

METODOLOGÍA PARA EVALUAR LA CONFIABILIDAD DE UN SISTEMA EMPLEANDO LÓGICA COMBINACIONAL

Ing. Msc. Guillermo Tejada Muñoz
d270031@unmsm.edu.pe

Facultad de Ingeniería Electrónica de la Universidad Nacional Mayor de San Marcos de Lima -Perú

Resumen: El presente trabajo presenta una metodología para evaluar la confiabilidad de sistemas y su cálculo a través de herramientas sencillas basadas en lógica combinacional. Finalmente es presentado un ejemplo que ilustra la metodología sugerida.

Abstract: The present work presents a methodology to evaluate the reliability of systems and the calculations through simple tools based on combinatorial logical. Finally it is presented an example that illustrates the suggested methodology.

Palabras claves: Confiabilidad, Modelo Combinacional, Tasa de Falla, MTTF, MTBF, Disponibilidad.

I. INTRODUCCIÓN

En sistemas como aeronaves, trenes, equipos de telecomunicaciones, equipos médicos, militares, etc. los ingenieros deben evaluar diferentes diseños para estas aplicaciones en términos de costo, desempeño, confiabilidad o una combinación de estas medidas. La confiabilidad de un sistema, equipo, dispositivo, etc. esta íntimamente ligado a su calidad y en muchos diseños la confiabilidad es una norma que debe cumplirse para que no se ponga en riesgo grandes recursos materiales o invaluable vidas humanas. Por estos motivos, la confiabilidad es un tópico importante que el ingeniero diseñador no debería ignorar.

Los modelos de confiabilidad pueden ser usadas para:

- Ayudar e interpretar los requisitos para establecer sistemas confiables;
- Predecir la confiabilidad de diferentes configuraciones de sistemas;
- Identificar tempranamente los puntos débiles o los cuellos de botella de un producto o sistema de tal manera que los diseñadores puedan hacer cambios menos costosos; y
- Determinar las estrategias de rentabilidad y mantenimiento.

II. MODELOS DE CONFIABILIDAD

Los modelos de confiabilidad no son útiles aisladamente, ellos son parte de un gran proceso para producir un sistema confiable a un razonable costo. Para evaluar un sistema, los diseñadores deben formular un modelo

preliminar donde los subsistemas deben ser cajas negras. El modelo preliminar puede servir inicialmente para ayudar a colocar los requisitos de confiabilidad para el subsistema. Posteriormente, los resultados de estos servirán para actualizar los modelos. En este camino se pueden identificar, evaluar y si es necesario rediseñar subsistemas que podrían ser potenciales cuellos de botellas. El proceso puede repetirse reiteradamente de tal modo que el modelo sea cada vez mas refinado. [Reibman y Veeraraghavam, 1991].

En este modelo iterativo de confiabilidad se pueden distinguir seis etapas:

- (1) Escoger las métricas para el análisis del sistema.
- (2) Construir un modelo de confiabilidad del sistema.
- (3) Analizar el modelo.
- (4) Refinar el modelo hasta conseguir su exactitud.
- (5) Usar los resultados para mejorar un modelo que pueda ayudar a tomar decisiones en el sistema.
- (6) Actualizar el modelo.

Este proceso se presenta en la figura 1.

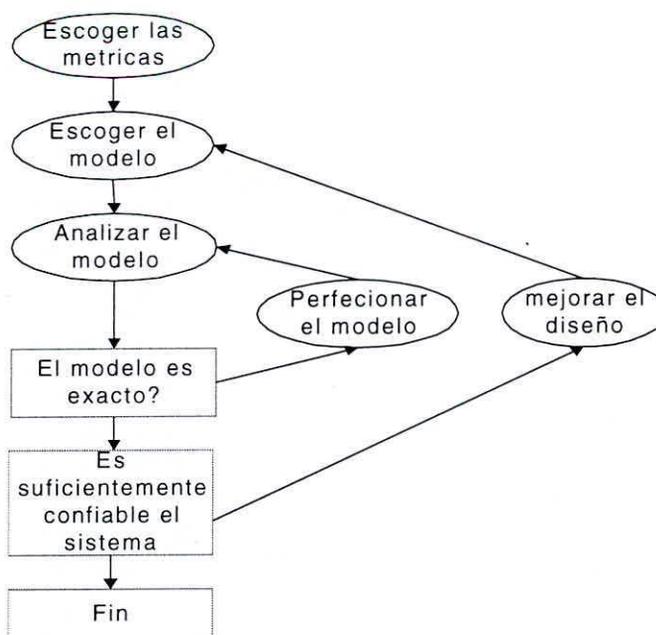


Figura 1 Diagrama de flujo para modelar el sistema.

