Mecánica Computacional Vol. XXII
M. B. Rosales, V. H. Cortínez y D. V. Bambill (Editores)
Bahía Blanca, Argentina, Noviembre 2003.

MODELOS DE MARKOV: ANÁLISIS DE REPARACIONES IMPERFECTAS EN SISTEMAS DE CONTROL PARA SEGURIDAD

Roberto A. Castellano y Mabel C. Sánchez

Planta Piloto de Ingeniería Química (UNS – CONICET)
Camino La Carrindanga km 7, B8000CPB Bahía Blanca, Argentina.
TE: 54-(0291)-4861700–Interno 249, FAX: 54-(0291) 4861600
e-mail: msanchez@plapiqui.edu.ar, web page: http://www.plapiqui.edu.ar/

Palabras clave: Modelos de Markov, Seguridad, Aplicaciones Industriales.

Resumen. *En este trabajo se presenta una metodología para calcular la Probabilidad de Falla ante la Demanda promedio en el último intervalo operativo de la vida útil de los Sistemas Instrumentados de Seguridad (SIS), cuando las tareas de inspección y reparación son imperfectas. Se utilizan Modelos de Markov continuos para evaluar la probabilidad de los estados del sistema entre intervalos de inspección, mientras que se emplea una cadena de Markov discreta para calcular esta probabilidad inmediatamente después de la inspección periódica. La estrategia involucra el cálculo de la exponencial de la matriz de velocidades de transición del modelo de Markov y submatrices de ella. Se fundamenta la selección de la estrategia de cálculo utilizada en función de su aplicación en el contexto del diseño óptimo de SIS. Se incluyen ejemplos de aplicación para la arquitectura 1oo2.*

1 INTRODUCCIÓN

Los avances tecnológicos experimentados por la industria química en los últimos treinta años han originado la aparición de nuevos materiales, procesos y productos químicos. Las plantas se operan frecuentemente en condiciones extremas de presión y temperatura, siendo más vulnerables a la falla de equipos. En este marco operativo complejo, la utilización de Sistemas de Instrumentación para Seguridad (SIS – Safety Instrumented Systems) constituye una alternativa eficaz para la reducción del riesgo a niveles tolerables, evitando pérdidas económicas y humanas. Estos sistemas efectúan cálculos lógicos, utilizando las mediciones del proceso, con el fin de identificar situaciones peligrosas; en caso que resulte necesario actúan sobre los elementos finales (válvulas de control, elementos de corte de emergencia, etc.) para mitigar el riesgo.

Recientemente han aparecido regulaciones internacionales específicas para los SIS. La International Society of Measurement and Control (ISA) redactó el Standard S84.01-1996[1] en Estados Unidos de América, mientras que en Europa, la International Electrotechnical Comission preparó los estándares IEC61508[2] (2000) e IEC61511[3] (2003); este último es la versión para la industria de procesos del código IEC61508.

Los estándares establecen Niveles Seguros de Integridad (SIL – Safety Integrated Level) discretos para las Funciones de Seguridad (SIF – Safety Instrumented Functions) de los SIS. Estos niveles están asociados a un rango de probabilidad de falla ante la demanda (PFD). Además debe comprobarse la satisfaccción del SIL seleccionado considerando la fracción de falla segura y el factor de tolerancia a las fallas de sus componentes físicos.

Según lo indicado por estas reglamentaciones, las empresas son responsables de especificar y documentar el SIL de sus sistemas de protección; además las posteriores etapas de diseño, operación y mantenimiento deben satisfacer el SIL seleccionado. Sin embargo los estándares no aportan recomendaciones específicas para estas etapas. Por lo tanto los diseñadores se enfrentan con la tarea de evaluar diseños alternativos, que cumplan las especificaciones de una manera práctica y económica. En tal sentido han aparecido trabajos que discuten la aplicabilidad de estrategias cualitativas y cuantitativas para evaluar el SIL apropiado para un proceso químico[4,5] y metodologías de diseño. Algunas son de tipo semiempíricas, tales como las de Dowell y Green[6] y Ford y Summers[7,8], otras han incursionado en el diseño óptimo en el ciclo de vida del SIS.

