevadas a cabo, para asegurar el cumplimiento de las funciones de las ESC importantes para la seguridad. Seguidamente, se presentan los requerimientos para vigilar la eficacia del mantenimiento, los cuales son aplicables en cualquiera de las condiciones de operación de la planta.

La Regla de Mantenimiento exige la evaluación de las actividades de mantenimiento preventivo para asegurar que el objetivo de prevenir fallos de las ESC a través del mantenimiento se encuentra en equilibrio con el objetivo de minimizar las indisponibilidad debida a las pruebas de vigilancia y a los mantenimientos preventivos. Como se establece en las directrices de la Regla de Mantenimiento (Nuclear Energy Institute, 2000), los tiempos fuera de servicio incluyen los debidos a mantenimiento correctivo, preventivo, reemplazamiento y vigilancia. Así, en el marco definido por la RM, se debe controlar y vigilar la indisponibilidad debida a las actividades de mantenimiento y la debida a los requisitos de vigilancia. Este criterio se puede expresar como:

$$\min u_{MT} = \min\{u_M + u_T + u_C + u_O\} \quad (5.32)$$

Donde  $u_T$ ,  $u_M$ ,  $u_C$  y  $u_O$  se determinan mediante las Ecuaciones (5.20), (5.21), (5.22) y (5.23), respectivamente.

Además, la RM, en el apartado (a)(1) del 10 CFR 50.65 (USNRC, 1991a), requiere que los valores de indisponibilidad debida a los tiempos fuera de servicio,  $u_{MT}$ , de las ESC importantes para la seguridad, se sitúen por debajo de un valor objetivo que garantice que son capaces de realizar su función en la planta. Este valor límite se determina en función de la importancia para la seguridad del componente y la experiencia operacional del componente. Esta restricción puede ser formulada como:

$$u_{MT} < u_{MT}^{\lim} \quad (5.33)$$

Donde  $u_{MT}^{\text{lim}}$ , representa el valor límite de indisponibilidad debido a los tiempos fuera de servicio, el cual no viene fijado por el regulador, obteniéndose usualmente a partir de la experiencia operativa en planta.

Así mismo, el apartado (a)(4) del 10 CFR 50.65 (USNRC, 1991a) requiere que antes de realizar actividades de mantenimiento, las cuales incluyen, pero no se limitan a requisitos de vigilancia y actividades de mantenimiento preventivo y correctivo, los titulares deben evaluar y gestionar el incremento del riesgo resultante de las actividades de mantenimiento propuestas, manteniéndolo por debajo de un valor objetivo. Este último criterio puede formularse como:

$$R_{MT} \approx u_{MT} B_i < R_{MT}^{\text{lim}} \quad (5.34)$$

$R_{MT}^{\text{lim}}$  tampoco viene fijado por el marco regulador, obteniéndose a partir de la experiencia operativa en planta.

#### **5.4. Estudio de la optimización de la vigilancia y mantenimiento informada en el riesgo de un componente considerando envejecimiento**

El caso de aplicación aquí presentado compara distintos enfoques o estrategias de vigilancia y mantenimiento, empleando los modelos de indisponibilidad y de riesgo dependientes de la edad definidos en los apartados precedentes, para un componente crítico de la central. El objetivo es encontrar aquella estrategia de pruebas y mantenimiento que, cumpliendo con los criterios del Apartado 5.3, garantice los mayores niveles de disponibilidad del componente para un horizonte temporal dado. Con ese fin, se plantean tres problemas de optimización (*Optimization Problem*, OP) considerando dichos criterios.

En los siguientes apartados se muestran, en primer lugar, los parámetros asociados al componente sobre el que se realiza el caso de aplicación, concretamente, una motoválvula del Sistema de Agua de Alimentación Auxiliar (AAA) de un reactor PWR. Posteriormente, se plantean los problemas de optimización. Finalmente, se exponen los resultados obtenidos para cada uno de ellos.

##### **5.4.1. Parámetros RAM de la MOV**

Se dispone de un APS de Nivel 1, en el cual se ha integrado, siguiendo el ejemplo del APSE (Martón, 2014), el modelo RAM dependiente de la edad del Apartado 5.1 para una MOV del AAA, ajustado con el histórico de datos del Capítulo 4. De esta manera, se podrán obtener las medidas de la indisponibilidad y del riesgo, en función de los intervalos de pruebas y mantenimiento para el horizonte temporal considerado, que en este caso es de 10 años (87600h).

A modo de resumen, la Tabla 5.1 muestra los valores medios de los parámetros relativos a la fiabilidad e indisponibilidad de la MOV, así como los intervalos de pruebas y mantenimiento considerados inicialmente en el APS:

**Tabla 5.1 Parámetros RAM y valores iniciales de  $T$  y  $M$  para la MOV**

Descripción	Parámetro	Valor
Tasa de fallos en espera residual	$\lambda_0(h^{-1})$	5.86E-06
Efectividad del mantenimiento para fallos en espera	$\varepsilon_S(-)$	0.716
Factor de envejecimiento lineal	$\alpha(h^{-2})$	3.424E-10
Eficiencia de las pruebas de vigilancia para detectar fallos en espera	$\eta_D(-)$	0.6
Eficiencia de las pruebas funcionales para detectar fallos en espera	$\eta_R(-)$	1
Probabilidad de fallo a la demanda residual	$\rho_0(-)$	6.42E-03
Factor de degradación asociado a los fallos a la demanda	$p_I(-)$	5.415E-3
Efectividad del mantenimiento para fallos a la demanda	$\varepsilon_D(-)$	0.886
Eficiencia de las pruebas de vigilancia para detectar fallos a la demanda	$\eta_D(-)$	1
Tiempo fuera de servicio medio debido a las pruebas de vigilancia	$\varphi(h)$	1
Tiempo fuera de servicio medio debido al mantenimiento preventivo	$\delta(h)$	1
Tiempo fuera de servicio medio debido al mantenimiento correctivo	$\mu(h)$	6
Tiempo fuera de servicio medio debido a los reemplazamientos	$\theta(h)$	24
Vida útil del componente	$RP(h)$	87600
Intervalo de pruebas de vigilancia del APS	$T_{APS}(h)$	2190
Periodo de mantenimiento preventivo del APS	$M_{APS}(h)$	13140

Tal y como se determinó en el Apartado 4.3.2, el modelo de mantenimiento imperfecto que mejor ajusta el comportamiento de la MOV respecto a los datos disponibles, para los dos modos de fallo considerados, es el modelo PAS.

#### 5.4.2. Formulación de los problemas de optimización

Un problema de optimización simple objetivo es aquel que incluye un vector  $x$  de variables de decisión, una función objetivo (*Objective Function*, OF),  $f(x)$ , y un conjunto de restricciones,  $g(x)$ , las cuales pueden aplicar tanto a los criterios de decisión como a las variables de decisión.

En particular, para los problemas que se analizan en este caso de aplicación, las variables de decisión  $x$  son el intervalo de pruebas de vigilancia,  $T$ , y el periodo de mantenimiento,  $M$ . La función objetivo, al igual que las restricciones, se definen en la formulación de cada problema de optimización planteado, teniendo en cuenta los criterios definidos en el Apartado 5.3. Concretamente, al tratarse únicamente de cambios en la frecuencia de vigilancia o intervalos de pruebas y el periodo de mantenimiento, y no disponer de la experiencia operacional de la planta, el único criterio que se tiene en cuenta como restricción en los OP corresponde al definido por la Ecuación (5.29) para la  $\Delta FDN$ . En el conjunto de restricciones que hace referencia a las variables de decisión,  $T$  y  $M$ , se encuentra la impuesta por la Ecuación (5.1).

Los problemas de optimización se han resuelto empleando un algoritmo de búsqueda exhaustiva. Como su nombre indica, la búsqueda exhaustiva consiste en evaluar cada una de las soluciones del espacio de búsqueda hasta encontrar la mejor solución global

(Michalewicz & Fogel, 2004). Mediante esta técnica, si no se conoce el valor correspondiente a la mejor solución global, solo se puede asegurar que se ha encontrado la mejor solución si se examinan todas las posibles. Como el tamaño del espacio de búsqueda no es grande, al tratarse de variables de decisión discretas y acotadas, no se requiere apenas tiempo computacional para evaluar cada una de las soluciones.

A continuación, se presentan los tres casos y la definición de sus correspondientes problemas de optimización.

#### 5.4.2.1 Caso 1: optimización del mantenimiento en base a la RM

El primer caso propone una estrategia de mantenimiento dinámico, fijando la frecuencia de vigilancia. Este caso es coherente con los requisitos que establece la Regla de Mantenimiento, la cual exige que el objetivo de prevenir fallos de las ESC a través del mantenimiento preventivo se encuentra en equilibrio con el de minimizar la indisponibilidad debida a los tiempos fuera de servicio.

El problema de optimización planteado,  $OP_1$ , busca minimizar la indisponibilidad debida a los tiempos fuera de servicio,  $u_{MT}$ , en función del intervalo de mantenimiento preventivo,  $M$ , fijando el intervalo de pruebas. Este corresponde al establecido en el APS para la MOV y que se encuentra en la Tabla 5.1,  $T_{APS}$ , siendo de 2190h (3 meses). Teniendo en cuenta la condición que establece la Ecuación (5.1), los intervalos de mantenimiento considerados variarán desde 4180h (6 meses) hasta 43800h (5 años). Así, el  $OP_1$  puede formularse de la siguiente manera:

$$\left. \begin{array}{l} \text{Min} \quad u_{MT}(M) \\ \text{s.a:} \quad \Delta FDN(M) < 1.0E - 06 / \text{año} \\ \quad \quad 4180h \leq M \leq 43800h \\ \quad \quad M = aT \\ \quad \quad a \in \mathbb{N} \end{array} \right\} \quad (5.35)$$

#### 5.4.2.2 Caso 2: optimización del intervalo de pruebas de vigilancia en base a las ETF

El segundo caso propone una estrategia de mantenimiento dinámico y una frecuencia de vigilancia flexible. Una vez fijado el intervalo de mantenimiento como aquel que minimiza la indisponibilidad debida a los tiempos fuera de servicio, se busca un cambio en las pruebas de vigilancia que minimice la suma de la indisponibilidad debida a la falta de fiabilidad y a las pruebas de vigilancia, de forma coherente con lo establecido en las ETF.

El problema de optimización planteado,  $OP_2$ , parte del intervalo de mantenimiento que soluciona el  $OP_1$ ,  $M_{opt1}$ , o lo que es lo mismo, aquel que minimiza la indisponibilidad debida a los tiempos fuera de servicio,  $u_{MT}$ . A continuación, fijando  $M_{opt1}$ , se varía el



intervalo de pruebas de vigilancia buscando aquel que minimiza la suma de las contribuciones a la indisponibilidad debidas a la falta de fiabilidad y a las pruebas de vigilancia,  $u_{RT}$ . Así, el OP<sub>2</sub> puede formularse de la siguiente manera:

$$\left. \begin{array}{l}
 \text{Min} \quad u_{RT}(T) \\
 \text{s.a:} \quad \Delta FDN(T) < 1.0E - 06 / \text{año} \\
 \quad \quad 182.5h \leq T \leq 6570h \\
 \quad \quad M = aT \\
 \quad \quad a \in \mathbb{N}
 \end{array} \right\} \quad (5.36)$$

#### 5.4.2.3 Caso 3: optimización de los intervalos de mantenimiento y pruebas en base al RITS-5b

El tercer caso propone una estrategia de mantenimiento y una frecuencia de vigilancia dinámica. Dicha estrategia se basa en la hibridación de los enfoques anteriores, desarrollada en el RITS-5b. Este enfoque pretende introducir mejoras desde el punto de vista de la mejora de la eficacia en términos de la indisponibilidad total del componente.

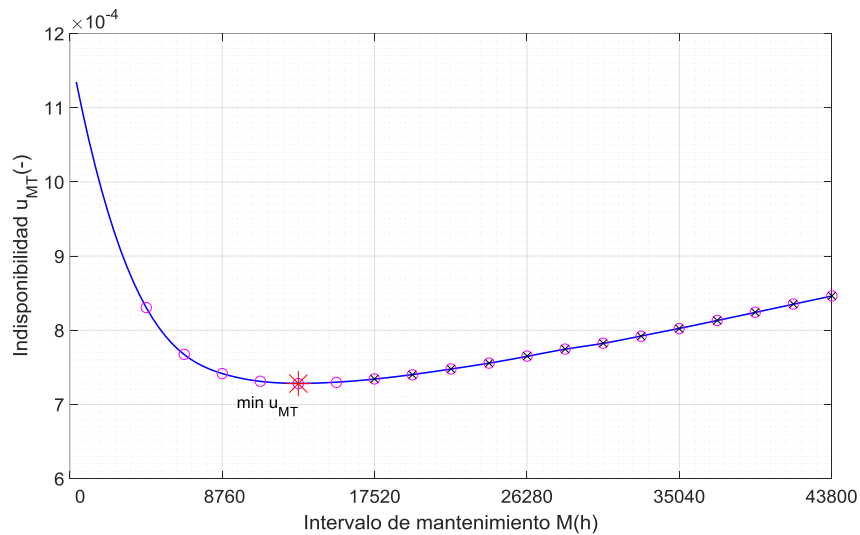
El problema de optimización planteado, OP<sub>3</sub>, busca minimizar la indisponibilidad total,  $u$ , suma de la indisponibilidad debida a la falta de fiabilidad,  $u_R$ , y los tiempos fuera de servicio provocados por las pruebas de vigilancia y las actividades de mantenimiento,  $u_{MT}$ . Con dicho fin, se varía el intervalo de pruebas de vigilancia,  $T$ , y el intervalo de mantenimiento preventivo,  $M$ . Teniendo en cuenta la condición que establece la Ecuación (5.1), los intervalos de pruebas considerados variaran desde 182.5h (1 semana) hasta 8760h (1 año) y los intervalos de mantenimiento considerados lo harán entre 365h (2 semanas) y 43800h (5 años). Así, el OP<sub>3</sub> puede formularse de la siguiente manera:

$$\left. \begin{array}{l}
 \text{Min} \quad u(M, T) \\
 \text{s.a:} \quad \Delta FDN(M, T) < 1.0E - 06 / \text{año} \\
 \quad \quad 182.5h \leq T \leq 6570h \\
 \quad \quad 365h \leq M \leq 43800 \\
 \quad \quad M = aT \\
 \quad \quad a \in \mathbb{N}
 \end{array} \right\} \quad (5.37)$$

### 5.4.3. Resultados

#### 5.4.3.1 Caso 1

La Figura 5.1 representa los valores de  $u_{MT}$ , en función de  $M$ . Los círculos magenta representan los valores que cumplen la restricción a la variable de decisión, establecida en la Ecuación (5.1). A partir de estos, se dibuja una línea azul que representa la evolución de  $u_{MT}$  en función de  $M$ , para un  $T$  fijado,  $T_{APS}$ . Esta función se estima interpolando mediante *splines*. Aquellos círculos en los que se sobreimprime una cruz negra corresponden a aquellas combinaciones de  $T$  y  $M$  que no cumplen la restricción impuesta por  $\Delta FDN < 1.0E-06/año$ .

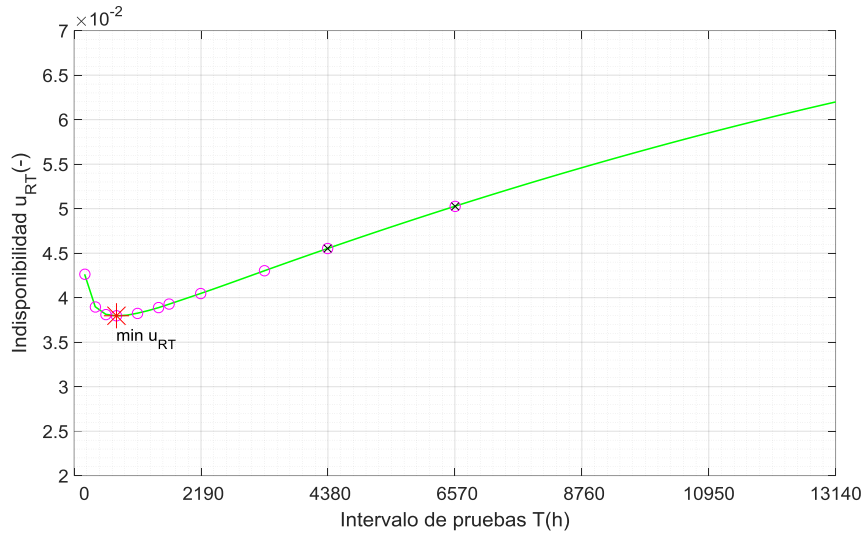


**Figura 5.1** Indisponibilidad debida a los tiempos fuera de servicio en función de  $M$ , para  $T_{APS}$

La función objetivo de  $OP_1$ ,  $FO_1$ , es minimizar el valor de  $u_{MT}$ . El valor de  $M$  para el que se obtiene el valor mínimo de  $u_{MT}$ , que se señala en la Figura 5.1 a través de un asterisco rojo ( $u_{MT}=7.28E-04$ ),  $M_{opt1}$ , es de 13140h (18 meses).