III. MÉTRICAS PARA ANÁLISIS DE SISTEMAS

En esta primera etapa, se escoge la métrica correcta, después de analizar la información sobre los requisitos del sistema. Las métricas comunes incluyen:

- Métricas dependientes del tiempo
- Métricas independientes del tiempo

3.1 Métricas Dependientes del Tiempo

3.1.1 Confiabilidad

Confiabilidad $R(t)$ es la probabilidad que el sistema no falle durante un tiempo igual a t o que el sistema falle para un tiempo mayor que t , matemáticamente es igual a:

$$R(t) = \exp\left[-\int_0^t \lambda(t') dt'\right]$$

Donde $\lambda(t')$ es la función de "tasa de falla".

La figura 2a muestra la curva de fallas de muchas computadoras y otros equipos electrónicos. La zona inicial de la curva, llamada de fallas prematuras o de "mortalidad infantil" es producida por los componentes con defectos de fabricación, las cuales pueden ser eliminadas por el control de calidad del producto. La zona media de la curva es llamada de "vida útil", las fallas en esta zona son solo aleatorias. La zona derecha de la curva es llamada de "envejecimiento" y es producida por la degradación de las características de los componentes a lo largo del tiempo, sin embargo sus efectos podrían ser disminuidos por el mantenimiento preventivo del sistema.

La figura 2b muestra la curva de fallas típica para el caso de los programas de software, cuyas características, en la mayoría de los casos son la causa de las fallas ocultas o por defectos que aparecen en la fase de inicio del desarrollo de los programas de software.

Finalmente, la figura 2c muestra la curva típica de fallas para equipamientos de naturaleza mecánica como máquinas electromecánicas, válvulas, bombas, etc. [Tejada, 1998]

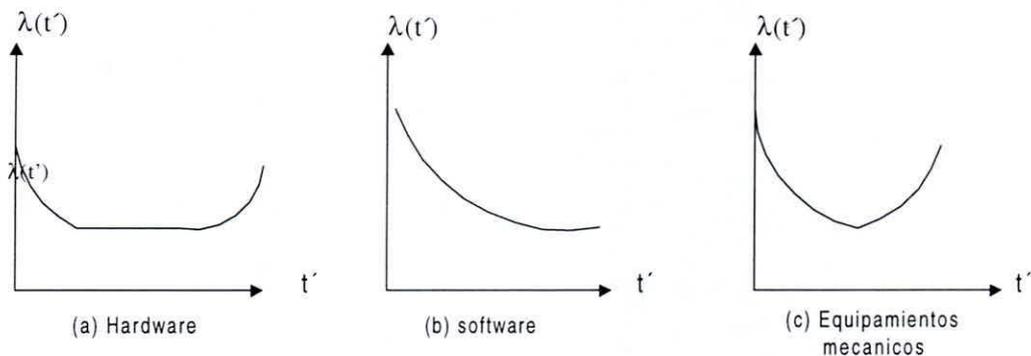


Figura 2 Curva de falla para diferentes sistemas

En la mayoría de los cálculos de confiabilidad solo se considera una tasa de falla como la mostrada en (a) y en la región donde ella permanece constante ($\lambda(t') = cte.$). En este caso de la ecuación de confiabilidad es:

$$R(t) = \exp(-\lambda t) \quad (1)$$

3.2 Métricas Independientes del Tiempo

3.2.1 Tasa de Falla Constante (λ)

El parámetro constante λ que acabamos de definir es un parámetro independiente del tiempo y que podría usarse para dar una primera idea de la Confiabilidad de un dispositivo o sistema, con estas mismas características existen igualmente otros parámetros, los cuales son muy utilizados y a los cuales se les denominan *Mean Time to Failures* (MTTF) y *Mean Time Between Failures* (MTBF), los mismos que serán definidos a continuación.