Martorell y co.[9] y Giuggioli y co.[10] optimizaron el intervalo entre inspecciones para arquitecturas y componentes fijos, considerando como criterios de optimización el costo y la disponibilidad. Recientemente Noya y co.[11] formularon el problema de diseño como uno de optimización combinatorial, cuya función objetivo es el costo en el ciclo de vida del SIS y sus restricciones son el SIL y la probabilidad de falla segura. Las variables de optimización son la arquitectura de los subsistemas que componen el SIS y el intervalo entre inspecciones. Los mismos autores[12] extendieron el diseño anterior para incorporar configuraciones con componentes físicos diversos y propusieron una estrategia evolutiva basada en Algoritmos Genéticos para su resolución.

Los trabajos sobre diseño óptimo previos consideran que las inspecciones y reparaciones son perfectas. Sin embargo existe cierta probabilidad que estas tareas sean imperfectas como consecuencia del factor humano. Esto incrementa la PFD del SIS, la cual resulta mayor a medida que se hacen más inspecciones en el ciclo de vida de los componentes.

En este trabajo, se presenta una metodología para calcular la PFD promedio en el último intervalo operativo de la vida útil de los SIS cuando las inspecciones son imperfectas. Se utilizan Modelos de Markov continuos para evaluar la probabilidad de los estados del subsistema entre intervalos de inspección, mientras que se aplica un modelo de Markov discreto para calcular la probabilidad de estos estados inmediatamente después de la inspección periódica. Esta estrategia se ha incorporado como restricción del problema de optimización formulado para el diseño óptimo de SISs.

Esta presentación se organiza de la siguiente manera: las Secciones 2 y 3 contienen los conceptos básicos relacionados con los SIS y la representación de sus estados con Modelos de Markov, respectivamente. La Sección 4 describe la metodología de cálculo de la PFD promedio para el último intervalo de la vida útil del SIS, mientras que en la Sección 5 se hace referencia a las alternativas analizadas en el cálculo de la exponencial de una matriz. La Sección 6 contiene un ejemplo de aplicación y la Sección 7 incluye las conclusiones.

2 SISTEMAS INSTRUMENTADOS DE SEGURIDAD

El estudio de Análisis de Riesgo de un proceso permite establecer la severidad y la probabilidad de ocurrencia de eventos riesgosos. Si las barreras de protección existentes resultan insuficientes para prevenir un peligro, entonces se considera la instalación de un SIS. Este es un sistema de control formado por sensores, uno o más controladores y elementos de acción final, esquematizado en la Figura 1. El propósito de un SIS es monitorear un proceso industrial con el fin de detectar condiciones potencialmente peligrosas y ejecutar acciones preprogramadas para prevenir o mitigar eventos peligrosos.

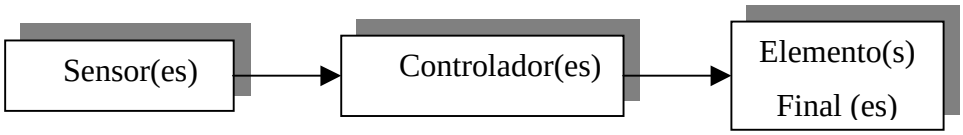

Figura 1: Esquema de un SIS

El SIS reduce el riesgo si opera exitosamente en respuesta a una demanda del proceso. El desempeño en seguridad de los sistemas de protección se caracteriza por su índice SIL. Mayores valores del SIL indican mayores requisitos de seguridad, puesto que cada índice tiene asociado un rango de disponibilidad de la SIF que incrementa con el SIL ó a la inversa, un rango de PFD que disminuye con el aumento del SIL, tal como indica la Tabla 1^2 para sistemas con baja demanda.

Tabla 1: Relación entre el índice SIL y medidas de desempeño del SIS

SIL	PFD	Disponibilidad
1	1.e-2 - 1.e-1	90.00% - 99.00%
2	1.e-3 - 1.e-2	99.00% - 99.90%
3	1.e-4 - 1.e-3	99.90% - 99.99%
4	1.e-5 - 1.e-4	> 99.99%

La PFD del SIS se calcula en función de las PFD de los subsistemas que lo componen. Si éstos funcionan independientemente, resulta la siguiente fórmula

$$PFD_{SIS} = \Sigma PFD_S + \Sigma PFD_C + \Sigma PFD_{EF} \quad (1)$$

La PFD de cada subsistema del SIS depende principalmente de su arquitectura ó arreglo de sus componentes físicos, de la velocidad de falla de estos componentes y del intervalo entre inspecciones. Una revisión de las arquitecturas utilizadas para los controladores se presenta en el libro de Goble[13] y algunas de ellas son empleadas también para los sensores y elementos de acción final.