#### 5.4.3.2 Caso 2

La Figura 5.2 representa los valores de  $u_{RT}$ , en función de  $T$ . Nuevamente, los círculos magenta representan los valores que cumplen la restricción a la variable de decisión establecida en la Ecuación (5.1). A partir de estas, se dibuja una línea verde que representa la evolución de  $u_{RT}$  en función de  $T$ , para un  $M$  fijado,  $M_{opt1}$ . Aquellos círculos en los que se sobreimprime una cruz negra corresponden a aquellas combinaciones de  $T$  y  $M$  que no cumplen la restricción impuesta por  $\Delta FDN < 1.0E-06/año$ .

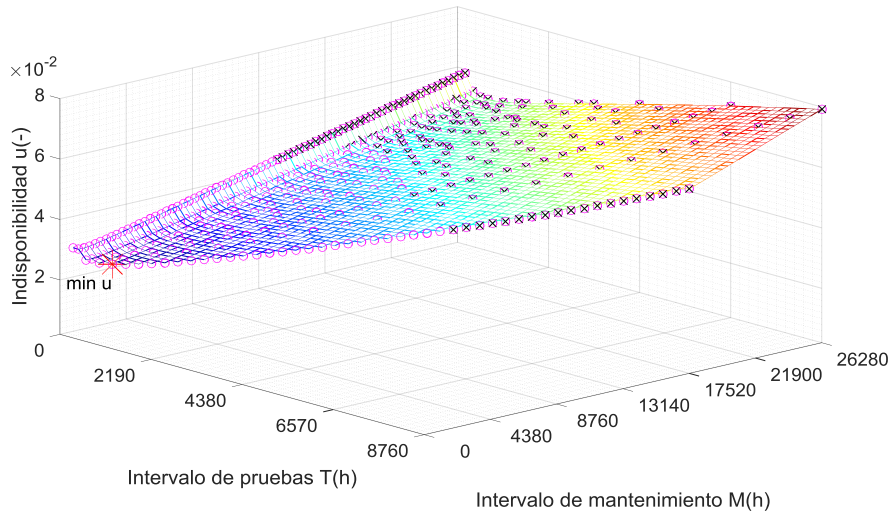


**Figura 5.2 Indisponibilidad debida a la falta de fiabilidad y al tiempo fuera de servicio debido a las pruebas en función de  $T$ , para  $M_{opt1}$**

La función objetivo de  $OP_2$ ,  $FO_2$ , es minimizar el valor de  $u_{RT}$ . El valor de  $T$  para el que se obtiene el valor mínimo de  $u_{RT}$ , que se señala en la Figura 5.2 a través de un asterisco rojo ( $u_{RT}=3.80E-02$ ),  $T_{opt2}$ , es de 730h (1 mes).

#### 5.4.3.3 Caso 3

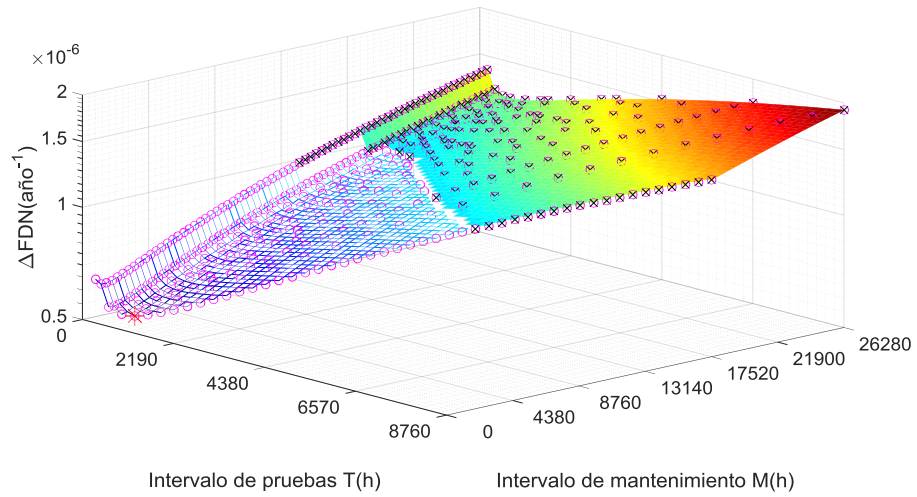
La Figura 5.3 representa los valores de  $u$ , en función de los valores de  $T$  y  $M$  que cumplen las condiciones mencionadas. También en esta ocasión, los círculos magenta representan los valores que cumplen la restricción a las variables de decisión establecida en la Ecuación (5.1). A partir de estos, se dibuja una rejilla que representa  $u$  en función de  $T$  y  $M$ . Esta función se estima interpolando mediante *splines*. Aquellos círculos en los que se superimprime una cruz negra corresponden a aquellas combinaciones de  $T$  y  $M$  que no cumplen la restricción del criterio  $\Delta FDN < 1.0E-06/\text{año}$ .



**Figura 5.3 Indisponibilidad total en función de  $T$  y  $M$**

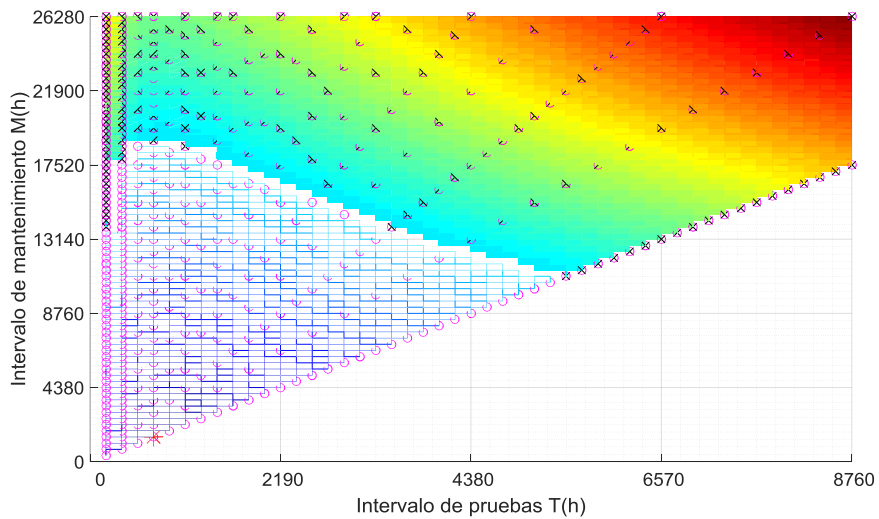
La función objetivo de  $OP_3$ ,  $OF_3$ , es minimizar el valor de  $u$ . Los valores de  $T$  y  $M$  para los que se obtiene el valor mínimo de  $u$ , que se señala en la Figura 5.3 a través de un asterisco rojo ( $u_{RT}=2.62E-2$ ),  $T_{opt}$  y  $M_{opt}$ , respectivamente, son de 730h (1 mes) y 1460h (2 meses), respectivamente.

En la Figura 5.4, se observa como varía la  $\Delta FDN$  en función de  $T$  y  $M$ . En ella, se pueden visualizar dos partes diferenciadas. Por un lado, la rejilla, donde se sitúan los círculos con las posibles combinaciones de  $T$  y  $M$  que cumplen todas las restricciones del  $OP_3$ . Por otro lado, la superficie, contiene todas aquellas posibles combinaciones de  $T$  y  $M$  que no cumplen la restricción impuesta por  $\Delta FDN < 1.0E-06/año$ .



**Figura 5.4 Variación de la  $\Delta FDN$  en función de  $T$  y  $M$**

Realizando la proyección paralela al plano  $MT$ , mostrada en la Figura 5.5, se observan claramente cuales son todas las posibles combinaciones de  $T$  y  $M$  que cumplen el conjunto de restricciones definido en el  $OP_3$ .



**Figura 5.5 Proyección en el plano  $TM$  de la variación de la  $\Delta FDN$**

#### 5.4.4. Resumen de los resultados

En la Tabla 5.2 se muestra un resumen de los datos significativos en términos de indisponibilidad y riesgo para cada OP planteado. Pese a no haber sido incluidos como restricciones en los distintos OP, se añaden los valores de  $R_{MT}$  y  $R_{RT}$ , calculados a partir de los valores contenidos en sus columnas adjuntas,  $u_{MT}$  y  $u_{RT}$ , por el Birnbaum del componente, cuantificado en el APS. Las dos últimas columnas hacen referencia a la indisponibilidad total  $u$  y la  $\Delta FDN$  para cada caso.

Tabla 5.2 Resumen de los resultados de los distintos MOP

Caso	$T(h)$	$M(h)$	$u_{MT}$	$R_{MT}(\text{año}^{-1})$	$u_{RT}$	$R_{RT}(\text{año}^{-1})$	$u$	$\Delta FDN(\text{año}^{-1})$
<i>Inicial</i>	2190	13140	7.28E-04	5.14E-06	4.05E-02	2.85E-04	4.08E-02	9.03E-07
1	2190	13140	<b>7.28E-04</b>	5.14E-06	4.05E-02	2.85E-04	4.08E-02	9.03E-07
2	730	13140	1.74E-03	1.23E-05	<b>3.80E-02</b>	2.68E-04	3.83E-02	8.39E-07
3	730	1460	2.27E-03	1.60E-05	2.53E-02	1.79E-04	<b>2.62E-02</b>	5.21E-07

En el primer caso, la combinación de  $T$  y  $M$  resultante de minimizar la indisponibilidad debida a los tiempos fuera de servicio,  $u_{MT}$ , coincide con los intervalos en los que se efectúan actualmente los requisitos de vigilancia y las actividades de mantenimiento en la central nuclear de cuyo APS se ha dispuesto.

En el segundo caso, se reduce el intervalo de pruebas para lograr el cometido de minimizar la suma de las contribuciones a la indisponibilidad debida a la falta de fiabilidad y a las pruebas de vigilancia,  $u_{RT}$ .

Por último, en el tercer caso se muestra la combinación de  $T$  y  $M$  que minimiza el valor de la indisponibilidad total, reduciéndose ambos valores de forma significativa, lo que aumentaría considerablemente la frecuencia de ambas actividades respecto a la situación actual. La opción de un periodo de mantenimiento preventivo y una frecuencia de vigilancia flexible, representada por el caso 3, obtiene los mejores resultados también desde el punto de vista de la  $\Delta FDN$ , considerándose por ello la mejor estrategia a adoptar para un horizonte temporal de 10 años.

# Capítulo 6

## Evaluación del impacto en la fiabilidad humana y el riesgo para cambios en las ETF

El presente capítulo desarrolla una metodología de evaluación del impacto en el riesgo para cambios en el tiempo de indisponibilidad permitido (CT) de un componente de seguridad, incluido en las ETF, usando un modelo de APS refinado mediante códigos termohidráulicos *best-estimate* (BE) y técnicas de AFH. Dicha metodología se basa en la metodología descrita por S. Martorell, Martón, et al. (2014) y S. Martorell, Villamizar, et al. (2014), para cambios en los RV y el CT considerando el efecto de las incertidumbres. La utilización de códigos BE permite descubrir nuevas secuencias accidentales no contempladas en el APS original y una cuantificación más realista de las PEH para las acciones involucradas en las mismas. El caso de aplicación presentado evalúa los cambios en la cuantificación de las PEH y el riesgo del cambio en el CT. Este capítulo amplía la investigación presentada en el artículo de P. Martorell et al. (2018).

### 6.1. Importancia del factor humano en la Toma de Decisiones Informada en el Riesgo

Como se observó en el Apartado 2.2.2 del Capítulo 2, está ampliamente reconocido que el factor humano es una parte importante del diseño y la evaluación del riesgo de sistemas complejos. Como parte del APS, el AFH supone un marco sistemático para identificar, modelar y cuantificar los sucesos de origen humano que tienen lugar en la operación de una central nuclear. Diversos estudios se han centrado en los beneficios de usar de forma conjunta el ADS y el APS para mejorar la estimación de las ventanas temporales disponibles para el operador en una situación accidental. Una ventana temporal (VT) es el intervalo del tiempo en el cual los operadores deben efectuar una acción para conducir a la planta a una situación segura. Calcular la PEH puede ser llevado a cabo por las

técnicas de AFH (Karanki, Rahman, Dang, & Zerkak, 2017; Prasad & Gaikwad, 2015; Prošek & Čepin, 2008; Voronov & Alzbutas, 2011), mientras que las simulaciones termohidráulicas (TH) empleando códigos *best-estimate* pueden analizar la idoneidad de los escenarios accidentales preestablecidos en los modelos del APS, identificando y caracterizando secuencias accidentales y criterios de éxito desconocidos previamente (Lee, Lim, Yoon, & Jeong, 2014). Tomando como punto de partida el marco definido por la IAEA (IAEA, 2011), los resultados combinados de ambos enfoques proporcionan elementos de entrada para la TDIR que garantizan la seguridad de los reactores (Borysiewicz, Kowal, & Potemski, 2015; Di Maio, Rai, & Zio, 2016; Hess, 2009; Ibáñez et al., 2016).

Los cambios en las ESC se pueden cumplir directamente mediante el uso de la RG 1.174. Aunque trabajos previos se han centrado en la evaluación del impacto en el riesgo de cambios en las ETF de ESC (S. Martorell, Martón, et al., 2014; S. Martorell, Villamizar, et al., 2014), los cambios en las acciones humanas también han de ser evaluados. El NUREG-1764 (USNRC, 1994) proporciona la orientación para evaluar cambios en las acciones del operador relevantes para la seguridad, con especial atención a aquellas contenidas en la base de licencia de la planta, de forma consistente con la Guía Reguladora RG 1.174.

## 6.2. Metodología

La Figura 6.1 muestra los tres pasos esenciales de la metodología para la evaluación del impacto en el riesgo de cambios en el CT, dentro de las ETF de las centrales nucleares, usando un modelo APS refinado a través de códigos termohidráulicos BE y del AFH. El enfoque propuesto es consistente con los principios y el marco de la TDIR para cambios en la base de licencia de una central nuclear.

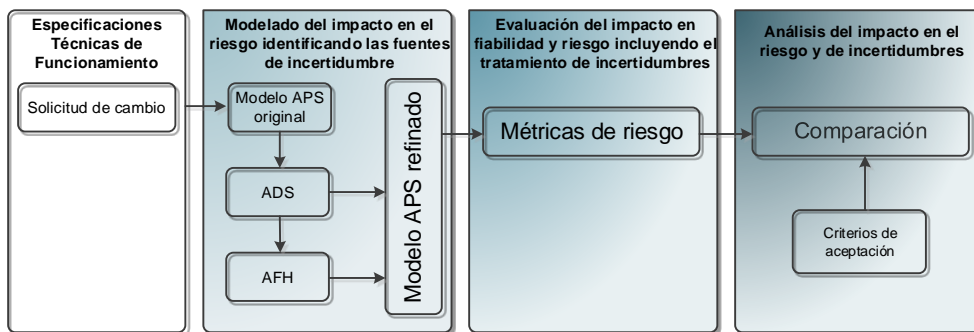


Figura 6.1 Esquema de la TDIR para cambios en las ETF



La metodología incluye la identificación, tratamiento y análisis de las incertidumbres, como dictan la RG 1.174 y la RG 1.177. Diversos trabajos en los últimos años han mostrado la necesidad de considerar las incertidumbres en el APS en la TDIR. El NUREG-1855 (Drouin et al., 2009) y el EPRI-1026511 (EPRI, 2012) contienen orientaciones para llevar a cabo este proceso

### **6.2.1. Modelado del impacto en el riesgo**

En primer lugar, atendiendo al modelado del riesgo esquematizado en la Figura 6.1, el modelo y los datos del APS son refinados a través de los resultados de las simulaciones TH, así como de una cuantificación de las PEH más realista. En este paso se identifica, no solo las fuentes de incertidumbre ligadas con el modelo y los datos del APS, sino también las fuentes de incertidumbre de modelo y parámetro asociadas con los supuestos del CT (USNRC, 2011).