3.2.2 Mean Time to Failures (MTTF)

El *Mean Time to Failures* (MTTF, Tiempo Medio para Fallar) es el tiempo esperado para que un dispositivo falle, es un parámetro importante para comparar diferentes diseños no reparables (circuito integrado, transistor, etc.) y no depende del tiempo. El MTTF especifica un tiempo medio donde el sistema podría funcionar sin presentar fallas, por este motivo, no acompaña la variabilidad (es independiente del tiempo) de muchos sistemas, así por ejemplo, a pesar que el MTTF del sistema electrónico de un avión, fuera significativamente mayor que el tiempo empleado por una misión de vuelo, no necesariamente este hecho garantizará que durante ese tiempo el sistema no pueda fallar o que sea altamente confiable. [Reibman y Veeraraghavam 1991], [Lewis, 1987]

Matemáticamente el MTTF es definido como:

$$MTTF = \int_0^{\infty} R(t)dt = \int_0^{\infty} \exp(-\lambda t) = \lambda^{-1}$$

3.2.3 Mean Time Between Failures (MTBF)

Mientras que el MTTF es un parámetro que evalúa la confiabilidad para un sistema no reparable, el parámetro *Mean Time Between Failures* (MTBF, Tiempo Medio entre Fallas) evalúa la confiabilidad para un sistema reparable (equipos electrónicos, etc.), matemáticamente se calcula igual que el MTTF:

$$MTBF = \lambda^{-1}$$

IV. TIPOS DE MODELOS DE CONFIABILIDAD

Existen principalmente tres tipos de modelos de confiabilidad, los cuales son:

- (a) Modelo de Contar Partes
- (b) Modelo Combinacional
- (c) Modelo de Espacio de Estado o Markov

4.1 Modelo de Contar Partes

El modelo de Contar Partes puede dar una primera aproximación de la confiabilidad en un sistema a través del cálculo de su tasa de falla. En este modelo la falla de cualquier componente provocaría la falla del sistema. La tasa de falla es calculada como la suma de todas las tasas de falla de cada componente o parte. El modelo generalmente provee una estimación adecuada de la confiabilidad, sobre todo para el caso de tarjetas electrónicas o pequeñas computadoras. Sin embargo, el modelo no sería útil si el equipo o sistema presenta algunas características de tolerancia a fallas.

Este modelo de predicción es aplicable durante la fase inicial del proyecto, cuando hay insuficiente información como para estimar la confiabilidad del componente. La expresión matemática general para el cálculo de la tasa de falla del equipamiento es:

$$\lambda_{EQUIP} = \sum_{i=1}^n (N\lambda_g \Pi_Q)_i \quad (2)$$

donde,

- λ_{EQUIP} = Tasa de falla total del equipo;
- N = Cantidad de componentes del tipo i ;
- λ_g = Tasa de falla genérica del componente de tipo i ;
- Π_Q = Factor de calidad del componente de tipo i ;
- n = Diferentes tipos de componentes en el equipo.

En otros cálculos más rigurosos la tasa de falla es expresada como:

$$\lambda_p = \lambda_b \Pi_Y \Pi_Q \dots \Pi_N \quad (3)$$

Donde, λ_b es la tasa de falla base que lleva en cuenta las características de temperatura y los parámetros eléctricos a los cuales el componente opera. $\Pi_Y \Pi_Q \dots \Pi_N$, son los llamados factores de corrección, donde el factor Π_Y representa las condiciones rigurosas de prueba a la cual el componente fue expuesto y el factor Π_Q representa la calidad de su fabricación. [Military Handbook, 1991]

4.2 Modelo Combinacional

El modelo Combinacional incluye a los modelos llamados "fallas en árbol" o "árbol de éxitos" diagramas de bloques de confiabilidad. Este modelo puede capturar algunos aspectos de tolerancia de fallas en el sistema, pero no aquellos como la reparación y la reconfiguración del sistema.

En un modelo combinacional, el comportamiento del sistema será representado apropiadamente por una serie de eventos concatenados. Así por ejemplo, la representación de un sistema constituido por dos computadoras y una fuente de energía puede ser realizada a través de una puerta AND y un bloque que representa el éxito del sistema (figura 3). En este modelo todos los componentes en la entrada de la puerta deberían estar sin fallas para lograr el éxito, es decir para evitar su falla.