2.1 Modos de falla del subsistema

Se consideran dos modos de falla: peligroso (D) y seguro (S). Si el subsistema falla en forma peligrosa, no está disponible para responder ante una demanda del proceso. En cambio, si lo hace en forma segura, el proceso se interrumpe, quedando en un estado seguro aunque no existió una condición potencialmente peligrosa.

Algunos subsistemas del SIS tienen capacidad de diagnóstico en línea, lo que les permite detectar la presencia de fallas antes de la inspección periódica. En consecuencia pueden fallar en forma detectada (D) o no detectada (U).

Por otra parte, si existen elementos redundantes o diversos, los modos de falla anteriores pueden originarse por una causa común. Si éste efecto no se considera, resultan evaluaciones de confiabilidad y seguridad optimistas.

2.2 Velocidad de falla de un componente

La velocidad de falla total de un componente del subsistema, λ, se asume igual a la suma de la falla peligrosa y segura como sigue:

$$\lambda = \lambda^D + \lambda^S \quad (2)$$

El Factor de Covertura C mide la proporción de las fallas que son detectadas. En consecuencia λ^D y λ^S se dividen en sus porciones detectadas y no detectadas, teniendo en cuenta el Factor de de Covertura de las fallas peligrosas, C^D, y seguras, C^S, respectivamente, obteniéndose las siguientes fórmulas:

$$\lambda^{DD} = C^D \lambda^D \quad (3)$$

$$\lambda^{DU} = (1 - C^{D})\,\lambda^{D} \tag{4}$$

$$\lambda^{SD} = C^{S}\,\lambda^{S} \tag{5}$$

$$\lambda^{SU} = (1 - C^{S})\,\lambda^{S} \tag{6}$$

representado λ^{DD} y λ^{SD} las fallas peligrosas y seguras detectadas, mientras que λ^{DU} y λ^{SU} indican las fallas peligrosas y seguras no detectadas.

A fin de considerar las fallas por causa común se utiliza el Modelo Beta, que consiste en establecer la proporción de la falla total asignable a una causa común. Para evaluar el efecto del diagnóstico en línea y la falla por causa común, las cuatro velocidades de falla λ^{DD}, λ^{SD}, λ^{DU}, λ^{SU} se dividen usando el factor Beta y se obtienen las ocho categorías de fallas presentadas en la Tabla 2.

Tabla 2: Tipos de Falla de un Componente

Tipo de Falla	Forma de Cálculo
Peligrosa Detectada Normal	$\lambda^{DDN} = (1-\beta)\,\lambda^{DD}$
Peligrosa Detectada Causa Común	$\lambda^{DDC} = \beta\ \lambda^{DD}$
Segura Detectada Normal	$\lambda^{SDN} = (1-\beta)\,\lambda^{SD}$
Segura Detectada Causa Común	$\lambda^{SDC} = \beta\,\lambda^{SD}$
Peligrosa No Detectada Normal	$\lambda^{DUN} = (1-\beta)\,\lambda^{DU}$
Peligrosa No Detectada Causa Común	$\lambda^{DUC} = \beta\ \lambda^{DU}$
Segura No Detectada Normal	$\lambda^{SUN} = (1-\beta)\,\lambda^{SU}$
Segura No Detectada Causa Común	$\lambda^{SUC} = \beta\,\lambda^{SU}$

3 MODELOS DE MARKOV

Los modelos de Markov se aplican a procesos en los cuales la probabilidad de moverse desde un estado o condición a otro depende sólo del estado actual y no de los previos. El proceso se modela definiendo los estados mutuamente excluyentes en los cuales puede encontrarse el subsistema y las transiciones entre ellos. Son una técnica de modelado de gran flexibilidad para la evaluación de los sistemas de control.

Los subsistemas del SIS pueden encontrarse en el estado de operación exitosa, de operación degradada ó de falla durante el intervalo entre inspecciones. Los estados degradados son aquellos en los cuales el sistema opera exitósamente, pero es más vulnerable a la falla. Dependiendo de su arquitectura, se analizan los estados posibles y se esquematiza el diagrama de Markov correspondiente. Este consta de un conjunto de círculos y arcos. Los círculos rotulados representan estados mutuamente excluyentes de éxito ó falla. El sistema efectúa una

transición de un estado a otro cuando ocurre una falla o una reparación. Las transiciones entre estados se muestran con arcos, que están rotulados con la probabilidad de falla o reparación. En este trabajo se asume que las probabilidades de transición entre los estados no varían con el tiempo, es decir, las velocidades de falla y reparación son constantes.