#### **6.2.1.1 Modelado del Análisis Determinista de Seguridad**

Los primeros análisis de seguridad de las centrales nucleares se caracterizaban por su conservadurismo, producto de las limitaciones en el conocimiento (IAEA, 2010a). El ADS se basaba en el uso de códigos informáticos que tomaban condiciones iniciales y de frontera conservadoras, los cuales no proporcionaban evaluaciones precisas de los márgenes de seguridad. Los avances en el desarrollo de los códigos, junto a la mayor disponibilidad de datos experimentales, devinieron en un enfoque más realista de los análisis, el cual incluía la evaluación de las incertidumbres (Wilson, 2013).

Los llamados códigos *best-estimate*, son capaces de proporcionar información más realista del comportamiento físico de la planta, identificando así los problemas más relevantes en cuestión de seguridad. Entre ellos, los errores humanos derivados de un diagnóstico erróneo o una ejecución inadecuada de una acción durante una situación accidental, representan una importante contribución al riesgo. Este hecho es especialmente notable cuando la planta se encuentra en otros modos distintos al de plena potencia (Vaurio, 2009). Por ello es importante que las PEH incluidas en el APS puedan ser estimadas de forma apropiada.

La actuación humana es fuertemente dependiente del tiempo que dispone el operador para realizar las acciones, tiempo que se calcula mediante el análisis de escenarios accidentales. Los códigos termohidráulicos BE utilizan modelos de planta específicos para determinar la cantidad de tiempo disponible que tiene el operador para actuar, sin que se superen los parámetros de seguridad establecidos. Este tiempo recibe el nombre de ventana temporal (Prošek & Čepin, 2008). Para obtener las ventanas temporales, se ejecutan una serie de simulaciones termohidráulicas del escenario accidental. Estas ventanas temporales sirven posteriormente para estimar las PEH a través de las técnicas de AFH pertinentes.

### 6.2.1.2 Análisis de Fiabilidad Humana: modelado de la probabilidad de error humano

El AFH se lleva a cabo como parte del APS de una central nuclear, para determinar cómo afecta la actuación humana a la seguridad de la planta de una forma estructurada, que permita identificar acciones humanas erróneas y estimar sistemáticamente la probabilidad de error de las mismas, usando datos, modelos o juicio de expertos (ASME, 2000). Estas probabilidades reciben el nombre de Probabilidades de Error Humano.

La *Nuclear Energy Agency* (NEA) clasifica tres tipos de errores en función del momento de la acción respecto al inicio de un transitorio (Nuclear Energy Agency, 1998):

- Tipo A: acciones humanas pre-iniciador. En este grupo se engloban acciones como mantenimiento, reparación, calibración y prueba de equipos.
- Tipo B: acciones humanas que pueden causar un iniciador. Estos errores conllevan a dejar indisponibles componentes. Se modelan explícitamente en el APS.
- Tipo C: Acciones humanas post-iniciador. Suceden cuando se intenta activar una función de seguridad, usar un sistema alternativo o ejecutar acciones de recuperación. Representan la mayor contribución a la Frecuencia de Daño al Núcleo.

Las acciones erróneas humanas post-iniciador son errores cometidos durante la actuación como respuesta a un accidente o suceso iniciador (*Initiating Event*, IE). Cada acción errónea humana post iniciador puede dividirse en dos fases: la fase de diagnóstico y la fase de ejecución. La primera comprende aquellas situaciones que demandan la intervención del operador, incluyendo el tiempo para pensar y tomar una decisión, mientras que la segunda corresponde a la ejecución de la acción misma. De esta forma, la PEH total de una acción humana errónea post-iniciador puede expresarse como:

$$PEH = P_d + (1 - P_d)P_e \quad (6.1)$$

Donde  $P_d$  es la probabilidad de error del diagnóstico o cognitiva y  $P_e$  es la probabilidad de error en la ejecución. Estas probabilidades de error se calculan de forma independiente, ya que están afectadas por una serie distinta de factores, esto es, tiempo, estrés, etc. Estos factores reciben el nombre de factores de influencia (PSF). No obstante, la parte más importante en el proceso de cálculo de  $P_d$  y  $P_e$  está relacionada con el análisis del tiempo dedicado a cada fase, lo cual está intrínsecamente relacionado con los resultados del análisis termohidráulico *best-estimate*. Primero, es necesario identificar las VT para ejecutar la acción, tras las cuales es demasiado tarde realizar cualquier acción. Estas VT incluyen el intervalo de tiempo para diagnosticar y tomar una decisión, así como el tiempo necesario para llevarla cabo. La PEH puede entonces ser calculada partiendo de una técnica de AFH apropiada.

Existen una gran variedad de técnicas de AFH, las cuales poseen diversas ventajas e inconvenientes, difiriendo en los distintos aspectos que rodean una acción humana y el

nivel de detalle que ofrecen respecto a ellos (Alvarenga, Frutuoso e Melo, & Fonseca, 2014; Bell & Holroyd, 2009). Partiendo de los informes de la NRC relativos a las buenas prácticas en el campo del AFH (Kolaczkowski et al., 2005, 2006), dos técnicas fueron seleccionadas para calcular la PEH post-iniciador de las acciones erróneas humanas: el método *Time Reliability Correlation* (TRC) (Hall et al., 1982) para la fase de diagnóstico y el método *Technique for Human Error Rate Prediction* (THERP) (Swain & Guttmann, 1983) para la fase de ejecución. La selección de estas técnicas se basa en el APS de Nivel 1 original tomado como referencia, el cual cuantifica el valor de las PEH mediante este procedimiento. Ambos métodos se describen brevemente a continuación:

- El método TRC emplea una distribución log-normal para calcular la probabilidad de que un operador responda satisfactoriamente a una situación en un tiempo dado. Este sistema de cuantificación depende principalmente de tres factores: el tiempo disponible, si es una acción tomada en base a reglas (acciones procedimentales) o en base al conocimiento (no procedimental), y si la posibilidad de dudar existe (Dougherty & Fragola, 1988).
- El método THERP calcula la probabilidad de la ejecución exitosa de todas las actividades necesarias para completar una tarea, proporcionando una descripción exhaustiva del contexto y tarea de cada una de esas actividades. Los resultados se representan gráficamente en un árbol de eventos de AFH, siendo una representación formal de la secuencia de acciones requerida. THERP se sirve de una extensa base de datos de fiabilidad humana que contiene PEH, las cuales se han inferido a partir de datos de planta y juicio de expertos. También tiene en cuenta el efecto de otros PSF, como la experiencia, la carga de trabajo, el estrés, los procedimientos, etc., los cuales deben ser identificados por los expertos.

### 6.2.1.3 Modelo APS refinado

La IAEA establece que el proceso de evaluación de la seguridad debe incluir el uso complementario del análisis determinista y el análisis probabilista de seguridad (IAEA, 2016). Los árboles de eventos (ET) y los árboles de fallos (FT) del APS se definen a partir del juicio de expertos y son estudiados en detalle a partir de las simulaciones deterministas de la planta, como por ejemplo la simulación termohidráulica de las condiciones físicas de la planta tras un suceso accidental.

El potencial de los códigos *best-estimate* proporciona resultados provechosos en la búsqueda de criterios de éxito y en la configuración apropiada de los escenarios accidentales para un determinado suceso iniciador del APS de una planta. Este hecho muestra la posibilidad de mejora de los modelos APS mediante el uso conjunto de ambas técnicas. El enfoque presentado aquí persigue las siguientes mejoras:

- Identificar y caracterizar los escenarios previamente desconocidos, así como la posible incompletitud, sobreestimando o subestimando el conservadurismo de los modelos del APS y del ADS. Los códigos termohidráulicos BE pueden eva-

luar la idoneidad de los escenarios accidentales preestablecidos en el APS, identificando y caracterizando las secuencias accidentales y los criterios de éxito. Estos resultados se reflejan en el modelo del APS, modificando secuencias y sucesos básicos en los árboles de eventos y los arboles de fallos.

- Modelar y cuantificar con mayor exactitud las PEH de las acciones humanas. Las simulaciones termohidráulicas con códigos BE determinan el tiempo disponible por el operador para realizar las acciones, esto es, la ventana temporal. El resultado de estas simulaciones proporciona estimaciones más realistas de las PEH a través de las técnicas de AFH adecuadas. Las nuevas PEH se incluyen en el APS como nuevos valores de probabilidad de los sucesos básicos correspondientes a los árboles de fallos.

Ambos propósitos conducen al desarrollo de un modelo de APS refinado, el cual proporciona mejores estimaciones en su aplicación para la evaluación y análisis del riesgo.

### 6.2.2. Evaluación del impacto en el riesgo

Seguidamente, partiendo de la Figura 6.1, se presenta la evaluación del impacto en el riesgo mediante la adopción de las métricas de riesgo habituales para analizar los cambios en el tiempo de indisponibilidad permitido (Samanta et al., 1994).

La Guía Reguladora RG 1.174 y la Guía de Seguridad GS 1.14 establecen que el APS debe ser realizado de forma que sea consistente con las prácticas aceptadas, determinando además que la calidad del APS puede ser medida en términos de idoneidad respecto a su alcance, nivel de detalle y aceptabilidad técnica. La Guía Reguladora RG 1.177 exige que la calidad del APS debe ser compatible con las implicaciones en materia de seguridad de los cambios en las ETF solicitados y el papel que adoptan en la justificación del cambio.

El modelo APS original disponible debe entonces ser refinado si es necesario, en base a la revisión de las capacidades del APS para una aplicación particular del cambio en el CT, así como para la forma en que las incertidumbres han de ser evaluadas.

Las medidas de riesgo básicas en la evaluación del impacto en el riesgo de cambios en el CT son (USNRC, 2011): el riesgo instantáneo, el riesgo simple y el riesgo anual. Adoptando la  $FDN$  como métrica de riesgo base, estas tres medidas pueden ser formuladas de la siguiente manera:

$$\Delta FDN_M = FDN_1 - FDN_0 \quad (6.2)$$

$$ICPDN_M = d_M \Delta FDN_M \quad (6.3)$$

$$FDN_M = f_M ICPDN_M \quad (6.4)$$

La Ecuación (6.2) evalúa el incremento de riesgo condicionado a la ocurrencia de un suceso determinado, en el caso de un cambio en el CT, la realización de un mantenimiento. Se formula como la diferencia entre el incremento absoluto de riesgo condicionado conociendo con total certeza que el equipo esta indisponible por mantenimiento,  $FDN_1$  (año<sup>-1</sup>), y la disminución del nivel de riesgo conociendo con total certeza que el equipo no está indisponible por mantenimiento,  $FDN_0$  (año<sup>-1</sup>). La Ecuación (6.3) evalúa el riesgo simple a través del Incremento Condicional de la Probabilidad de Daño al Núcleo ( $ICPDN_M$ ), representando el riesgo esperado sobre la duración del periodo de indisponibilidad asociado con el CT,  $d_M$ . La Ecuación (6.4) evalúa la contribución de la desviación al riesgo medio a largo plazo, el cual se asume normalmente como un año, pudiendo representarse como el producto de la frecuencia de ocurrencia del CT a lo largo de un año  $f_M$ , por el riesgo simple asociado a la duración del CT.

En general, la RG 1.174 establece dos métricas de riesgo para evaluar el impacto en el riesgo de cualquier cambio en la base de licencia. Estos son la Frecuencia de Daño al Núcleo anual,  $FDN$ , y el cambio anual en la Frecuencia de Daño al Núcleo,  $\Delta FDN$ , la cual puede formularse como:

$$\Delta FDN = FDN_a - FDN_b \quad (6.5)$$

Donde  $FDN_b$  y  $FDN_a$  son la Frecuencia de Daño al Núcleo antes y después del cambio, respectivamente. Utilizando los resultados de S. Martorell, Martón, et al. (2014) y S. Martorell, Villamizar, et al. (2014), se obtiene la siguiente relación:

$$FDN = FDN_0 + u_M \Delta FDN_M = FDN_0 + FDN_M \quad (6.6)$$

Siendo  $u_M$  la indisponibilidad media del componente debida al mantenimiento. Nótese que el término  $FDN_M$  viene dado por la Ecuación (6.4). Además, la Ecuación (6.5) puede reescribirse a partir de la Ecuación (6.6) como:

$$\Delta FDN = (u_{M,a} - u_{M,b}) \Delta FDN_M = \Delta u_M \Delta FDN_M \quad (6.7)$$

Donde  $\Delta u_M = f_M (d_{M,a} - d_{M,b})$  representa la diferencia en la contribución a la indisponibilidad debida al tiempo fuera de servicio antes y después del cambio.

De forma específica para las ETF, la RG 1.177 establece una métrica de riesgo específica para evaluar el impacto en el riesgo asociado con el cambio en el CT. Esta se corresponde con la Ecuación (6.3), del riesgo simple, el cual se determina a partir del tiempo fuera de servicio asumido,  $d_M$ .

Finalmente, la RG 1.177 señala la necesidad de analizar una tercera métrica de riesgo para cambios en el CT,  $\Delta FDN_M$ , la cual es dependiente del riesgo condicionado, tal y como se fórmula en la Ecuación (6.2).

### 6.2.3. Análisis del impacto en el riesgo

En este último paso, el análisis de riesgo consiste en la comparación de los resultados de la evaluación del impacto en el riesgo del cambio con los criterios de aceptación, incluyendo el tratamiento de las incertidumbres (Caruso et al., 1999).

Adoptando las métricas de riesgo precedentes, el impacto en el riesgo debe ser calculado de forma que las incertidumbres sean tratadas de la manera más apropiada. Esto incluye la identificación de las incertidumbres ligadas con los modelos y datos de APS, así como de las fuentes de incertidumbre de modelo y de parámetro relacionadas con los supuestos del cambio en el CT.

Una vez que el impacto en el riesgo del cambio en el modelo de APS ha sido evaluado, debe ser comparado con los criterios de aceptación dados en la RG 1.174 (véase la sección 2.4 de la RG 1.174). Además, para cambios en las ETF, el impacto en el riesgo debe ser comparado con los criterios de aceptación definidos en la sección 2.4 de la RG 1.177.

En particular, la RG 1.177 propone adoptar dos criterios de aceptación para la evaluación de cambios en el CT empleando un APS de Nivel 1. El primero coincide con el propuesto en la Guía Reguladora RG 1.174 para evaluar cualquier cambio en la base de licencia, usando la FDN de referencia,  $FDN$ , y la  $\Delta FDN$ . Luego, los valores límites establecidos por los criterios de aceptación se describen en la RG 1.174 como regiones definidas en el espacio de los valores  $\{FDN, \Delta FDN\}$ , donde se sitúan los resultados del impacto en el riesgo del cambio en el CT (Figura 6.2).

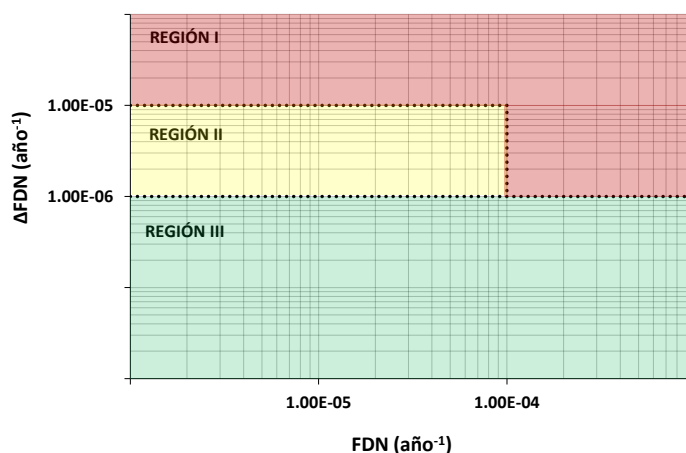


Figura 6.2 Criterios de aceptación definidos en la RG 1.174 para  $\{FDN, \Delta FDN\}$

La RG 1.177 establece otro criterio de aceptación específico para evaluar el riesgo asociados a cambios en el CT, relacionándolos con la métrica de riesgo simple de un CT evaluada tras el cambio en el CT. Determina que el propietario debe demostrar que el cambio en el CT solo tiene un pequeño impacto cuantitativo en el riesgo condicionado de la planta. Por ejemplo, un  $ICPDN$  menor de  $5.0E-07$  se considera pequeño para un solo cambio del CT usando un APS de Nivel 1. En relación a este segundo criterio, la RG 1.177 establece que la contribución del  $ICPDN_M$  debe distribuirse en el tiempo de manera que cualquier incremento en el riesgo condicional asociado esté dentro de la normalidad de la fluctuación de la evolución del riesgo de la central. El valor límite asumido para  $ICPDN$  de  $5.0E-07$  se deriva de la situación hipotética en la cual el equipo estudiado en una planta representativa está fuera de servicio 5 horas. Esto provoca un aumento en la FDN de la planta, considerando una FDN de referencia de  $1.0E-04$  por reactor año, que aumenten su riesgo condicional  $1.0E-03$  reactor año durante este periodo de 5 horas. En base a este segundo criterio de aceptación de la RG 1.177, se puede definir dos regiones del espacio de valores  $\{FDN_I, ICPDN\}$  donde se sitúan los resultados del impacto en el riesgo del cambio en el CT. La región de aceptación del cambio se sitúa por debajo del punto  $\{1.0E-03, 5.0E-07\}$ .