Los círculos F, C1 y C2, ver figura 3, representan la fuente de energía y las computadoras respectivamente, los cuales pueden tener el valor de 0 lógico (en caso estuvieran con falla) ó 1 lógico (en caso estuvieran sin falla). La confiabilidad del sistema será la probabilidad de ocurrencias favorables (no presentar fallas) de los eventos F, C1 y C2. La salida del sistema será igual a:

$$S = F.C1.C2 \quad (4)$$

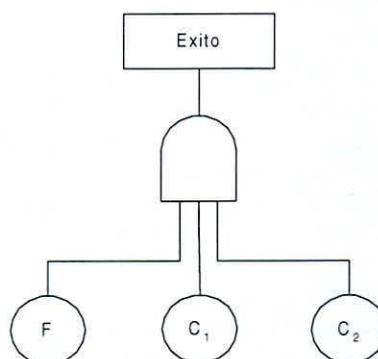


Figura 3 - Arbol de Exito para un sistema serie

Si consideramos que F, C1 y C2 son eventos independientes, la probabilidad que el sistema tenga éxito (no falle) será:

$$P(S) = P(FC_1C_2) = P(F).P(C_1).P(C_2) \quad (5)$$

La probabilidad que el sistema, las computadoras o la fuente de alimentación no fallen es lo mismo que hallar de su confiabilidad, por lo tanto si la confiabilidad de las computadoras es R_C y el de la fuente de alimentación R_F , entonces de (5) obtenemos:

$$R = R_F R_C^2 \quad (6)$$

Por otra parte, el modelo que representa la posibilidad que el sistema continúe funcionando a pesar de que una de las computadoras falle, podría representarse como se muestra en la figura 4.

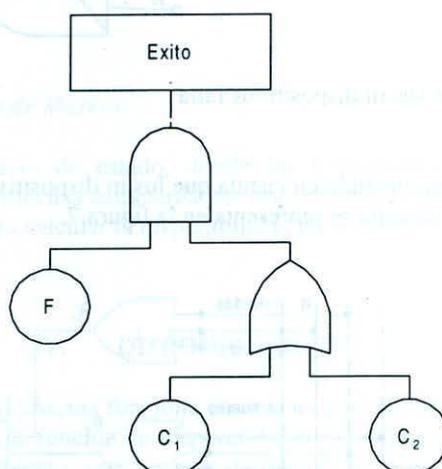


Figura 4 Arbol de Exito para un sistema paralelo

El sistema ahora incluye la puerta OR. La salida del sistema en esta caso será:

$$S = F(C_1 + C_2) \quad (7)$$

Considerando nuevamente que C_1 , C_2 y F son eventos independientes, la probabilidad que el sistema tenga éxito (no falle) es:

$$P(S) = P(F)[P(C_1) + P(C_2) - P(C_1)P(C_2)] \quad (8)$$

En términos de confiabilidad:

$$R = R_F(R_C + R_C - R_C R_C) = R_F(2R_C - R_C^2) \quad (9)$$

La figura 5, muestra algunas equivalencias importantes entre los circuitos lógicos que podrían ayudar al cálculo de la confiabilidad.

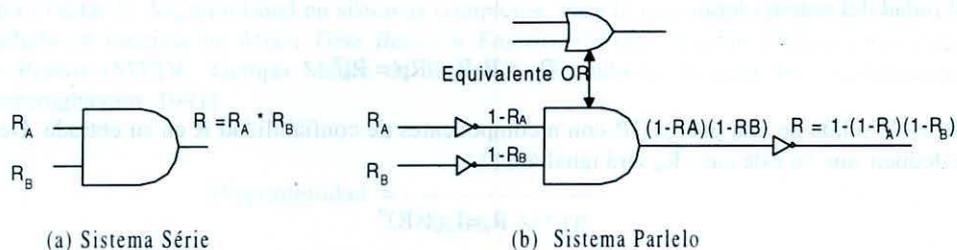


Figura 5 Equivalencia para el cálculo de la confiabilidad

VI. PERFECCIONAMIENTO DEL MODELO

En esta etapa los proyectistas deben decidir si el modelo es suficientemente exacto para permitir tomar decisiones sobre el sistema. Los errores más comunes en esta etapa son:

- Error en el modelo.- son inexactitudes causadas por suposiciones incorrectas, como por ejemplo, independencia o distribución incorrecta de fallas.
- Error de especificación, son errores accidentales estructurales en el modelo, como por ejemplo estados innecesarios u otros dejados de lado.
- Errores de parámetros, son errores incorrectos en los parámetros del modelo, como por ejemplo, las tasas de reparo y de fallas. Los diseñadores obtienen los parámetros de fuentes o resultados de pruebas equivocadas.
- Errores en la solución, son producidos por aplicar equivocadamente aproximaciones, los procedimientos numéricos, y las simulaciones en la solución del modelo. Los diseñadores podrían reducir estos errores, con el uso cuidadoso de algoritmos especiales y de simulación.