En el diagrama de Markov se distinguen dos tipos de estados: transitorios y absorbentes. Estos últimos se producen en sistemas cuyas fallas los conducen a estados, desde los cuales no existe salida mediante reparación durante el período de interés.

El diagrama de Markov correspondiente a una arquitectura 1oo2 para cualquier tiempo entre inspecciones se muestra en la Figura 2. Esta arquitectura está formada por dos componentes cuyas salidas están conectadas en serie a fin de reducir el efecto de las fallas peligrosas. El sistema tiene tres estados de éxito. En el estado 1 ambos componentes operan satisfactoriamente, mientras que en los estados 2 y 3 un componente ha fallado pero el otro puede satisfacer los requerimientos de una demanda. En el estado 2 la falla ha sido detectada en línea e inmediatamente se inicia la reparación. Los estados 4, 5 y 6 son estados de falla y representan la condición de falla segura, peligrosa detectada y peligrosa no detectada respectivamente. Si bien la falla de ambos componentes se asocia a los estados 5 y 6, la correspondiente al estado 6 es la más peligrosa porque no se pone de evidencia hasta el momento de la inspección. En consecuencia el estado 6 es un estado absorbente en el período entre inspecciones. Las suposiciones utilizadas para generar el diagrama de la Figura 2 son las siguientes: existencia de capacidad de diagnóstico en línea, efecto de falla por causa común, reparación inmediata de una falla detectada, inspección y reparación perfectas a intervalos preespecificados.

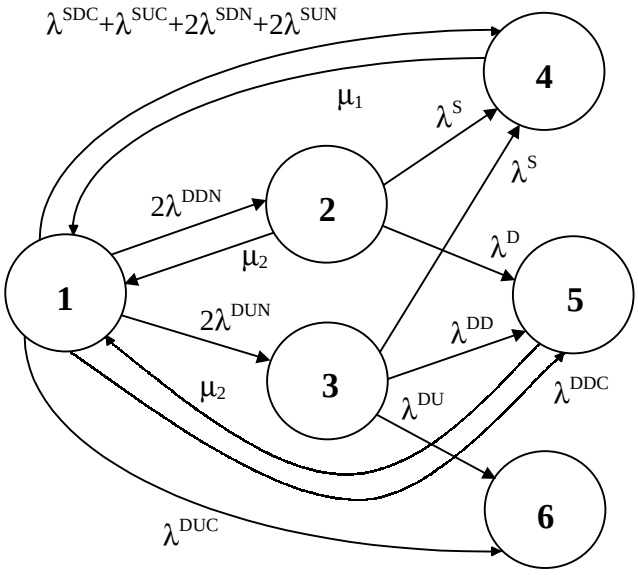

Figura 2: Diagrama de Markov de la Arquitectura 1oo2

4 PROBABILIDAD PROMEDIO DE FALLA ANTE LA DEMANDA

Para evaluar la PFD promedio del subsistema durante el intervalo entre inspecciones, al cual se designa con *TI*, es necesario evaluar la probabilidad que éste se encuentre en el estado de falla peligrosa detectada y no detectada. Por ejemplo, para la arquitectura 1oo2, se debe calcular la probabilidad promedio de permanencia en los estados 5 y 6 durante el intervalo *TI*. En este trabajo el interés se centra en la PFD promedio durante el último intervalo de la vida útil del subsistema.

Sea $\mathbf{P}(t)$ el vector, de dimensión (1 x p), correspondiente a la probabilidad de los estados contenidos en el diagrama de Markov del subsistema analizado, en general se verifica que:

$$\frac{d\mathbf{P}(t)}{dt} = \mathbf{P}(t)\,\mathbf{Q}$$
$$\mathbf{P}(t) = \mathbf{P}(0)\exp(\mathbf{Q}\,t) \qquad t>0 \tag{7}$$

siendo $\mathbf{Q}$ (p x p) la matriz de velocidades de transición ó matriz generadora. Para el caso de cadenas de Markov continuas en el tiempo y homogéneas, los elementos q_{jk} con $j \neq k$ representan las velocidades de transición desde el estado j al estado k mientras que los q_{jj} indican la suma de las velocidades de transición que sacan al sistema del estado j.