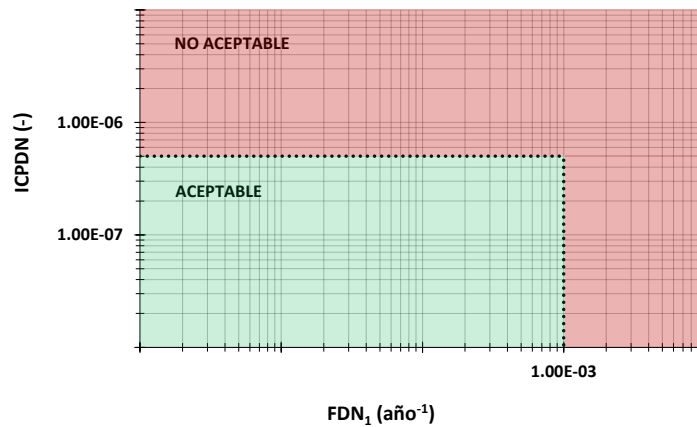


Figura 6.3 Criterios de aceptación definidos en la RG 1.177 para  $\{FDN_I, ICPDN_M\}$

### 6.3. Caso de aplicación

Este apartado muestra los resultados de combinar los modelos determinista y probabilista en la evaluación del impacto en el riesgo de un cambio en el CT del Sistema de Extracción del Calor Residual (*Residual Heat Removal System*, RHR) de un reactor PWR, considerando la evaluación del cambio en las acciones humanas mediante el AFH. Con el fin de simplificar, solo se estudia en detalle el escenario accidental de pérdida del RHR durante el proceso de enfriamiento en parada caliente (Modo 4 de la central). El análisis de esta secuencia se enmarca en el APS en Otros Modos de operación (APSOM) de un reactor de agua a presión.

La metodología propuesta en el Apartado 6.2 se utiliza para evaluar y analizar el impacto en el riesgo del cambio propuesto, a partir del APS refinado. Previamente, se lleva a cabo el análisis determinista con el fin de modelar con la mayor fidelidad el escenario accidental de pérdida del RHR, de manera que se ajusten mejor las PEH. En el Apartado 6.3.1, se propone el modelo refinado a partir del modelo APS original (Apartado 6.3.2.1), el cual tiene en cuenta los resultados del análisis TH desarrollado en el Apartado 6.3.2.2. Tomando como punto de partida el análisis TH, la PEH se recalcula, mostrando los resultados en el Apartado 6.3.2.3. El conjunto de estos resultados conducen a la elaboración del modelo refinado para el escenario accidental de pérdida del RHR, que se presenta en el Apartado 6.3.2.4. Finalmente, los Apartados 6.3.2.5 y 6.3.3 muestran los resultados de la evaluación y el análisis del impacto en el riesgo del cambio en el CT utilizando el nuevo modelo.

#### 6.3.1. Descripción del sistema y cambio del CT propuesto

El RHR consiste en dos subsistemas mecánicos redundantes e independientes, los cuales reciben suministro eléctrico desde uno de los dos trenes eléctricos. Cada subsistema está compuesto por una bomba, un intercambiador de calor y sus correspondientes tuberías, válvulas e instrumentación. La función principal del RHR es extraer el calor de decaimiento, que permanece en el núcleo del reactor para reducir la temperatura del Sistema de Refrigerante del Reactor (SRR) durante el enfriamiento de la planta y el periodo de recarga.

En condiciones de parada caliente (Modo 4), un tren del RHR extrae el calor residual del núcleo. Cuando el RHR pierde el tren que está operando, los procedimientos de emergencia solicitan la comprobación manual de la disponibilidad del tren redundante, el cual normalmente se encuentra en espera. Una acción humana, AH1, se requiere para arrancar manualmente el tren redundante. Si el tren en espera no es recuperado, una manera alternativa de enfriar el núcleo es empleando el inventario de agua de los generadores de vapor (GV) del secundario, los cuales se encuentran en conservación húmeda. Sin embargo, el Sistema de Agua de Alimentación Auxiliar (AAA) debe arrancar para evitar el secado de los GV. Una acción humana, AH2, se requiere para arrancar las bombas del AAA manualmente. Si no es posible extraer el calor a través de los GV, la función de



*Feed and Bleed* es requerida. Las bombas de carga inyectan agua para recuperar el inventario perdido y mantener el enfriamiento, mientras que el calor residual se extrae a través de las válvulas de alivio de los GV o de la válvula de seguridad del RHR. En este caso, es necesario restituir el depósito de almacenamiento de agua de recarga (*Refueling Water Storage Tank*, RWST) para mantener la planta en condiciones estables.

Las ETF del modelo APSOM establecen que el RHR solo puede permanecer inoperable 1 hora, esto es, que el CT es de 1 hora cuando opera en parada caliente. Las condiciones límites de operación especifican que las bombas del RHR solo pueden ser desenergizadas durante un tiempo de 1 hora. El cambio en el CT propuesto consiste en extender el actual CT de 1 a 24 horas.

### 6.3.2. Modelado del impacto en el riesgo

#### 6.3.2.1 Modelo APS original

El APSOM de Nivel 1 de un reactor PWR es usado como modelo de referencia. El árbol de eventos original para la pérdida del RHR en Modo 4 de una central incluye las tres funciones de seguridad siguientes, como puede observarse en la Figura 6.4.

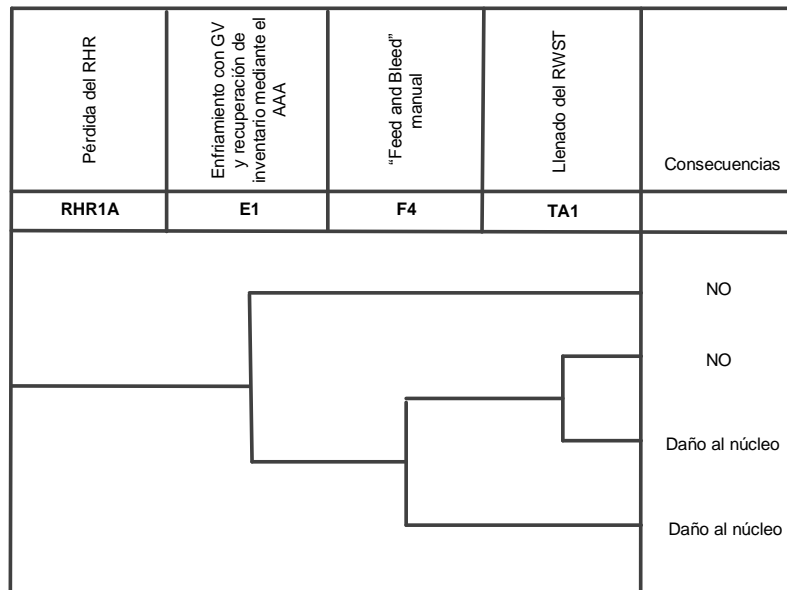


Figura 6.4 Modelo original del árbol de eventos para la pérdida del RHR

La primera función de seguridad, E1, determina que los GV son una alternativa para evacuar el calor residual. De manera conservadora, solo requiere de dos GV, cuyo inventario debe ser recuperado a través de las bombas del AAA.

La segunda función, F4, requiere de la operación manual de *Feed and Bleed* con una bomba de carga del RWST.

La tercera función de seguridad, TA1, consiste en el llenado del RWST. El inventario de agua debe ser mantenido a través de las bombas de carga del RWST para asegurar que el calor residual es extraído del núcleo del reactor.

Por lo tanto, en el modelo APS original, la posibilidad de recuperar el tren del RHR en servicio no se considera, es decir, AH1 no se tiene en cuenta. Se asume que la potencia del núcleo en el momento de la pérdida del tren del RHR en funcionamiento es muy alta. Como consecuencia, el umbral de temperatura para arrancar el tren del RHR en reserva se excede rápidamente, no dejando ningún tiempo disponible que permita al operador arrancar el tren redundante del RHR. De esta forma, no se da crédito a AH1.

#### *6.3.2.2 Modelo determinista*

Un reactor PWR de 3 lazos ha sido modelado mediante el código TRACE y ejecutado con la versión V5.0 Patch 4 (USNRC, 2014), usando la interfaz de SNAP para simular las secuencias accidentales mostradas en la Figura 6.4. El modelo termohidráulico del RHR desarrollado está conectado con el sistema primario, como se describe en detalle en Martorell, Sánchez-Sáez, Villanueva, & Carlos (2017).

Este modelo termohidráulico se emplea para estudiar la ventana temporal que dispone el operador para efectuar AH1; arrancar el tren en espera del RHR durante la evolución del transitorio. Con este fin, se ejecutan una serie de simulaciones TH considerando las incertidumbres de los parámetros termohidráulicos.

Por ejemplo, uno de los parámetros más importantes es el relacionado con el momento en el que tiene lugar el suceso iniciador, una vez que la planta se encuentra a baja potencia. La Figura 6.5 considera que el suceso iniciador puede ocurrir de forma aleatoria en un rango que comprende desde 100s hasta 2000s después del inicio de las condiciones de parada caliente del reactor. Este periodo representa aproximadamente la frontera entre las condiciones de parada caliente (Modo 4) y parada fría (Modo 5), considerando el ritmo de enfriamiento normal de la planta. La Figura 6.5 muestra la evolución de la temperatura del SRR ( $T_{SRR}$ ) para distintas simulaciones de la primera de las secuencias accidentales de la Figura 6.4, donde los GV actúan de forma alternativa para enfriar el núcleo. La evolución del transitorio sugiere la posibilidad de arrancar el tren del RHR en espera justo después de la ocurrencia del suceso iniciador, ya que hay suficiente tiempo desde la pérdida del tren del RHR en operación hasta que la temperatura del SRR aumenta por encima de la temperatura umbral ( $T_{límite}$ ) para arrancar el tren de reserva mediante AH1. También es posible recuperar el RHR más tarde, tan pronto como las condiciones de operación lo permitan, gracias al enfriamiento de los GV.

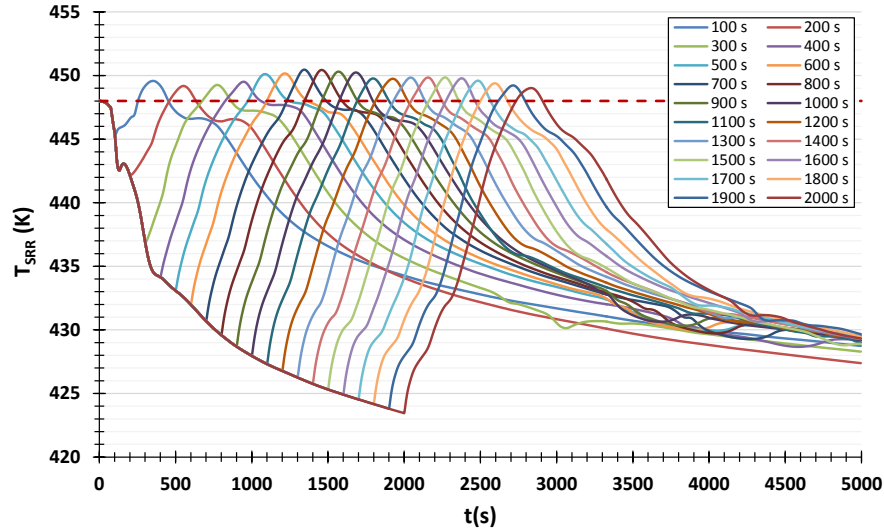


Figura 6.5 Simulaciones TH para la secuencia de pérdida del RHR

La Figura 6.6 muestra una de las simulaciones ejecutadas, para un tiempo de ocurrencia del suceso iniciador de 1000 segundos, tras el inicio de operación del reactor en baja potencia. Este ejemplo expone claramente la existencia de las siguientes VT a lo largo de la evolución de la secuencia accidental.

Primero, a diferencia del modelo APS original, es posible arrancar el tren en reserva del RHR justo después de que falle el tren en operación. El tiempo disponible para efectuar AH1 es suficiente para seguir evacuando el calor del SRR mediante el tren redundante del RHR. El tiempo disponible para llevar a cabo AH1 es VT1.

Segundo, después de que la temperatura se haya incrementado por encima de  $T_{\text{límite}}$ , el calor se evacúa de forma alternativa a través de los GV, los cuales deben mantenerse bajo condiciones de conservación húmeda. Sin embargo, las motobombas del AAA deben arrancarse manualmente para evitar el secado de los mismos, acción correspondiente a AH2. Esta acción ya se contemplaba en el modelo APS original. El tiempo disponible para llevar a cabo AH2 es VT2.

Tercero, los GV permiten reducir la temperatura del SRR por debajo de  $T_{\text{límite}}$ , permitiendo así arrancar el tren en reserva del RHR, lo cual corresponde a AH3. El tiempo disponible para llevar a cabo AH3 es VT3.

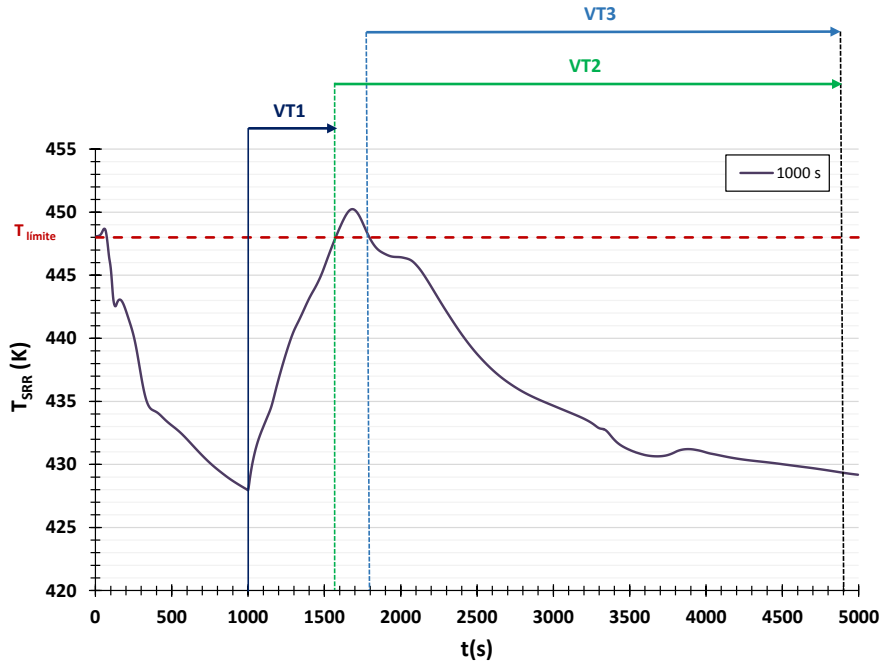


Figura 6.6 Ventanas temporales disponibles durante la secuencia de pérdida del RHR

Por lo tanto, el modelo TH no solo se usa para estudiar las ventanas temporales disponibles para el operador en la ejecución de AH1 a lo largo de la evolución del transitorio, sino también para estudiar las ventanas temporales para efectuar AH2 y AH3. Con este objetivo, se ejecutan una serie de simulaciones termohidráulicas, considerando la incertidumbre de los parámetros termohidráulicos. Se utiliza el método de Monte Carlo con un muestreo de Hípercubo Latino y un tamaño de muestra de 1000 para obtener muestras de las ventanas temporales VT1, VT2 y VT3.