Los siguientes consejos pueden ayudar a reducir los errores:

- Explicar las simplificaciones del modelo.
- Documentar y revisar minuciosamente las fuentes de información de los parámetros, determinando la veracidad de la información.
- Aproximar la confiabilidad del sistema como la media entre un modelo conservador y otro optimista. El modelo conservador podría ser obtenido, por ejemplo, incrementando la tasa de fallas de los componentes o asumiendo fallas múltiples de los componentes, que causarían fallas al sistema, mientras que el modelo optimista podría ser obtenido asumiendo ausencia de fallas de los componentes del modelo.
- Detectar aquellos parámetros cuyos cambios afectarían el modelo. El hecho de que el modelo sea sensible a los cambios de un particular parámetro, puede estar indicando un punto débil. La confiabilidad del sistema aumentaría considerablemente mejorando los componentes que podrían ser el cuello de botella del sistema.
- Revisar el modelo, por especialistas con el objetivo de eliminar el mayor número posible de errores de tal manera que pueda capturar importantes aspectos del comportamiento del sistema.

VII. EJEMPLO DE ANÁLISIS DE UN SISTEMA

7.1 Red Hipotética de Procesamiento de Datos en una Aeronave

A continuación se muestra un ejemplo sugerido por Reibman y Veeraraghavam, 1991 pero a diferencia del artículo referido en nuestro trabajo, se calculará la confiabilidad del sistema, sobre la base de modelos combinatoriales, sin necesidad de recurrir a modelos complejos como los modelos de Markov.

La figura 9 muestra el diseño de la red a estudiar, el cual consiste de tres idénticos subsistemas, cada uno de los cuales consiste de cinco nodos interconectados en anillo y un procesador conectado a él a través de dos enlaces. Los nodos que ocupan la misma posición en diferentes anillos son sensores o actuadores del mismo tipo. Así por ejemplo, los nodos A1, A2 y A3 están todos enlazados a sensores de temperatura.

Luego de analizar el funcionamiento de la red, puede imponerse las siguientes condiciones:

- Si dos de tres sensores o actuadores del mismo tipo fallan el sistema es declarado inoperativo;
- Si un nodo falla, el sensor o actuador unido a él esta indisponible;
- Si un procesador falla, el anillo unido a él esta indisponible.

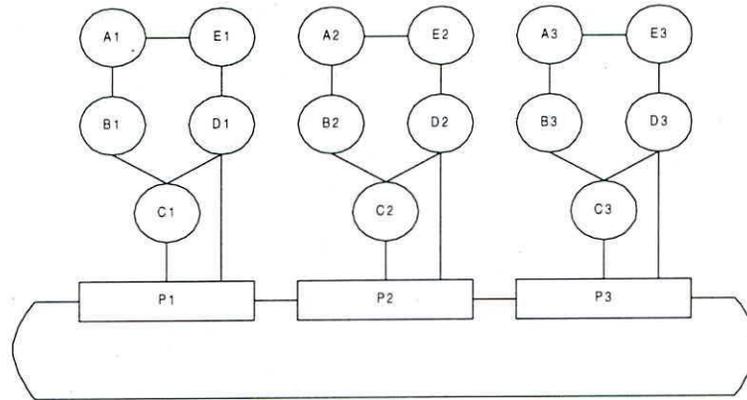


Figura 9 - Red de procesamiento de datos en una aeronave

7.1.1 Modelo de Contar Partes: Cálculo de la Tasa de Falla

La siguiente Tabla muestra la tasa de falla de los componentes de la red.

Tabla 1 - Tasa de falla de los componentes de la red

Dispositivo	Tasa de Falla	Valor (falla / hora)
Procesador	λ_P	1.0×10^{-4}
Nodo con Sensor y Actuador	λ_N	6.0×10^{-6}

7.1.2 Cálculo de la Confiabilidad a través de circuitos combinacionales

Para nuestro análisis se asumirá que:

- Los componentes tienen una tasa de falla constante con una función de distribución de falla exponencial;
- Todos los componentes fallan independientemente;
- Los equipos no son reparados durante las horas de vuelo;
- Todos los enlaces son totalmente confiables;
- Tres diferentes combinaciones de fallas causan la falla del sistema:
 - 1- Falla cuando dos o tres procesadores fallan;
 - 2- Falla cuando dos nodos en la misma posición o dos diferentes anillos fallan;
 - 3- Falla cuando cualquier nodo en un anillo falla y cualquier procesador controlando a otro anillo falla.