Para evaluar la probabilidad promedio de los estados del sistema en forma analítica, se requiere integrar $\mathbf{P}$(t) en el intervalo comprendido entre inspecciones, ésto no es factible pues $\mathbf{Q}$ es singular. Cabe aclarar además que no se considera conveniente aplicar en forma exclusiva modelos discretos de Markov porque interesa conocer el desempeño en seguridad del SIS durante el último periodo de su vida útil. En consecuencia se estudia una estrategia alternativa en base a modelos discretos y continuos de Markov.

Con el fin de aislar en la matriz $\mathbf{Q}$ la porción asociada a los estados transitorios ($\mathbf{Q_1}$) y absorbentes ($\mathbf{Q_2}$), $\mathbf{Q}$ se particiona de la siguiente manera:

$$\begin{bmatrix} \mathbf{Q}_1 & \mathbf{Q}_2 \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \tag{8}$$

En el caso que nos ocupa, el subsistema sólo podrá salir del estado absorbente, con cierta probabilidad, cuando se produzca el evento determinístico correspondiente a la inspección periódica realizada luego de transcurrido un intervalo de longitud *TI*.

Si se asume que la vida útil estimada del SIS son n años, es posible discretizar la escala de tiempos en intervalos coincidentes con el período de inspección y calcular por pasos el vector $\mathbf{P_1}(t)$ correspondiente a la probabilidad de los estados transitorios. El número de intervalos operativos resulta:

$$I = n / TI \tag{9}$$

y el vector $\mathbf{P_1}$ (t) para los diferentes intervalos se calcula mediante las siguientes expresiones:

$$\begin{aligned}
\mathbf{P_1}\,(t) &= \mathbf{P_1}\,(0)\,\exp\,(\mathbf{Q_1}\,t) \qquad 0 \le t \le TI \\
\mathbf{P_1}\,(t) &= \mathbf{P_1}\,(TI^+)\,\exp\,[\mathbf{Q_1}\,(t\text{-}TI)] \qquad TI \le t \le 2\,TI \\
&\vdots \\
\mathbf{P_1}\,(t) &= \mathbf{P_1}\,(i\,TI^+)\,\exp\,[\mathbf{Q_1}\,(t\text{-}i\,TI)] \qquad i\,TI \le t \le (i\text{+}1)\,TI \\
&\vdots \\
\mathbf{P_1}\,(t) &= \mathbf{P_1}\,[(I\text{-}1)TI^+]\,\exp\,\{\mathbf{Q_1}\,[\text{t-}(I\text{-}1)\,TI]\} \qquad (I\text{-}1)\,TI \le t \le I\,TI
\end{aligned} \tag{10}$$

siendo $\mathbf{P_1}\,(i\,TI^+)$ el vector de probabilidad de los estados transitorios después de la *i*-ésima inspección.

La probabilidad de los estados del sistema antes de la *i*-ésima inspección es $\mathbf{P}(i\,TI)$. Este vector puede modificarse como consecuencia del proceso de inspección y reparación. A fin de considerar el efecto de la confiabilidad humana sobre $\mathbf{P}(t)$, se introduce la matriz de reparación $\mathbf{R}$[14], de manera tal que:

$$\begin{aligned}
\mathbf{P}(TI^+) &= \mathbf{P}(TI)\,\mathbf{R} = \mathbf{P}(0)\,\exp\,(\mathbf{Q}\,TI)\,\mathbf{R} \\
\mathbf{P}(2\,TI^+) &= \mathbf{P}(2\,TI)\,\mathbf{R} = \mathbf{P}(TI^+)\,\exp\,(\mathbf{Q}\,TI)\,\mathbf{R} = \mathbf{P}(0)\,[\exp\,(\mathbf{Q}\,TI)\,\mathbf{R}]^2 \\
&\vdots \\
\mathbf{P}(i\,TI^+) &= \mathrm{P}(iTI)\,\mathbf{R} = \mathbf{P}(0)\,[\exp\,(\mathbf{Q}\,TI)\,\mathbf{R}]^i \\
&\vdots \\
\mathbf{P}[(I\text{-}1)\,TI^+] &= \mathrm{P}[(I\text{-}1)\,TI]\,\mathbf{R} = \mathbf{P}(0)\,[\exp\,(\mathbf{Q}\,TI)\,\mathbf{R}]^{I\text{-}1}
\end{aligned} \tag{11}$$

Los elementos de la matriz $\mathbf{R}$ (p x p) son tales que: r_{jk} indica la probabilidad que el mantenimiento lleve el sistema del estado j al estado k, mientras que r_{jj} determina la probabilidad que los estados degradados o de falla no sean identificados durante la inspección. La suma de los elementos de cada fila de $\mathbf{R}$ es la unidad. El uso de bases de datos sobre errores de mantenimiento permite determinar cuáles son los estados degradados del subsistema más difíciles de detectar ó aquellos más susceptibles a errores de reparación con el fin de construir la correspondiente matriz de reparación.