### 6.3.2.3 Cálculo de la PEH

Una vez que las diferentes ventanas temporales se han determinado partiendo de las simulaciones TH, las correspondientes PEH deben ser evaluadas para cada ventana temporal, usando los correspondientes valores de VT1, VT2 y VT3. La relación entre las acciones humanas relacionadas con esta secuencia, las VT extraídas de las simulaciones TH y los errores humanos son las siguientes:

- Fallo del operador al realizar la AH1 para arrancar el tren en reserva del RHR durante la VT1, llamada FORHRS\_W2.
- Fallo del operador al realizar la AH2 para arrancar el tren en reserva del RHR durante la VT3, llamada FORHRS\_E1.

- Fallo del operador al realizar la AH1 para arrancar las motobombas del AAA durante la VT2, llamada FOAFWS\_E1.

El cálculo de la PEH depende de  $P_d$  y  $P_e$ , como se muestra en la Ecuación (6.1).

Para la fase de diagnóstico,  $P_d$  se calcula con el método TRC para cada error humano, FORHRS\_W2, FOAFWS\_E1 y FORHRS\_E1; considerando el correspondiente tiempo disponible, VT1, VT2 y VT3; respectivamente. El cálculo se realiza a partir de los datos de la correlación entre el tiempo de respuesta y la probabilidad, proporcionados en la Figura 6-1 de Hall et al. (1982), considerando que son acciones basadas en reglas sin ambigüedad. La probabilidad  $P_d$  representa la probabilidad de fallo de un diagnóstico equivocado en cada VT.

Para la fase de ejecución, la probabilidad de fallo en la ejecución  $P_e$  se calcula mediante el método THERP. Cada acción humana asociada con una VT es dividida en tareas más simples, requeridas para ejecutar satisfactoriamente la acción correspondiente. Luego, la probabilidad de fallo de estas tareas simples se estima usando la Tabla 20-1 y siguientes de Swain & Guttman (1983). El estrés durante la operación se considera como factor de influencia en el cálculo de  $P_e$ . Se asume inicialmente un alto nivel de estrés en tareas rutinarias o procedimentales, puesto que el operador dispone de un corto periodo determinado por el CT para ejecutar de forma exitosa todas las tareas (véase Tabla 17-1 de Swain & Guttman (1983)). Originalmente, para las acciones humanas AH1 y AH3, los operadores disponen como máximo de 1 hora para ejecutar las acciones, sin importar la disponibilidad de VT1 y VT3. Esto es debido a que las ETF vigentes establecen que el RHR solo puede estar fuera de servicio durante una hora, es decir, el tiempo de indisponibilidad permitido es de 1 hora según las ETF.

La Tabla 6.1 proporciona los resultados obtenidos mediante el análisis de fiabilidad humana. Esta tabla muestra ambas contribuciones, la probabilidad de error en la fase de diagnóstico ( $P_d$ ) y la probabilidad de error en la fase de ejecución ( $P_e$ ), así como la PEH total, calculada mediante la Ecuación (6.1) para cada ventana temporal. Estas probabilidades de error se caracterizan a través de sus valores medios y las desviaciones típicas de una distribución log-normal, la cual se ha determinado por el método de Monte Carlo con un muestreo de Hipercubo Latino. Las PEH obtenidas se incluyen en el modelo de APS refinado para otros modos.

**Tabla 6.1 PEH obtenida para cada ventana temporal**

Ventana temporal	Suceso básico	$P_d$		$P_e$		PEH	
		Media	Desviación típica	Media	Desviación típica	Media	Desviación típica
VT1	FORHRS_W2	6.94E-03	2.93E-04	1.00E-02	6.14E-04	1.69E-02	1.75E-03
VT2	FOAFWS_E1	4.91E-06	1.47E-10	1.56E-03	1.56E-05	1.60E-03	1.57E-05
VT3	FORHRS_E1	4.16E-05	1.05E-08	1.00E-02	6.14E-04	1.00E-02	6.20E-04

### 6.3.2.4 Modelo APS refinado

Como consecuencia de los resultados derivados del análisis determinista y el cálculo de las PEH, es necesario introducir ciertas modificaciones al árbol de eventos correspondiente a la pérdida del RHR del modelo APS original.

Por un lado, el modelo APS original no contemplaba la posibilidad de arrancar el tren en reserva del RHR. Se asumía que  $T_{\text{límite}}$  se superaba rápidamente, no dejando margen a que el operador realizará dicha acción. Sin embargo, las simulaciones TH dan crédito a la posibilidad de arrancar el tren redundante, es decir, a realizar AH1, con una probabilidad de error humano FORHRS \_W2. Se añade por tanto un nuevo cabecero, W2\*, además de una nueva secuencia en el árbol de eventos que conduce a la planta a un estado seguro. La Tabla 6.1 muestra el valor de la PEH para FORHRS \_W2.

Por otro lado, las simulaciones TH demuestran que es posible recuperar el tren redundante del RHR más tarde, cuando la temperatura del SRR desciende por debajo de  $T_{\text{límite}}$ . Este hecho tiene lugar tras usar el inventario inicial de los GV mantenidos en conservación húmeda. En este caso, existen dos opciones para que la función de seguridad E1 logre el éxito: bien arrancar las motobombas del AAA llevando a cabo la AH2 o bien arrancar el tren en reserva del RHR ahora disponible, mediante la AH3. El nuevo cabecero en este caso se le denomina E1\*. La Tabla 6.1 muestra el valor de las PEH para las acciones AH2 y AH3, correspondientes a FOAFWS \_E1 y FORHRS \_E1, respectivamente.

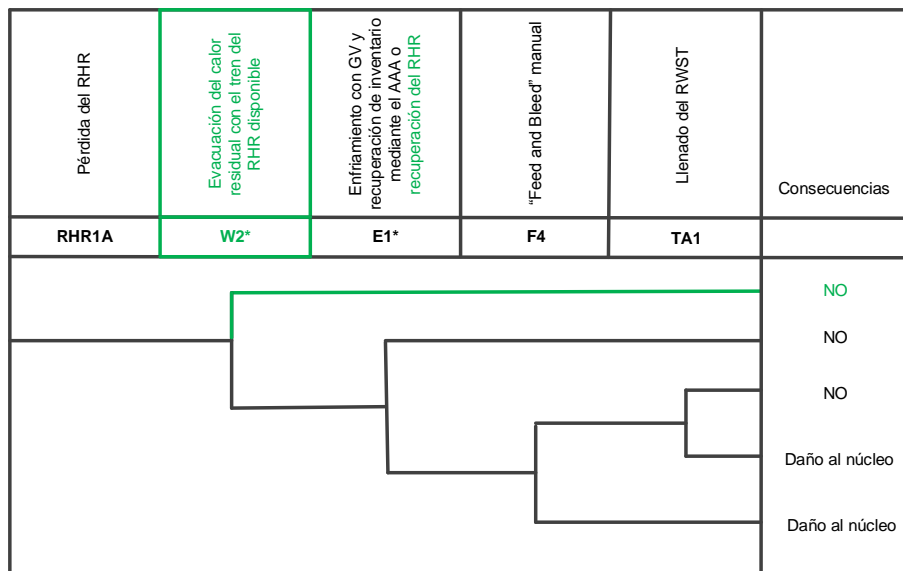


Figura 6.7 Modelo refinado del árbol de eventos para la pérdida del RHR

La Figura 6.7 muestra el árbol de eventos refinado de pérdida del RHR, incluyendo el nuevo cabecero W2\* y actualizando el cabecero E1\*. El árbol de fallos E1\* sustituye al árbol de fallos original E1 (véase Figura 6.8). Estos cambios, junto a las modificaciones de las PEH de las acciones mencionadas, determinan el modelo APS refinado.

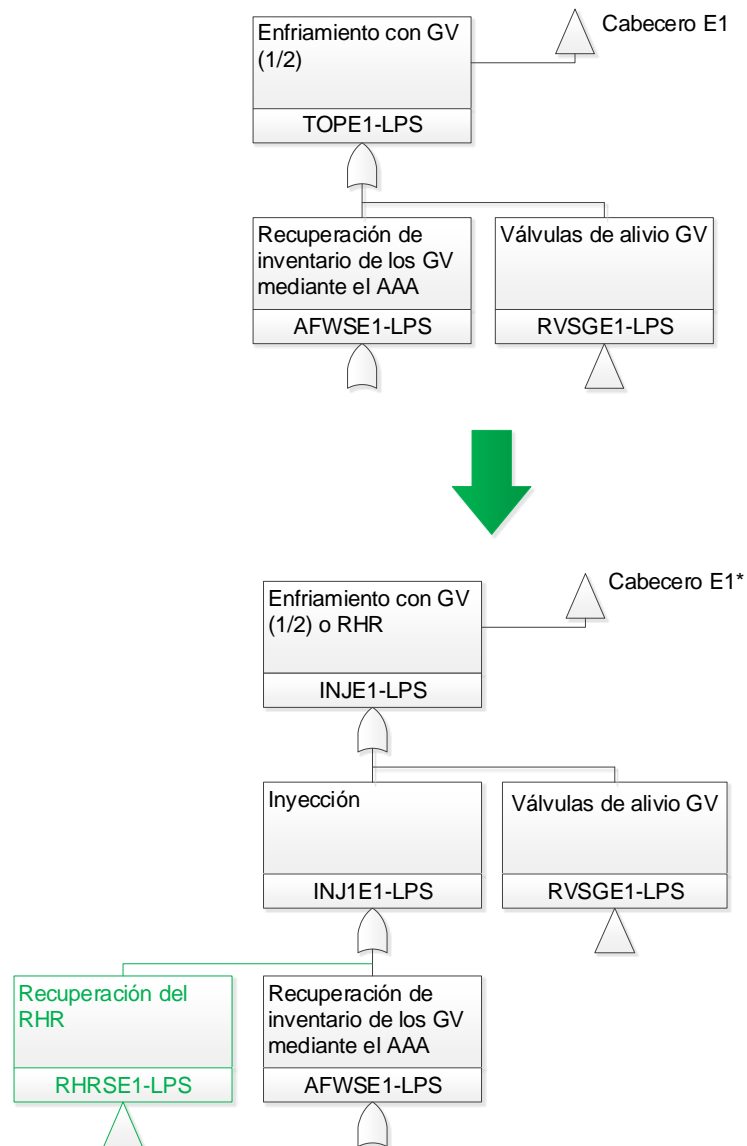


Figura 6.8 Modificación del árbol de fallos correspondiente a la función de seguridad E1

### 6.3.2.5 Evaluación del impacto en la fiabilidad humana y el riesgo del cambio en el CT

El cambio en el CT propuesto consiste en extender el actual tiempo de indisponibilidad permitido del RHR en otros modos de 1 hora hasta 24 horas. El cambio supone que el operador dispondrá de más tiempo para realizar las acciones requeridas, y por tanto, el nivel de estrés se reducirá. Este hecho repercute en la fase de ejecución de la acción.

Las PEH mostradas en la Tabla 6.1 son reevaluadas teniendo en cuenta el nuevo CT. Las PEH y sus contribuciones son calculadas tal como se explica en el Apartado 6.3.2.3, adoptando ciertas modificaciones. Así, el cambio solo afecta a la probabilidad de error en la fase de ejecución,  $P_e$ , de las acciones humanas ejecutadas sobre el RHR, es decir, AH1 y AH3. Específicamente,  $P_e$  se recalcula considerando un nivel de estrés bajo (véase la Tabla 17-1 en Swain & Guttman (1983)). El cambio no afecta a la probabilidad de error en el diagnóstico,  $P_d$ , porque las ventanas temporales VT1 y VT3 son menores a 1 hora. Por lo tanto, extender de 1 a 24 horas el CT no tiene impacto en el diagnóstico.

Los resultados de los cálculos en las PEH tras el cambio propuesto se exponen en la Tabla 6.2. Reseñar que las PEH son caracterizadas por un valor medio, así como por la desviación típica para una distribución log-normal.

**Tabla 6.2 PEH obtenida para cada ventana temporal tras el cambio en el CT**

Ventana temporal	Suceso básico	$P_d$		$P_e$		PEH		$\Delta PEH$ (%)
		Media	Desviación típica	Media	Desviación típica	Media	Desviación típica	
VT1	FORHRS_W2	6.94E-03	2.93E-04	2.00E-03	2.45E-05	8.94E-03	4.87E-04	-89.6%
VT2	FOAFWS_E1	4.91E-06	1.47E-10	1.60E-03	1.56E-05	1.60E-03	1.57E-05	0.0%
VT3	FORHRS_E1	4.16E-05	1.05E-08	2.01E-03	2.45E-05	2.05E-03	2.56E-05	-391.7%

En la Tabla 6.2, la columna 9 muestra  $\Delta PEH$ , la cual mide la subida o caída en el valor de la PEH calculada en la Tabla 6.1. Los resultados señalan que la PEH de AH1 y AH3 son considerablemente menores tras el cambio en el CT.

Una vez que la PEH ha sido calculada para cada acción humana considerada, el modelo APS refinado en otros modos, se usa para calcular de forma apropiada el riesgo. Específicamente, las medidas básicas de riesgo  $FDN_1$  y  $FDN_0$ , las cuales permiten calcular el incremento condicional del nivel de riesgo,  $\Delta FDN_M$ , usando la Ecuación (6.2).

El CT fue utilizado en vez del tiempo medio para el mantenimiento,  $d_M$ , para calcular la segunda métrica de riesgo, el incremento condicional de la probabilidad de daño al núcleo asociado con un tiempo de indisponibilidad asociado con el CT,  $ICPDN_M$ , dada por la Ecuación (6.3).



La frecuencia de ocurrencia de la CLO se estima utilizando datos reales del mantenimiento de un reactor PWR, siendo aproximadamente.  $f_M=0.00137$  año<sup>-1</sup>. Cabe destacar que este parámetro es necesario para cuantificar el riesgo anual debido al CT,  $FDN$ , usando la Ecuación (6.4). Partiendo de esta métrica, se halla  $\Delta FDN$  mediante la Ecuación (6.7).

La Tabla 6.3 proporciona los resultados de las métricas de riesgo,  $FDN_1$  y  $ICPDN_M$ , antes y después del cambio. La Tabla 6.4 contiene los resultados de las métricas de riesgo,  $FDN$  y  $\Delta FDN$ . Ambas tablas incluyen no solo los valores medios, sino también los percentiles de las distintas métricas.

**Tabla 6.3 Impacto del cambio en el CT en  $FDN_1$  e  $ICPDN_M$**

Estudio	$FDN_1$ (año <sup>-1</sup> )			$ICPDN_M$ (-)		
	Media	5% perc.	95% perc.	Media	5% perc.	95% perc.
Modelo APS refinado [CT=1h]	1.18E-05	5.20E-06	2.33E-05	3.76E-10	1.67E-10	7.65E-10
Modelo APS refinado [CT=24h]	1.12E-05	5.07E-06	2.21E-05	8.88E-09	3.89E-09	1.84E-08

**Tabla 6.4 Impacto del cambio en el CT en  $\Delta FDN$**

Estudio	$FDN$ (año <sup>-1</sup> )			$\Delta FDN$ (-)		
	Media	5% perc.	95% perc.	Media	5% perc.	95% perc.
Modelo APS refinado [CT de 1 hasta 24 h]	8.59E-06	3.83E-06	1.57E-05	1.17E-11	5.10E-12	2.41E-11

### 6.3.3. Aceptación del impacto en el riesgo

Este apartado compara los resultados obtenidos en el apartado precedente, con los criterios de aceptación establecidos en las guías reguladoras RG 1.174 y RG 1.177.

En primer lugar, la pareja de valores que representan  $\{FDN, \Delta FDN\}$  se debe situar en la región correspondiente al primer criterio de aceptación establecido por la RG 1.174 y la GS 1.14. Las regiones del espacio de dicho criterio se han representado anteriormente en la Figura 6.2. La Figura 6.9 muestra la evaluación del impacto en el riesgo del cambio en el CT, incluyendo la reevaluación de las PEH. De acuerdo a la RG 1.174, las medidas apropiadas para comparar los valores numéricos señalados por los criterios de aceptación con los resultados obtenidos en el APS son los valores medios, los cuales se refieren a la media de las funciones de distribución de probabilidad, resultado de la propagación de las incertidumbres de los parámetros de entrada y las incertidumbres de modelo. Estos valores se representan explícitamente por el punto medio representado en la Figura 6.9.

Los resultados antes y después del cambio en el CT, incluyendo la reevaluación de las PEH, confirman que las directrices todavía se cumplen, incluso teniendo en cuenta las nuevas hipótesis asumidas. Es decir, los valores obtenidos tras el cambio permanecen en la región apropiada tanto para su valor medio como para sus percentiles, como se observa en la Figura 6.9.