La intención es crear un simple modelo combinatorial que refleje las condiciones de fallas, lograrlo es algo difícil, así que en su lugar se analizará dos modelos, un modelo conservativo y otro optimista; la confiabilidad del sistema descansará entre los valores calculados para esos modelos.

En el modelo conservador, asumiremos que un anillo falla, debido a la inoperatividad de sus nodos o del procesador enlazado a este. Por otro lado la falla de dos anillos provocará que falle el sistema. La figura 10 representa esta situación.

Asumiremos que R_p es la confiabilidad de cada procesador y R_N es la confiabilidad de cada nodo, las expresiones matemáticas para cada caso son:

$$R_p = \exp(-\lambda_p t),$$

$$R_N = \exp(-\lambda_N t),$$

La confiabilidad en los puntos de salida S_1 , S_2 y S_3 será respectivamente:

$$S_1 = S_2 = S_3 = R_p R_N^5 = S$$

La confiabilidad en la salida del sistema será:

$$R_{T1} = [1 - (1 - S)^2]^3$$

Para los valores de la tabla 1 y para un vuelo de cinco horas de misión la confiabilidad del sistema será:

$$R_{T1} = 0.9999987333$$

O una inconfiabilidad de:

$$U_1 = 1 - R_{T1} = 0.0000012667 = 1.2667 \times 10^{-6}$$

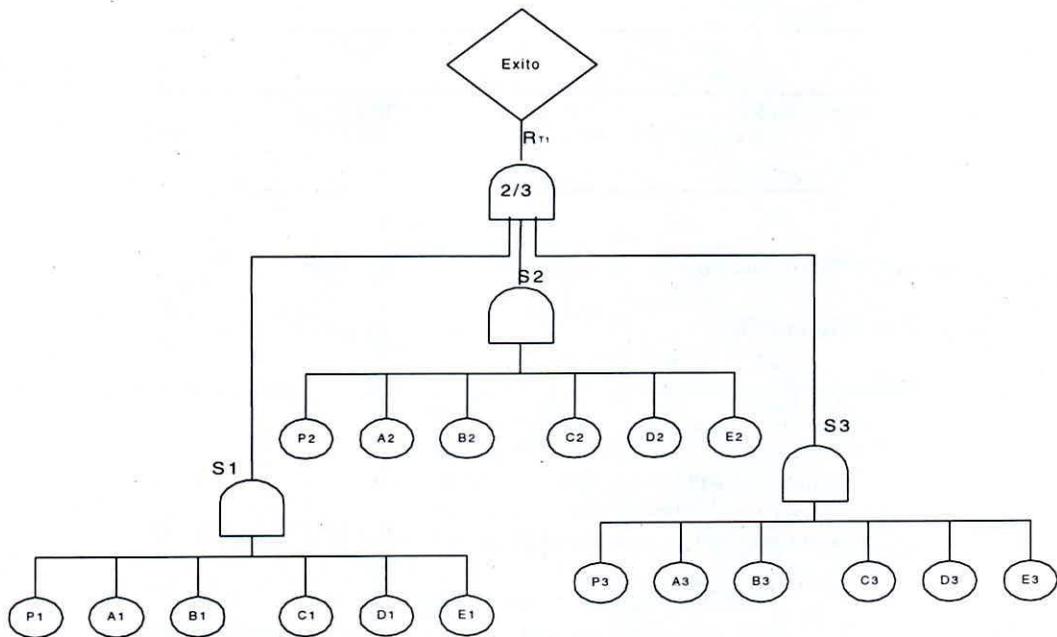


Figura 10 Modelo combinacional conservador

Por otro lado, el modelo optimista asume que el sistema es tolerante a fallas. La inoperatividad del sistema se producirá si dos de cualquiera de los componentes del mismo tipo fallan. La figura 11 muestra este caso.