A fin de evaluar $\mathbf{P_1}\,(i\,TI^+)$ en la Ecuación (10), se multiplica $\mathbf{P}(i\,TI^+)$ por una matriz $\mathbf{Z}$ de dimensión [p x (p-1)] tal que:

$$\mathbf{Z} = \begin{bmatrix} \mathbf{I} \\ \mathbf{0} \end{bmatrix} \tag{12}$$

siendo $\mathbf{I}$ una matriz identidad de dimensión [(p-1) x (p-1)] y $\mathbf{0}$ un vector fila de ceros de dimensión (p-1). En consecuencia:

$$\mathbf{P_1}\,(i\,TI^+) = \mathbf{P}\,(i\,TI^+)\,\mathbf{Z} = \mathbf{P}(0)\,[\exp\,(\mathbf{Q}\,TI)\,\mathbf{R}]^i\,\mathbf{Z} \tag{13}$$

La PFD del subsistema está asociada a los estados de su diagrama de Markov en los cuales éste no puede responder ante un peligro como consecuencia de experimentar una falla total detectada ó no detectada. Para calcular la PFD para el intervalo operativo (i+1) comprendido entre las inspecciones periódicas i e (i+1)se realiza el siguiente procedimiento:

a) se elimina el aporte del estado de falla detectada del vector $\mathbf{P_1}$ y se suman las

probabilidades promedio de los restantes estados, según indica la siguiente formulación:

$$\overline{P}_{ES}^{\,i+1} = \frac{1}{TI} \int_{i\,TI}^{(i+1)\,TI} \mathbf{P_1}(t) \left[\mathbf{1_E}\ \mathbf{1_S}\ \mathbf{0_{DD}}\right]^{\mathbf{T}} dt \tag{14}$$

siendo $\overline{P}_{ES}^{\,i+1}$ = probabilidad promedio de los estados de éxito y falla segura, $\mathbf{1_E}$ = vector fila con elementos iguales a la unidad para cada estado de éxito, $\mathbf{1_S}$ = vector fila conteniendo unos para los estados de falla segura, $\mathbf{0_{DD}}$ = vector fila nulo para los estados peligrosos detectados. Reemplazando en la Ecuación (14), $\mathbf{P_1}(t)$ por su expresión resulta:

$$\begin{aligned} \overline{P}_{ES}^{\,i+1} &= \frac{1}{TI} \int_{i\,TI}^{(i+1)\,TI} \mathbf{P_1}(i\,TI^{+}) \exp\left[\mathbf{Q_1}(t - i\,TI)\right] dt \left[\mathbf{1_E}\ \mathbf{1_S}\ \mathbf{0_{DD}}\right]^{\mathbf{T}} = \\ \overline{P}_{ES}^{\,i+1} &= \frac{1}{TI}\, \mathbf{P_1}(0) \left[\exp(\mathbf{Q}\,TI)\,\mathbf{R}\right]^{i} \mathbf{Z} \left[\exp\left(\mathbf{Q_1}\,TI\right) - \mathbf{I}\right] \mathbf{Q_1^{-1}} \left[\mathbf{1_E}\ \mathbf{1_S}\ \mathbf{0_{DD}}\right]^{\mathbf{T}} \end{aligned} \tag{15}$$

b) se calcula la $\overline{PFD}^{\,i+1}$ restándole a la unidad la probabilidad promedio de los estados de éxito y falla segura, $\overline{P}_{ES}^{\,i+1}$, del mismo intervalo

$$\overline{PFD}^{\,i+1} = 1 - \overline{P}_{ES}^{\,i+1} \tag{16}$$

La probabilidad promedio de falla ante la demanda del último intervalo de la vida útil del subsistema, es decir luego de haber efectuado la inspección número (*I*-1), es:

$$\overline{PFD}^{\,I} = 1 - \frac{1}{TI}\, \mathbf{P_1}(0) \left[\exp(\mathbf{Q}\,TI)\,\mathbf{R}\right]^{I-1} \mathbf{Z} \left[\exp\left(\mathbf{Q_1}\,TI\right) - \mathbf{I}\right] \mathbf{Q_1^{-1}} \left[\mathbf{1_E}\ \mathbf{1_S}\ \mathbf{0_{DD}}\right]^{\mathbf{T}} \tag{17}$$

Esta probabilidad resulta mayor que la correspondiente al caso de mantenimiento perfecto.