Por otro lado, la pareja de valores  $\{FDN_1, ICPDN_M\}$  es comparada en este caso con el segundo criterio de aceptación, definido en la RG 1.177 y representado anteriormente en la Figura 6.3. Los resultados del cambio en el CT, incluyendo la reevaluación de las PEH, permanecen en la región apropiada tanto para sus valores medios como para los percentiles, como se observa en la Figura 6.10.

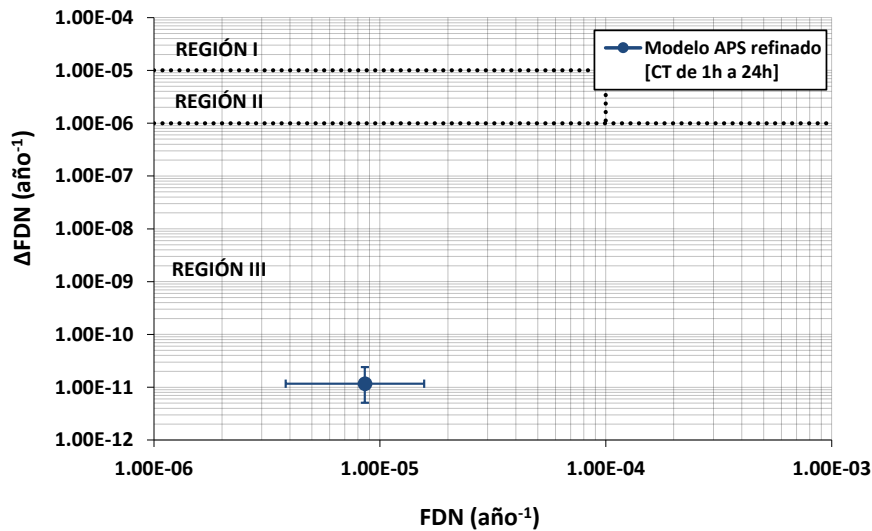


Figura 6.9 Impacto del cambio en el CT para  $\{FDN, \Delta FDN\}$

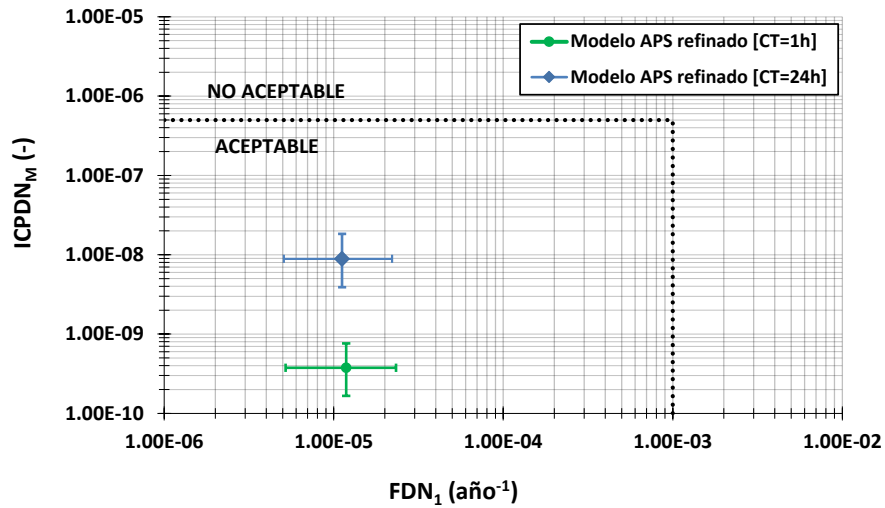


Figura 6.10 Impacto del cambio en el CT para  $\{FDN_1, ICPDN_M\}$

En síntesis, el cambio en el CT es aceptable desde el punto de vista del riesgo comparando los resultados de  $\{FDN, \Delta FDN\}$  con el primer criterio de aceptación, establecido en la RG 1.174. Además, la reevaluación de las PEH, teniendo en cuenta el estrés del operador como PSF, muestra una caída de  $FDN_1$ , hecho que es consistente con valores más bajos de las PEH. Sin embargo, el incremento del CT de 1h a 24h propuesto muestra un aumento en  $ICPDN_M$ , aunque desde el punto de vista del riesgo, el cambio es aceptable.



# Capítulo 7

## Conclusions and contributions

### 7.1. Conclusions

The first chapter of the Ph. Dissertation has pointed out some of relevant questions at present about NPPs safety; with the purpose of delimit the objectives of this work. These could be synthesizing in the development of models, methods and tools, which contribute to RIDM. Not only in the current framework of nuclear facilities, but especially also in a Long Term Operation scenario for the next years.

PSA allows estimating quantitatively the risk of an industrial facility. In nuclear area, the number of PSA applications have been increased considerably in last 20 years, with the aim of obtain profits to improve reactors safety. However, at present, PSA models are not able to evaluate risk impact of the ageing of safety-related SSC, due to their reliability and unavailability parameters do not depend explicitly on factors like degradation, or effects that introduce surveillance requirements and maintenance activities. Likewise, probability human errors, which also are a critical part of a PSA quantification, are subject to a huge uncertainty. Inconsistencies among analysts to evaluate human behaviour as well as the different hypothesis that adopts different HRA techniques are responsible of the remarkable differences in their results. Both facts justify the search of alternatives to this modelling, and consequently, the research described in this document.

In this context, Ph. Dissertation has covered the following objectives:

Firstly, it has developed in Chapter 3 a new reliability and unavailability model of a time-dependent probability failure on demand. The model considers explicitly degradation by

demand-induced stress, maintenance effectiveness and test efficiency. This model adds to age-dependent standby failure rate (Martón et al., 2015), knocking RAM model into shape which captures in a greater detail the safety components behaviour.

Next, Chapter 4 has focused on the parameters estimation of standby related and demand failure probability models, through an historical data of a NPP, which includes failures, maintenance activities and surveillance tests. It proposes a maximum likelihood estimation (MLE) approach for parameter estimation of both reliability models and to select the imperfect maintenance model, which had better adjust the component performance.

Later, it has validated in Chapter 5 the RAM model developed in previous chapters, within the framework of RIDM. It has been defined an age-dependent risk model based on RAM model. Both models are useful to select the most suitable approach for establishing surveillance test and preventive maintenance intervals, adopting RAM and risk criteria dictated by Technical Specifications and Maintenance Rule.

Finally, in Chapter 6, it has presented a methodology to evaluate the risk impact of completion time changes, combining PSA and DSA model insight and human reliability analysis. Using best-estimate codes, it has been demonstrated their capacity to obtain new accident scenarios for a postulated Initiating Event of a PSA. Moreover, it provides better accuracy in modelling human actions and quantifying their respective human error probabilities (HEP). The methodology presented includes treatment, identification and analysis of uncertainties associated with human actions and Technical Specifications changes.

Regarding future work, following the lines of research where this PhD is delimited, it is necessary to remark new fields like the following ones:

- Parameters estimation: safety components of NPP are characterized by a high reliability performance. Therefore, it is difficult to find failures in their historical data. Consequently, the results of parameter estimation are affected by an important degree of uncertainty. Related to this difficulty, it will be interesting to use other methods and techniques, like Bayesian inference, as an alternative to classic or frequentist techniques. The aim is to provide reliable results and to develop in a higher detail the different variables that include the RAM model exposed in this work.
- Managing technological obsolescence: obsolescence is defined as becoming out of date in comparison with current knowledge, codes, standards and regulations, and technology. Specially, general aspects of technological obsolescence have to be addressed within a part of Ageing Management Programs. In relation to the RAM model formulated in this document, it would be interesting modelling aspects such as the reduction of the effectiveness of preventive and corrective maintenance. Furthermore, given the impossibility of replacing the component, the unavailability caused in the systems by the increase in the duration of the

maintenance, or the ageing factor of a component once the obsolescence of the same has been reached.

- Study of the joint use of best-estimate codes and human reliability analysis: The case study presented in this work shows the potential of using best-estimate codes to determine time windows of operator actions, and lastly, in quantifying human error probabilities from human reliability analysis. As a part of the Safety Study, it will be certainly interesting compare the estimated results with operators simulator experiences, for other accidental sequences.

## 7.2. Scientific contributions

During the development of this thesis, the author published different articles to international scientific journals and contributed to international and national conferences. Table 7.1 presents the link between each contribution and the chapter, which it refers.

	Chapter 3	Chapter 4	Chapter 5	Chapter 6
1				X
2		X		
3	X			
4				X
5		X		
6			X	
7		X		
8		X		
9			X	
10	X			
11				X
12			X	
13				
14	X			
15			X	
16			X	

17			X	
18				X
19		X		
20	X			
21			X	
22	X			
23				X
24	X			
25			X	
26	X			
27			X	
28			X	
29			X	
30				X

**Tabla 7.1 Link between contributions and thesis chapters**

### *7.2.1. Articles in international scientific journals*

- Title:** Evaluation of risk impact of completion time changes combining PSA and DSA model insight and human reliability analysis  
**Authors:** Martorell, Pablo; Martorell Alsina, Sebastián Salvador; Sánchez Galdón, Ana Isabel; Martón Lluch, Isabel; Sánchez Sáez, Francisco, Saiz, Matilde.  
**Journal:** Reliability Engineering & System Safety (ISSN: 0951-8320)  
Volume: 178                      Pages: 97-107                      Year: 2018  
<https://doi.org/10.1016/j.res.2018.05.008>
- Title:** Parameter estimation of a reliability model of demand-caused and standby-related failures of safety components exposed to degradation by demand stress and ageing that undergo imperfect maintenance  
**Authors:** Martorell, Pablo; Martón Lluch, Isabel; Martorell Alsina, Sebastián Salvador; Mullor, Rubén; Sánchez Galdón, Ana Isabel



**Journal:** Mathematical Problems in Engineering (ISSN: 1563-5147)  
Volume: - Pages: - Year: 2017  
<https://doi.org/10.1155/2017/7042453>

- 3 **Title:** Unavailability model for demand-caused failures of safety components addressing degradation by demand-induced stress, maintenance effectiveness and test efficiency  
**Authors:** Martorell, Pablo; Martorell Alsina, Sebastián Salvador; Sánchez Galdón, Ana Isabel; Martón Lluch, Isabel  
**Journal:** Reliability Engineering & System Safety (ISSN: 0951-8320)  
Volume: 168 Pages: 18-27 Year: 2017  
<https://doi.org/10.1016/j.ress.2017.05.044>
- 4 **Title:** An approach to address probabilistic assumptions on the availability of safety systems for deterministic safety analysis  
**Authors:** Martorell Alsina, Sebastián Salvador; Martorell Aigües, Pablo; Martón Lluch, Isabel; Sánchez Galdón, Ana Isabel; Carlos Alberola, Sofía  
**Journal:** Reliability Engineering & System Safety (ISSN: 0951-8320)  
Volume: 160 Pages: 136-150 Year: 2017  
<https://doi.org/10.1016/j.ress.2016.12.009>
- 5 **Title:** Optimization of test and maintenance of ageing components consisting of multiple items and addressing effectiveness  
**Authors:** Martón Lluch, Isabel; Martorell Aigües, Pablo; Ruben; Sánchez Galdón, Ana Isabel; Martorell Alsina, Sebastián Salvador  
**Journal:** Reliability Engineering & System Safety (ISSN: 0951-8320)  
Volume: 153 Pages: 151-158 Year: 2016  
<https://doi.org/10.1016/j.ress.2016.04.015>

### 7.2.2. Contributions to international conferences

- 6 **Title:** A comparison between multi-objective optimization approaches for the harmonization of surveillance requirements and maintenance  
**Authors:** Martorell Aigües, Pablo  
**Conference:** 29th European Conference on Operational Research (EURO2018)  
**City:** Valencia, Spain Data: 11/07/2018  
**ISBN:** 978-84-09-02938-9
- 7 **Title:** Modelling demand-caused failures. Estimation procedure  
**Authors:** Mullor, Rubén; Martorell Aigües, Pablo; Martorell Alsina, Sebastián Salvador; Sánchez Galdón, Ana Isabel

- Conference:** 28th European Safety and Reliability Annual Conference (ESREL 2018)  
**City:** Trondheim, Norway **Data:** 17/06/2017  
**ISBN:** 978-0-815-38682-7
- 8 **Title:** Time-dependent unavailability model integrating on demand-caused and standby-related failures addressing positive and negative effects of testing and maintenance  
**Authors:** Martorell Aigües, Pablo; Martón Lluch, Isabel; Martorell Alsina, Sebastián Salvador; Sánchez Galdón, Ana Isabel; Carlos Alberola, Sofía  
**Conference:** 28th European Safety and Reliability Annual Conference (ESREL 2018)  
**City:** Trondheim, Norway **Data:** 17/06/2017  
**ISBN:** 978-0-815-38682-7
- 9 **Title:** An overview of optimization criteria in the context of advanced surveillance requirements  
**Authors:** Martorell Aigües, Pablo; Martón Lluch, Isabel; Martorell Alsina, Sebastián Salvador; Sánchez Galdón, Ana Isabel; Mullor, Rubén; Carlos Alberola, Sofía  
**Conference:** 27th European Safety and Reliability Annual Conference (ESREL 2017)  
**City:** Portoroz, Slovenia **Data:** 22/06/2017  
**ISBN:** 978-1-138-62937-0
- 10 **Title:** Unreliability model for degradation effects of safety components addressing demand-included stress and maintenance effectiveness  
**Authors:** Martorell Aigües, Pablo; Carlos Alberola, Sofía; Martorell Alsina, Sebastián Salvador; Sánchez Galdón, Ana Isabel; Martón Lluch, Isabel, Sofía  
**Conference:** 27th European Safety and Reliability Annual Conference (ESREL 2017)  
**City:** Portoroz, Slovenia **Data:** 22/06/2017  
**ISBN:** 978-1-138-62937-0
- 11 **Title:** An Extended-BEPU Approach for Safety Analysis on Nuclear Power Plants  
**Authors:** Sanchez Saez, Francisco; Carlos Alberola, Sofía; Martón Lluch, Isabel; Martorell Aigües, Pablo; Villanueva López, José Felipe; Martorell Alsina, Sebastián Salvador  
**Conference:** 11th International Topical Meeting on Nuclear Thermal-Hydraulics, Operation and Safety (NUTHOS-11)  
**City:** Gyeongju, Korea **Data:** 13/10/2016  
**ISBN:** -

- 12 **Title:** Development of advanced surveillance requirements of nuclear power plants using risk information  
**Authors:** Martorell Alsina, Sebastián Salvador; Martón Lluch, Isabel; Martorell Aigües, Pablo; Sánchez Galdón, Ana Isabel; Villanueva López, José Felipe; Carlos Alberola, Sofía; Sánchez Galdón, Ana Isabel; R. Mullor  
**Conference:** 13th International Probabilistic Safety Assessment and Management Conference (PSAM 13)  
**City:** Seoul, South Korea **Data:** 07/10/2016  
**ISBN:** -
- 13 **Title:** A comparison between traditional BEPU and Extended-BEPU approaches for deterministic safety analysis on nuclear power plants  
**Authors:** Sanchez Saez, Francisco; Carlos Alberola, Sofía; Martón Lluch, Isabel; Martorell Aigües, Pablo; Villanueva López, José Felipe; Martorell Alsina, Sebastián Salvador  
**Conference:** European Safety and Reliability Annual Conference (ESREL 2016)  
**City:** Glasgow, UK **Data:** 29/09/2016  
**ISBN:** 978-1-138-02997-2
- 14 **Title:** Availability modelling of ageing equipment addressing multiple items and failure causes  
**Authors:** Martorell Aigües, Pablo; Martón Lluch, Isabel; Carlos Alberola, Sofía; Martorell Alsina, Sebastián Salvador; Sánchez Galdón, Ana Isabel  
**Conference:** European Safety and Reliability Annual Conference (ESREL 2016)  
**City:** Glasgow, UK **Data:** 29/09/2016  
**ISBN:** 978-1-138-02997-2
- 15 **Title:** Development of advanced surveillance requirements of nuclear power plants using a risk-informed approach in the horizon 2020  
**Authors:** Martorell Alsina, Sebastián Salvador; Martón Lluch, Isabel; Martorell Aigües, Pablo; Villanueva López, José Felipe; Carlos Alberola, Sofía; Sánchez Galdón, Ana Isabel; Ruben  
**Conference:** European Safety and Reliability Annual Conference (ESREL 2016)  
**City:** Glasgow, UK **Data:** 29/09/2016  
**ISBN:** 978-1-138-02997-2
- 16 **Title:** RAM based metrics for safety assessment of safety systems with application to ageing management  
**Authors:** Martorell Alsina, Sebastián Salvador; Martón Lluch, Isabel; Martorell Aigües, Pablo; Carlos Alberola, Sofía; Sánchez Galdón, Ana Isabel  
**Conference:** European Safety and Reliability Annual Conference (ESREL 2015)  
**City:** Zürich, Switzerland **Data:** 10/09/2015