De la figura 11 en los puntos de salida S_P, S_A, S_B, S_E la confiabilidad será respectivamente:

$$S_P = [1 - (1 - R_P)^2]^3$$

$$S_A = S_B = S_C = S_D = S_E = [1 - (1 - R_N)^2]^3$$

Por lo tanto, la confiabilidad en la salida del sistema será:

$$R_{T2} = S_P S_A S_B S_C S_D S_E$$

$$R_{T2} = [1 - (1 - R_P)^2]^3 [1 - (1 - R_N)^2]^5$$

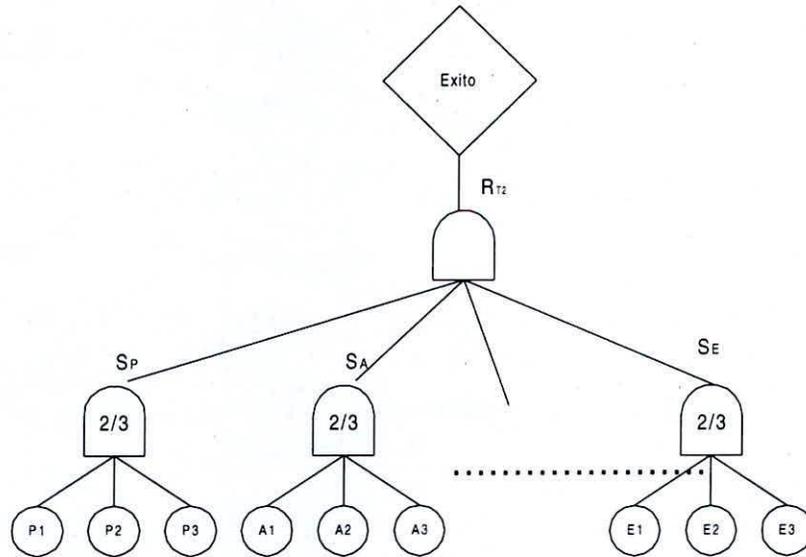


Figura 11 - Modelo Combinacional Optimista

Para los valores de la tabla 1 y para un vuelo de cinco horas la confiabilidad del sistema será:

$$R_{T2} = 0.9999992369$$

O una inconfiabilidad de:

$$U_2 = 1 - R_{T2} = 0.0000007631 = 7.631 \times 10^{-7}$$

Finalmente, la confiabilidad e inconfiabilidad del sistema, se obtiene como resultado de la media entre los modelos conservador y optimista:

$$R_T = (R_{T1} + R_{T2}) / 2 = 0.999998985$$

$$U_T = 1 - R_T = 1 \times 10^{-6}$$

Esto significa que para 5 horas de vuelo existe una probabilidad que el sistema falle de 0.000001.

VIII. REFINAMIENTO DEL MODELO

El primer paso para refinar el modelo es identificar las principales causas de falla del sistema, es decir los cuellos de botella.

A continuación haciendo uso de las mismas herramientas matemáticas, se analiza los modelos donde el sistema falla por causa de un nodo, un procesador y por causa de dos procesadores respectivamente.

La figura 12 muestra el caso que el sistema falla a causa de un nodo y un procesador.

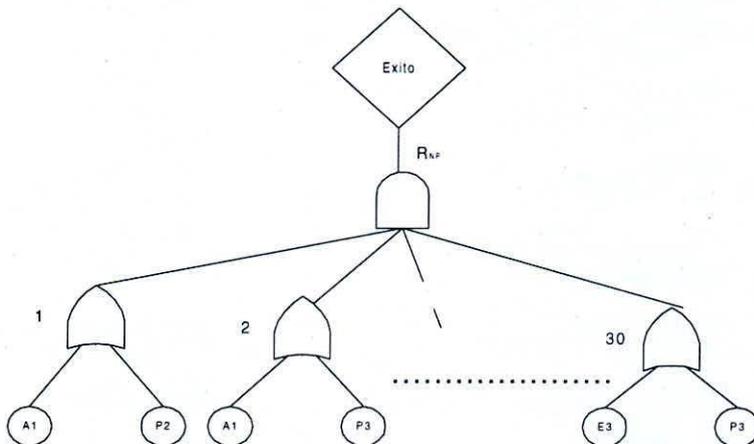


Figura 12 Modelo combinacional donde el sistema falla por causa de un nodo y un procesador

De la figura 12 se encuentra:

$$R_{NP} = [1 - (1 - R_N)(1 - R_P)]^{30} = 0.999999955$$

O una inconfiabilidad de:

$$U_{NP} = 1 - R_{NP} = 4.5 \times 10^{-7}$$

La figura 13 muestra el caso que el sistema falla a causa de 02 procesadores.