5 EXPONENCIAL DE UNA MATRIZ

El programa de optimización de SIS realiza tres cálculos de PFD promedio al evaluar si la restricción del SIL se verifica para una posible solución. Cada cálculo de la PFD involucra dos evaluaciones de la exponencial de una matriz, una se efectua para la matriz singular **Q** y otra para la no singular $\mathbf{Q_1}$.

Una alternativa de cálculo es utilizar un paquete de matemática simbólica para calcular las exponenciales en forma analítica[15] para cada arquitectura considerada, y luego incorporar estas expresiones en las correspondientes subrutinas. Estas tienen como entrada las velocidades de falla de los componentes y *TI*. Si bien este modo es viable para las arquitecturas más sencillas, no resulta robusto a medida que se incrementa el número de estados y sus interrelaciones en los diagramas de Markov. En consecuencia se utiliza el cálculo numérico de las exponenciales de matrices.

La exponencial de una matriz **A** se define como:

$$e^{\mathbf{Q}t} = \sum_{r=0}^{\infty} \mathbf{Q}^r \frac{t^r}{r!} \tag{18}$$

El uso directo de la Ecuación (18) es ineficiente por los errores de redondeo producidos al calcular las potencias de **Q**, dado que esta matriz presenta elementos positivos fuera de la diagonal y elementos negativos en la diagonal, y además porque se necesitan evaluar muchos términos de la suma infinita para conseguir una buena aproximación.

En este trabajo se aplica el método de Padé para calcular las exponenciales de matrices, pues se ha demostrado[16] que es numéricamente estable para matrices esencialmente no negativas, ésto es, matrices tales que: $q_{ij} \geq 0 \ \forall \ i \neq j$, que son las de interés para esta aplicación.

6 EJEMPLO DE APLICACIÓN

Dado el diagrama de Markov de la Figura 2 y considerando un subsistema formado por dos componentes iguales con velocidades de falla: λ_{SDC} = 299.88e-9 λ_{SUC}= 2.94e-9 λ_{DUC}= 3.36e-9 λ_{DDC}= 178.68e-9 λ_{SDN}= 9696.12e-9 λ_{SUN}= 95.06e-9 λ_{DDN}= 5777.32e-9 λ_{DUN}= 108.64e-9, se evalua el efecto de la confiabilidad humana sobre su desempeño en seguridad.

En este trabajo se asumen matrices de reparación con vectores columnas no nulos para los estados degradados o de falla asociados exclusivamente con fallas no detectadas.

En la Figura 3 se grafica la variación de la PFD promedio del último intervalo operativo en función del tiempo entre inspecciones *TI*, para matrices de reparación $\mathbf{R_1}$ (reparación perfecta), $\mathbf{R_2}$ y $\mathbf{R_3}$ (reparación imperfecta)

$$\mathbf{R_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad \mathbf{R_2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0.9 & 0 & 0.1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0.8 & 0 & 0.1 & 0 & 0 & 0.1 \end{bmatrix} \quad \mathbf{R_3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0.8 & 0 & 0.2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0.7 & 0 & 0.1 & 0 & 0 & 0.2 \end{bmatrix}$$

Se observa que es importante considerar el efecto del factor humano en los cálculos de la PFD y que éste se acentúa a medida que aumenta TI y la probabilidad de error en las tareas de inspección y reparación.