**ISBN:** 978-1-138-02879-1

- 17 **Title:** Risk based prioritization and management of relevant ageing components  
**Authors:** Martorell Alsina, Sebastián Salvador; Martón Lluch, Isabel; Martorell Aigües, Pablo; Carlos Alberola, Sofía; Sánchez Galdón, Ana Isabel  
**Conference:** European Safety and Reliability Annual Conference (ESREL 2015)  
**City:** Zürich, Switzerland **Data:** 10/09/2015  
**ISBN:** 978-1-138-02879-1
- 18 **Title:** Effect of human factor in the analysis of changes to Limiting Conditions for Operation (LCO) applied to Residual Heat Removal system  
**Authors:** Martón Lluch, Isabel; Martorell Aigües, Pablo; Martorell Alsina, Sebastián Salvador; Matilde  
**Conference:** European Safety and Reliability Annual Conference (ESREL 2015)  
**City:** Wroclaw, Poland **Data:** 18/09/2014  
**ISBN:** 978-1-138-02681-0

### *7.2.3. Contributions to national conferences*

- 19 **Title:** Modelo de indisponibilidad dependiente del tiempo para fallos en espera y en demanda integrando los efectos positivos y negativos de las pruebas y el mantenimiento  
**Authors:** Martorell Aigües, Pablo; Martón Lluch, Isabel; Sánchez Galdón, Ana Isabel; Martorell Alsina, Sebastián Salvador; Carlos Alberola, Sofía  
**Conference:** 44 Reunión Anual de la Sociedad Nuclear Española  
**City:** Ávila, España **Data:** 28/09/2018  
**ISBN:**
- 20 **Title:** Modelo de fiabilidad de componentes para fallos a la demanda considerando la degradación por pruebas y la efectividad del mantenimiento  
**Authors:** Martón Lluch, Isabel; Martorell Aigües, Pablo; Rubén; Sánchez Galdón, Ana Isabel; Martorell Alsina, Sebastián Salvador  
**Conference:** XIX Congreso de Confiabilidad 2017  
**City:** Alcobendas, España **Data:** 22/11/2017  
**ISBN:** 978-84-697-7913-2
- 21 **Title:** Criterios de optimización en el contexto de los Requisitos de Vigilancia Avanzados  
**Authors:** Martón Lluch, Isabel; Martorell Alsina, Sebastián Salvador; Martorell Aigües, Pablo; Sánchez Galdón, Ana Isabel; Carlos Alberola, Sofía  
**Conference:** 43ª Reunión Anual de la Sociedad Nuclear Española  
**City:** Málaga, España **Data:** 06/10/2017

**ISBN:** 978-84-090-1616-7

- 22 **Title:** Modelo de fiabilidad de componentes para fallos a la demanda considerando la degradación por pruebas y la efectividad del mantenimiento  
**Authors:** Martorell Aigües, Pablo; Martón Lluch, Isabel; Sánchez Galdón, Ana Isabel; Martorell Alsina, Sebastián Salvador; Carlos Alberola, Sofía  
**Conference:** 43ª Reunión Anual de la Sociedad Nuclear Española  
**City:** Málaga, España **Data:** 06/10/2017  
**ISBN:** 978-84-090-1616-7
- 23 **Title:** El factor humano en el ámbito de la seguridad: Herramientas para un correcto modelado  
**Authors:** Martorell Aigües, Pablo; Martón Lluch, Isabel; Sánchez Galdón, Ana Isabel; Martorell Alsina, Sebastián Salvador; Carlos Alberola, Sofía  
**Conference:** XVIII Congreso de Confiabilidad  
**City:** Madrid, España **Data:** 24/11/2016  
**ISBN:** 978-84-617-6643-7
- 24 **Title:** Modelos RAMS avanzados: causas de fallo y modos de fallo  
**Authors:** Martón Lluch, Isabel; Martorell Alsina, Sebastián Salvador; Martorell Aigües, Pablo; Sánchez Galdón, Ana Isabel; Carlos Alberola, Sofía  
**Conference:** XVIII Congreso de Confiabilidad  
**City:** Madrid, España **Data:** 24/11/2016  
**ISBN:** 978-84-617-6643-7
- 25 **Title:** Desarrollo de RV flexibles en la toma de decisiones informada en el riesgo  
**Authors:** Martorell Aigües, Pablo; Martorell Alsina, Sebastián Salvador; Sánchez Galdón, Ana Isabel; Carlos Alberola, Sofía; Mullor, Ruben; Villanueva López, José Felipe; Martón Lluch, Isabel  
**Conference:** 42 Reunión Anual de la Sociedad Nuclear Española  
**City:** Santander, España **Data:** 30/09/2016  
**ISBN:** 978-84-617-4660-6 / 1137-2885
- 26 **Title:** Modelado de la disponibilidad de equipos sometidos a envejecimiento considerando múltiples ítems y causas de fallo  
**Authors:** Martorell Aigües, Pablo; Martón Lluch, Isabel; Martorell Alsina, Sebastián Salvador; Sánchez Galdón, Ana Isabel; Carlos Alberola, Sofía  
**Conference:** 42 Reunión Anual de la Sociedad Nuclear Española  
**City:** Santander, España **Data:** 30/09/2016  
**ISBN:** 978-84-617-4660-6 / 1137-2885
- 27 **Title:** RAMS. Impacto del envejecimiento y la efectividad del mantenimiento

- Authors:** Martorell Aigües, Pablo; Martorell Alsina, Sebastián Salvador; Martón Lluch, Isabel; Sánchez Galdón, Ana Isabel  
**Conference:** XVII Congreso de Confiabilidad  
**City:** Zamudio, España  
**ISBN:** 978-84-608-4059-6  
**Data:** 26/11/2015
- 28 **Title:** Modelado RAM del envejecimiento en sistemas de seguridad considerando mantenimiento imperfecto y eficiencia de las pruebas  
**Authors:** Martorell Aigües, Pablo; Martorell Alsina, Sebastián Salvador; Martón Lluch, Isabel; Sánchez Galdón, Ana Isabel  
**Conference:** 41 Reunión Anual de la Sociedad Nuclear Española  
**City:** A Coruña, España  
**ISBN:** 978-84-608-2453-4 / 1137-2885  
**Data:** 25/09/2015
- 29 **Title:** Priorización de componentes críticos y gestión de su envejecimiento  
**Authors:** Martorell Aigües, Pablo; Martorell Alsina, Sebastián Salvador; Martón Lluch, Isabel; Sánchez Galdón, Ana Isabel  
**Conference:** 41 Reunión Anual de la Sociedad Nuclear Española  
**City:** A Coruña, España  
**ISBN:** 978-84-608-2453-4 / 1137-2885  
**Data:** 25/09/2015
- 30 **Title:** Influencia de la fiabilidad humana en la evaluación del impacto en el riesgo de cambios de CLO  
**Authors:** Martón Lluch, Isabel; Martorell Aigües, Pablo; Martorell Alsina, Sebastián Salvador; Matilde  
**Conference:** 40 Reunión Anual de la Sociedad Nuclear Española  
**City:** Valencia  
**ISBN:** 978-84-697-1656  
**Data:** 03/10/2014

# Capítulo 8

## References

- Alvarenga, M. A. B., Frutuoso e Melo, P. F., & Fonseca, R. A. (2014). A critical review of methods and models for evaluating organizational factors in Human Reliability Analysis. *Progress in Nuclear Energy*, 75, 25-41.
- Apostolakis, G., Cunningham, M., Lui, C., Pangburn, G., & Reckley, W. (2012). *A Proposed Risk Management Regulatory Framework (NUREG-2150)*. Washington, DC: US Nuclear Regulatory Commission.
- ASME. (2000). *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications*. New York, NY: The American Society of Mechanical Engineers.
- Atwood, C., Cronval, O., Patrik, M., & Rodionov, A. (2007). *Models and data used for assessing the ageing of systems, structures and components*. Petten.
- Barriere, M., Bley, D., Cooper, S., Forester, J., Kolaczowski, A., Luckas, W., ... Whitehead, D. (2000). *Technical basis and implementation guidelines for a technique for human event analysis (ATHEANA) (NUREG-1624)*. Washington, DC: US Nuclear Regulatory Commission.
- Bell, J., & Holroyd, J. (2009). *Review of human reliability assessment methods*. Health and Safety Laboratory, United Kingdom.
- Borysiewicz, M., Kowal, K., & Potemski, S. (2015). An application of the value tree analysis methodology within the integrated risk informed decision making for the nuclear facilities. *Reliability Engineering & System Safety*, 139, 113-119.
- Caballé, N. C., Castro, I. T., Pérez, C. J., & Lanza-Gutiérrez, J. M. (2015). A condition-based maintenance of a dependent degradation-threshold-shock model in a system with multiple degradation processes. *Reliability Engineering & System Safety*, 134, 98-109.

- Cadini, F., & Gioietta, A. (2016). A Bayesian Monte Carlo-based algorithm for the estimation of small failure probabilities of systems affected by uncertainties. *Reliability Engineering & System Safety*, 153, 15-27.
- Caruso, M. A., Cheok, M. C., Cunningham, M. A., Holahan, G. M., King, T. L., Parry, G. W., ... Thadani, A. C. (1999). An approach for using risk assessment in risk-informed decisions on plant-specific changes to the licensing basis. *Reliability Engineering & System Safety*, 63(3), 231-242.
- Chelson, P. O. (1971). *Reliability computation using fault tree analysis*. Technical Report NAS 7-10. NASA.
- Cheng CY, L. C. (2005). Statistical estimation on imperfectly maintained system. Advances in safety and reliability. En *Proceedings of the European Safety and Reliability Conference, ESREL 2005* (pp. 351-356). Tri City (Gdynia-Sopot-Gdansk).
- Choi, S. Y., Lee, J., & Yang, J.-E. (2010). An analysis for risk impact of Emergency Diesel Generator on modified Surveillance Test Interval by considering failure due to demand stress. *Nuclear Engineering and Design*, 240(10), 3577-3581.
- CSN. (1986). *Programa Integrado de Realización y Utilización de los APS en España*. Madrid: Consejo de Seguridad Nuclear.
- CSN. (2007a). *GS 1.14 (Rev. 1). Criterios básicos para la realización de aplicaciones de los Análisis Probabilistas de Seguridad*. Madrid: Consejo de Seguridad Nuclear.
- CSN. (2007b). *Instrucción IS-15, sobre Requisitos para la vigilancia de la eficacia del mantenimiento en centrales nucleares*. Madrid: Consejo de Seguridad Nuclear.
- CSN. (2010a). *Instrucción IS-25, sobre criterios y requisitos sobre la realización de los análisis probabilistas de seguridad y sus aplicaciones a las centrales nucleares*. Madrid: Consejo de Seguridad Nuclear.
- CSN. (2010b). *Instrucción IS-26, sobre requisitos básicos de seguridad nuclear aplicables a las instalaciones nucleares*. Madrid: Consejo de Seguridad Nuclear.
- CSN. (2011). *Instrucción IS-32, sobre Especificaciones Técnicas de Funcionamiento de centrales nucleares*. Madrid: Consejo de Seguridad Nuclear.
- CSN. (2016a). *Guía de Seguridad 1.18 (Rev. 1) Medida de la eficacia del mantenimiento en centrales nucleares*. Madrid: Consejo de Seguridad Nuclear.
- CSN. (2016b). *Plan de I+D del CSN 2016-2020*. Madrid: Consejo de Seguridad Nuclear.
- CSN. (2017a). *GS 1.10 (Rev. 2). Revisiones periódicas de la seguridad de las centrales nucleares*. Madrid: Consejo de Seguridad Nuclear.
- CSN. (2017b). *GS 1.15 (Rev. 1) Actualización y mantenimiento de los Análisis Probabilistas de Seguridad*. Madrid: Consejo de Seguridad Nuclear.
- De Felice, F., & Petrillo, A. (2018). An Overview on Human Error Analysis and Reliability Assessment. En F. De Felice & A. Petrillo (Eds.), *Human Factors and Reliability*



- 
- Engineering for Safety and Security in Critical Infrastructures: Decision Making, Theory, and Practice* (pp. 19-41). Cham: Springer International Publishing.
- Di Maio, F., Rai, A., & Zio, E. (2016). A dynamic probabilistic safety margin characterization approach in support of Integrated Deterministic and Probabilistic Safety Analysis. *Reliability Engineering & System Safety*, 145, 9-18.
- Di Pasquale, V., Iannone, R., Miranda, S., & Riemma, S. (2013). An Overview of Human Reliability Analysis Techniques in Manufacturing Operations. *Operations Management*, 221-240.
- Dougherty, E. M., & Fragola, J. R. (1988). Foundations for a time reliability correlation system to quantify human reliability. En *Conference Record for 1988 IEEE Fourth Conference on Human Factors and Power Plants*, (pp. 268-278). Monterey.
- Drouin, M., Parry, G., Lehner, J., Martinez-Guridi, G., LaChance, J., & Wheeler, T. (2009). *Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making — Main Report (NUREG-1855)*. Washington, DC: US Nuclear Regulatory Commission.
- Embrey, D., Humphreys, P., Rosa, E. A., Kirwan, B., & Rea, K. (1984). *SLIM-MAUD: an approach to assessing human error probabilities using structured expert judgment. Volume I. Overview of SLIM-MAUD*. Brookhaven National Lab., Upton, NY.
- EPRI. (2012). *Practical Guidance on the Use of PRA in Risk-Informed Applications with a Focus on the Treatment of Uncertainty. EPRI-1026511, Draft Report*. San Diego, CA: Electric Power Research Institute.
- European Commission. (2013). *Innovation, Council Regulation (Euratom) No 1314/2013 of 16 December 2013 on the Research and Training Programme of the European Atomic Energy Community (2014-2018) complementing the Horizon 2020 Framework Programme for Research and Innovation (2014-2)*. Brussels.
- European Commission. (2015). *Euratom Work Programme 2016 - 2017*. Brussels.
- European Commission. (2017a). Directiva 2014/87/Euratom del Consejo, de 8 de julio de 2014, por la que se modifica la Directiva 2009/71/Euratom, por la que se establece un marco comunitario para la seguridad nuclear de las instalaciones nucleares. Brussels.
- European Commission. (2017b). *Euratom Work Programme 2018*. Brussels.
- Gertman, D., Blackman, H., Marble, J., Byers, J., & Smith, C. (2005). *The SPAR-H human reliability analysis method (NUREG/CR-6883)*. Washington, DC: US Nuclear Regulatory Commission.
- Guure, C. B., & Ibrahim, N. A. (2012). Bayesian Analysis of the Survival Function and Failure Rate of Weibull Distribution with Censored Data. *Mathematical Problems in Engineering*, 2012, 18.
- Guure, C. B., Ibrahim, N. A., & Ahmed, A. O. M. (2012). Bayesian Estimation of Two-Parameter Weibull Distribution Using Extension of Jeffreys' Prior Information with

- Three Loss Functions. *Mathematical Problems in Engineering*, 2012, 13.
- Hall, R. E., Fragola, J., & Wreathall, J. (1982). *Post-event human decision errors: operator action tree/time reliability correlation (NUREG/CR-3010)*. Washington, DC: US Nuclear Regulatory Commission.
- Hannaman, G. W., & Spurgin, A. J. (1984). *Systematic Human Action Reliability Procedure Electric Power*. EPRI NP-3583. San Diego, CA: Electric Power Research Institute.
- Hess, S. M. (2009). Risk managed technical specifications. *Progress in Nuclear Energy*, 51(3), 393-400.
- Hollnagel, E. (1998). *Cognitive reliability and error analysis method (CREAM)*. Elsevier.
- IAEA. (1992). *Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1)*. IAEA-TECDOC-1267 (IAEA Safety Series). Vienna: International Atomic Energy Agency.
- IAEA. (1993). *Risk Based Optimization of Technical Specifications for Operation of Nuclear Power Plants*. IAEA-TECDOC-729. Vienna: International Atomic Energy Agency.
- IAEA. (2005). *Risk-informed regulation of nuclear facilities: overview of the current status*. IAEA-TECDOC-1436. Vienna: International Atomic Energy Agency.
- IAEA. (2010a). *Deterministic Safety Analysis for Nuclear Power Plants*. IAEA Safety Standards Series No. SSG-2. Vienna: International Atomic Energy Agency.
- IAEA. (2010b). *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants*. IAEA Safety Standards Series No. SSG-3. Vienna: International Atomic Energy Agency.
- IAEA. (2011). *A Framework for Integrated Risk-Informed Decision Making Process*. INSAG-25. Vienna: International Atomic Energy Agency.
- IAEA. (2014). *Regulatory Practices on Ageing Management and Long Term Operation of Nuclear Power Plants in the Ibero-American Region*. Vienna: International Atomic Energy Agency.
- IAEA. (2016). *Safety of Nuclear Power Plants: Design*. IAEA Safety Standards Series No. SSR-2/1 (Rev. 1). Vienna: International Atomic Energy Agency.
- Ibáñez, L., Hortal, J., Queral, C., Gómez-Magán, J., Sánchez-Perea, M., Fernández, I., ... Villalba-Jabonero, E. (2016). Application of the Integrated Safety Assessment methodology to safety margins. Dynamic Event Trees, Damage Domains and Risk Assessment. *Reliability Engineering & System Safety*, 147, 170-193.
- IEC. (2015). *IEC 60050 192, International electrotechnical vocabulary — Part 192: Dependability*.
- Kančev, D., & Čepin, M. (2011). Evaluation of risk and cost using an age-dependent unavailability modelling of test and maintenance for standby components. *Journal of Loss Prevention in the Process Industries*, 24(2), 146-155.