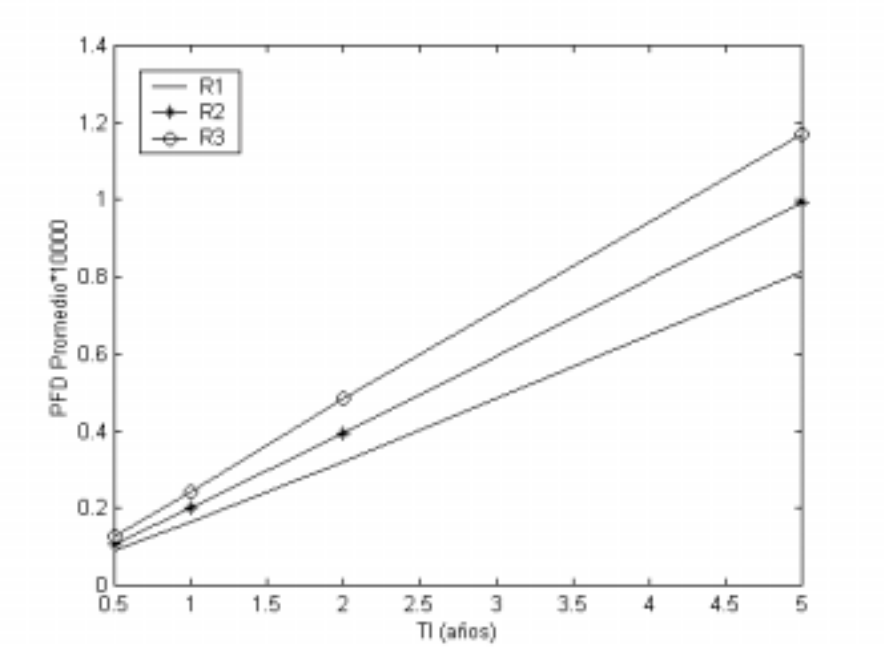

Figura 3: Reparación perfecta vs. Reparación imperfecta

7 CONCLUSIONES

En este trabajo se analiza el efecto de la confiabilidad humana sobre el desempeño de los SISs. Este se mide en función de la PFD en el último periodo de su vida útil. Para evaluar esta variable se formula una expresión compacta, que resulta de modelar las probabilidades de transición entre estados considerando:

a) Modelos de Markov Continuos para los periodos entre inspecciones
b) Modelos de Markov Discretos para los tiempos inmediatamente posteriores a las inspecciones.

El cálculo de la PFD involucra evaluar la exponencial de dos matrices, una de las cuales es singular. El método de Padé para resolución de la exponencial de matrices resultó satisfactorio para su incorporación en la estrategia de diseño óptimo del SIS.

8 REFERENCIAS

[1] ANSI/ISA S.84.01 “Application of Safety Instrumented Systems for the Process Industries”, American National Standard Institute, (1996).
[2] IEC 61508, “Functional Safety of Electric/Electronic/Programmable Electronic Safety-Related Systems, International Electrotechnical Commission, (2000).
[3] IEC 61511, “Functional Safety: Safety Instrumented Systems for the Process Industry Sector”, International Electrotechnical Commission, (2003).
[4] Summers A., “Techniques for assigning a target safety integrity level”, ISA Transactions, 95-104 (1998).
[5] Beckman, L. (1998). “Determining the required safety integrity level for your process”, ISA Transactions, 105-111, (1998).
[6] Dowell A. and Green D., “Formulate Emergency Shutdown Systems by Cookbook”,

Chemical Engineering Progress, 51-61, (1998).
[7] Ford K. and Summers A. (1998). “Are Your Instrumented Safety Systems Up to Standard?”, Chemical Engineering Progress, 55-58, (1998).
[8] Ford K. and Summers A. (1999). “Is Your SIS Grandfathered?”, Chemical Engineering Progress, 39-42, (1999).
[9] Martorell S., Carlos S., Sánchez A. and Serradell V., “Constrained optimization of test intervals using a steady state Genetic Algorithm”, Reliability Engineering and System Safety, 67, 215-232, (2000).
[10]Giuggioli P., M. Marseguerra, and E. Zio, “Application of Genetic Algorithms to the Multiple Objective Optimization of the Inspection Times of a Safety System of a Pressurized Water Reactor”, ESREL 2001 Conference, Torino, Italy, 1052-1060, (2001).
[11] Noya, G., M. Sánchez and A. Bandoni, “Reliability and Cost Issues in Safety Control System Design”, Proceedings of the Topical Conference “Process Plant Safety Symposium” AIChE Spring Meeting 2003, 10 pág, (2003).
[12] Noya, G., M. Sánchez and A. Bandoni, “Optimal Safety Control System Design”, Chemical Engineering Transactions, 3, 781-786, (2003).
[13] Goble, W., “Control Systems Safety Evaluation & Reliability”, Instrumentation Society of America, (1998).
[14] Bukowski, J., “Modeling and Analyzing the Effects of Periodic Inspection on the Performance of Safety Critical Systems”, IEEE Transactions on Reliability, 50, 321-329, (2001).
[15] Noble, B. and J. Daniel, Algebra Lineal Aplicada, Prentice-Hall Hispanoamericana, S. A.,México (1989).
[16] Arioli, M., B. Codenotti and C. Fassino, “The Padé Method for Computing the Matrix Exponential”, Linear Algebra and its Applications, 240, 111-130 (1996).