- 
- Kančev, D., & Čepin, M. (2012). Uncertainty and sensitivity analyses for age-dependent unavailability model integrating test and maintenance. *Nuclear Engineering and Design*, 246, 128-135.
- Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis*, 1(1), 11-27.
- Karanki, D. R., Rahman, S., Dang, V. N., & Zerkak, O. (2017). Epistemic and aleatory uncertainties in integrated deterministic and probabilistic safety assessment: Tradeoff between accuracy and accident simulations. *Reliability Engineering & System Safety*, 162, 91-102.
- Keller, W., & Modarres, M. (2005a). A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late Professor Norman Carl Rasmussen. *Reliability Engineering & System Safety*, 89(3), 271-285.
- Keller, W., & Modarres, M. (2005b). A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late Professor Norman Carl Rasmussen. *Reliability Engineering & System Safety*, 89(3), 271-285.
- Kim, I. S., Martorell, S. A., Vesely, W. E., & Samanta, P. K. (1994). Risk analysis of surveillance requirements including their adverse effects. *Reliability Engineering & System Safety*, 45(3), 225-234.
- Kim, I. S., Samanta, P. K., Martorell, S., & Vesely, W. E. (1992). *Quantitative evaluation of surveillance test intervals including test-caused risks (NUREG/CR-5775)*. Washington, DC: US Nuclear Regulatory Commission.
- Kolaczkwshi, A., Forester, J., Lois, E., & Cooper, S. (2005). *Good Practices for Implementing Human Reliability Analysis (HRA) (NUREG-1792)*. Washington, DC: US Nuclear Regulatory Commission.
- Kolaczkwshi, A., Forester, J., Lois, E., & Cooper, S. (2006). *Evaluation of Human Reliability Analysis Methods Against Good Practices (NUREG-1842)*. Washington, DC: US Nuclear Regulatory Commission.
- Kumamoto, H., & Henley, E. J. (1996). *Probabilistic risk assessment and management for engineers and scientists* (2nd ed.). New York : IEEE Press.
- Lagarias, J. C., Reeds, J. A., Wright, M. H., & Wright, P. E. (1998). Convergence properties of the Nelder-Mead simplex method in low dimensions. *SIAM Journal on Optimization*, 9(1).
- Lee, D. D., Lim, H.-G., Yoon, H. Y., & Jeong, J. J. (2014). Improvement of the LOCA PSA model using a best-estimate thermal-hydraulic analysis. *Nuclear Engineering and Technology*, 46(4), 541-546.
- Martón, I. (2014). *Gestión de la operación, vigilancia y mantenimiento de equipos de seguridad de centrales nucleares a corto y largo plazo*. Tesis doctoral. Universitat Politècnica de València, Valencia.

- Martón, I., Martorell, P., Mullor, R., Sánchez, A. I., & Martorell, S. (2016). Optimization of test and maintenance of ageing components consisting of multiple items and addressing effectiveness. *Reliability Engineering & System Safety*, *153*, 151-158.
- Martón, I., Sánchez, A. I., & Martorell, S. (2015). Ageing PSA incorporating effectiveness of maintenance and testing. *Reliability Engineering & System Safety*, *139*, 131-140.
- Martorell, P., Martón, I., Sánchez, A. I., & Martorell, S. (2017). Unavailability model for demand-caused failures of safety components addressing degradation by demand-induced stress, maintenance effectiveness and test efficiency. *Reliability Engineering & System Safety*.
- Martorell, P., Martón, I., Sánchez, A. I., Martorell, S., Sanchez-Saez, F., & Saiz, M. (2018). Evaluation of risk impact of completion time changes combining PSA and DSA model insight and human reliability analysis. *Reliability Engineering & System Safety*, *178*, 97-107.
- Martorell, S., Martón, I., Villamizar, M., Sánchez, A. I., & Carlos, S. (2014). Evaluation of risk impact of changes to Completion Times addressing model and parameter uncertainties. *Reliability Engineering & System Safety*, *130*, 190-201.
- Martorell, S., Martorell, P., Sanchez, A. I., Mullor, R., & Martón, I. (2017). Parameter estimation of a reliability model of demand-caused and stand-by related failures of safety components exposed to degradation by demand stress and ageing that undergo imperfect maintenance. *Mathematical Problems in Engineering*, *2017*, 11.
- Martorell, S., Sánchez-Sáez, F., Villanueva, J. F., & Carlos, S. (2017). An extended BEPU approach integrating probabilistic assumptions on the availability of safety systems in deterministic safety analyses. *Reliability Engineering & System Safety*, *167*, 474-483.
- Martorell, S., Sanchez, A., & Serradell, V. (1999). Age-dependent reliability model considering effects of maintenance and working conditions. *Reliability Engineering & System Safety*, *64*(1), 19-31.
- Martorell, S., Villamizar, M., Martón, I., Villanueva, J. F., Carlos, S., & Sánchez, A. I. (2014). Evaluation of risk impact of changes to surveillance requirements addressing model and parameter uncertainties. *Reliability Engineering & System Safety*, *126*, 153-165.
- Michalewicz, Z., & Fogel, D. B. (2004). *How to Solve It: Modern Heuristics*. Berlin, Heidelberg: Springer Berlin Heidelberg.
- Modarres, M. (2008). Probabilistic Risk Assessment. En K. B. Misra (Ed.), *Handbook of Performability Engineering* (pp. 699-718). London: Springer London.
- Mullor, R. (2006). Parameters estimation under preventive imperfect maintenance. En *Proceedings of the European Safety and Reliability Conference, ESREL 2006*. Estoril.
- Nelder, J. A., & Mead, R. (1965). A Simplex Method for Function Minimization. *The Computer Journal*, *7*(4), 308-313.

- 
- Nitoi, M., & Rodionov, A. (2012). Ageing probabilistic safety assessment network – Recent developments. *Progress in Nuclear Energy*, 56, 71-78.
- Nourbakhsh, H. P., Apostolakis, G., & Powers, D. A. (2018). The evolution of the U.S. nuclear regulatory process. *Progress in Nuclear Energy*, 102, 79-89.
- Nuclear Energy Agency. (1998). *Critical operator actions: human reliability modeling and data issues Principal Working Group No 5 - Task 94-1 Final Task Report prepared by a Group of Experts of the NEA Committee on the Safety of Nuclear Installations*. Nuclear Energy Agency of the OECD (NEA).
- Nuclear Energy Agency. (2005). *Nuclear regulatory decision making*. Nuclear Energy Agency of the OECD (NEA).
- Nuclear Energy Institute. (2000). *Nuclear Energy Institute Industry Guideline for Monitoring the Effectiveness of Maintenance at NPPs. NUMARC 93-01, Revision 4A (Vol. 3)*. Washington, DC: US Nuclear Regulatory Commission.
- Nuclear Energy Institute. (2007). *Risk-Informed Technical Specifications Initiative 5b Risk-Informed Method for Control of Surveillance Frequencies Industry Guidance Document. NEI 04-10, Revision 1*. Washington, DC: US Nuclear Regulatory Commission.
- Prasad, M., & Gaikwad, A. J. (2015). Human error probability estimation by coupling simulator data and deterministic analysis. *Progress in Nuclear Energy*, 81, 22-29.
- Prošek, A., & Čepin, M. (2008). Success criteria time windows of operator actions using RELAP5/MOD3.3 within human reliability analysis. *Journal of Loss Prevention in the Process Industries*, 21(3), 260-267.
- Rasmussen, J. (1983). Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models. *IEEE Transactions on Systems, Man, and Cybernetics*, SMC-13(3), 257-266.
- Samanta, P. K., Kim, I. S., Mankamo, T., & Vesely, W. E. (1994). *Handbook of methods for risk-based analyses of technical specifications (NUREG/CR-6141)*. Washington, DC: US Nuclear Regulatory Commission.
- Sanchez, A., Carlos, S., Martorell, S., & Villanueva, J. F. (2009). Addressing imperfect maintenance modelling uncertainty in unavailability and cost based optimization. *Reliability Engineering & System Safety*, 94(1), 22-32.
- Sanchez, A. I. (2000). *Metodología de optimización conjunta y multi-criterio de requisitos de vigilancia y condiciones de mantenimiento de componentes de CC.NN*. Tesis Doctoral. Universitat Politècnica de València, Valencia.
- Shin, S. M., Jeon, I. S., & Kang, H. G. (2015). Surveillance test and monitoring strategy for the availability improvement of standby equipment using age-dependent model. *Reliability Engineering & System Safety*, 135, 100-106.
- Swain, A. D. (1987). *Accident Sequence Evaluation Program: Human reliability analysis*

- procedure*. Washington, DC: US Nuclear Regulatory Commission.
- Swain, A. D., & Guttman, H. E. (1983). *Handbook of human-reliability analysis with emphasis on nuclear power plant applications (NUREG/CR-1278), Final report*. Washington, DC: US Nuclear Regulatory Commission.
- Torres-Echeverría, A. C., Martorell, S., & Thompson, H. A. (2009). Modelling and optimization of proof testing policies for safety instrumented systems. *Reliability Engineering & System Safety*, 94(4), 838-854.
- Torres-Echeverría, A. C., Martorell, S., & Thompson, H. A. (2011). Modeling safety instrumented systems with Moon voting architectures addressing system reconfiguration for testing. *Reliability Engineering & System Safety*, 96(5), 545-563.
- USNRC. (1975). *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants [NUREG-75/014 (WASH-1400)]*. Washington, DC: US Nuclear Regulatory Commission.
- USNRC. (1990). *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants (NUREG-1150)*. Washington, DC: US Nuclear Regulatory Commission.
- USNRC. (1991a). *NRC- 10 CFR 50.65: requirements for monitoring the effectiveness of maintenance at nuclear power plants*. Washington, DC: US Nuclear Regulatory Commission.
- USNRC. (1991b). *Nuclear Plant Aging Research (NPAR) program plan*. Washington, DC: US Nuclear Regulatory Commission.
- USNRC. (1994). *Guidance for the Review of Changes to Human Actions (NUREG-1764)*. Washington, DC: US Nuclear Regulatory Commission.
- USNRC. (1995a). *10 CFR Part 54—Requirements for Renewal of Operating Licenses for Nuclear Power Plants*. Washington, DC: US Nuclear Regulatory Commission.
- USNRC. (1995b). Use of probabilistic risk assessment methods in nuclear activities: Final policy statement. *Federal Register*, 60, 42622.
- USNRC. (1998a). *Regulatory Guide 1.174. An Approach for Using Probabilistic Risk Assessment in Risk Informed Decisions on Plant-Specific Changes to the Licensing Basis*. Washington, DC: US Nuclear Regulatory Commission.
- USNRC. (1998b). *Regulatory Guide 1.175. An Approach for Plant-Specific, Risk-Informed Decision-Making: Inservice Testing*. Washington, DC: US Nuclear Regulatory Commission.
- USNRC. (1998c). *Regulatory Guide 1.177. An Approach for Plant-Specific, Risk-Informed Decision-Making: Technical Specifications*. Washington, DC: US Nuclear Regulatory Commission.
- USNRC. (1998d). *Regulatory Guide 1.178. An Approach for Plant-Specific, Risk-Informed Decision-Making: Inservice Inspection of Piping*. Washington, DC: US Nuclear Regulatory Commission.

- 
- USNRC. (2006). "Staff Requirements—Meeting with Advisory Committee on Reactor Safeguards," SRM M061020.
- USNRC. (2009). *Regulatory Guide 1.200. An approach for determining the technical adequacy of probabilistic risk assessment results for risk-informed activities, Revision 2*. Washington, DC: US Nuclear Regulatory Commission.
- USNRC. (2011). *Regulatory Guide 1.177. An approach for plant-specific, risk-informed decision making: technical specifications, Revision 1*. Washington, DC: US Nuclear Regulatory Commission.
- USNRC. (2014). *TRACE V5.840 User's and Theory manuals*. Washington, DC: US Nuclear Regulatory Commission.
- USNRC. (2018). *Regulatory Guide 1.160. Monitoring the Effectiveness of Maintenance at Nuclear Power Plants, Revision 4*. Washington, DC: US Nuclear Regulatory Commission.
- Vaurio, J. K. (2009). Human factors, human reliability and risk assessment in license renewal of a nuclear power plant. *Reliability Engineering & System Safety*, 94(11), 1818-1826.
- Vesely, W. E., Kurth, R. E., & Scalzo, S. M. (1990). *Evaluations of core melt frequency effects due to component aging and maintenance (NUREG/CR-5510)*. Washington, DC: US Nuclear Regulatory Commission.
- Vesely, W. E., & Wolford, A. J. (1988). Risk evaluations of aging phenomena: The linear aging reliability model and its extensions. *Nuclear Engineering and Design*, 108(1-2), 179-185.
- Volkanovski, A. (2012). Method for assessment of ageing based on PSA results. *Nuclear Engineering and Design*, 246, 141-146.
- Voronov, R., & Alzbutas, R. (2011). Probabilistic analysis of operators actions at the Ignalina nuclear power plant taking account of the specific conditions of accident sequences. *Atomic Energy*, 110(5), 297.
- Whaley, A., Xing, J., Boring, R. L., Hendrickson, S. M. L., Joe, J. C., Le Blanc, K. L., & Morrow, S. L. (2016). *Cognitive Basis for Human Reliability Analysis (NUREG-2114)*. Washington, DC: US Nuclear Regulatory Commission.
- Wilson, G. E. (2013). Historical insights in the development of Best Estimate Plus Uncertainty safety analysis. *Annals of Nuclear Energy*, 52, 2-9.
- Wolford, A. J., Atwood, C. L., & Roesener, W. S. (1992). *Aging data analysis and risk assessment: Development and demonstration study*. Washington, DC: US Nuclear Regulatory Commission.
- Xing, J., & Chang, Y. J. (2016). *The General Methodology of an Integrated Human Event Analysis System (IDHEAS)*. Washington, DC: US Nuclear Regulatory Commission.
- Xing, J., Parry, G., Presley, M., Forester, J., Hendrickson, S., & Dang, V. (2017). *An Integrated Human Event Analysis System (IDHEAS) for Nuclear Power Plant Internal*

*Events At-Power Application (NUREG-2199), vol. 1.* Washington, DC: US Nuclear Regulatory Commission.

Yang, L., Ma, X., Peng, R., Zhai, Q., & Zhao, Y. (2017). A preventive maintenance policy based on dependent two-stage deterioration and external shocks. *Reliability Engineering & System Safety*, *160*, 201-211.

Zhang, J., Huang, X., Fang, Y., Zhou, J., Zhang, H., & Li, J. (2016). Optimal inspection-based preventive maintenance policy for three-state mechanical components under competing failure modes. *Reliability Engineering & System Safety*, *152*, 95-103.

Zio, E., & Pedroni, N. (2012). *Overview of risk-informed decision-making processes.* FonCSI.