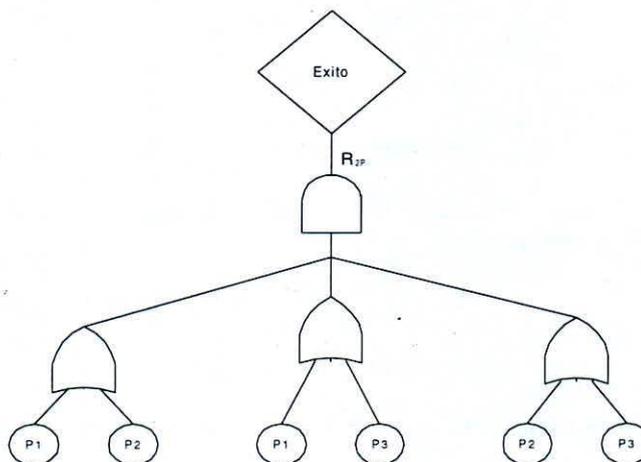


Figura 13 Modelo combinacional donde el sistema falla por causa de 02 procesadores.

De la figura 13 se encuentra que:

$$R_{2P} = [1 - (1 - R_P)^2]^3 = 0.9999992504$$

O una inconfiabilidad de:

$$U_{2P} = 1 - R_{2P} = 7.496 \times 10^{-7}$$

Por métodos análogos se podría encontrar la falla del sistema por causa de dos nodos encontrándose como resultado:

$$U_{2N} = 1.34 \times 10^{-8}$$

De estos resultados puede deducirse que la mayor frecuencia de falla del sistema ocurre al fallar un nodo y procesador y al fallar dos procesadores, entonces para mejorar la confiabilidad del sistema, pudiéramos optar por varias alternativas.

Incrementar la redundancia es una aproximación común para mejorar la confiabilidad, de esta manera podríamos agregar procesadores paralelos o hacer mejoras en el circuito interno de cada procesador, sin embargo estas soluciones podrían ser demasiado costosas. La mejor solución es cambiar la topología de la red como se muestra en la figura 14, donde al estar cada procesador conectado con dos anillos diferentes, se eliminará las causas más comunes de fallas, es decir: la falla de un procesador y nodo en diferentes anillos y la falla de dos procesadores (observar que el sistema podría funcionar aún fallando dos procesadores, debido a que con este cambio cualquier procesador podría controlar a dos anillos simultáneamente).

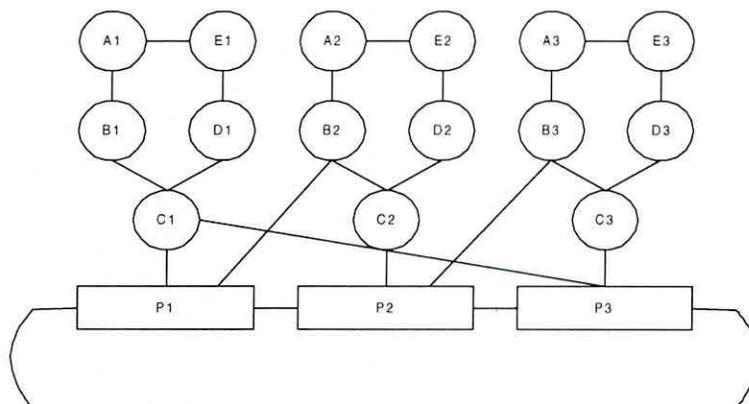


Figura 14 – Variación de la topología original

IX. CONCLUSIONES

A través de este trabajo, se está sugiriendo a los diseñadores no perder de vista, el importante tópico de confiabilidad en el desarrollo o diseño de sus productos o sistemas y se está mostrando una metodología para su cálculo. El desarrollo teórico de cada etapa, de la que consta la metodología presentada, así como los cálculos al detalle presentados en el ejemplo ilustrativo pretenden ser para el lector una guía clara de referencia para abordar problemas similares o más complejos.

Además, en el presente trabajo, ha diferencia de Reinboud, se ha calculado la confiabilidad del sistema hipotético de la aeronave a través de modelos simples, de lógica combinatorial sin necesidad de recurrir a las

herramientas matemáticas complejas, como los realizados a través de los modelos de espacio de estado de Markov. Sin embargo, este último modelo no deja de ser importante sobre todo cuando se analiza la disponibilidad en sistemas complejos con tolerancia a fallas, por este motivo se recomienda al lector consultar la bibliografía presentada.

X. REFERENCIAS BIBLIOGRAFICAS

- Clarke, A.B., R.L. Disney y R. L. *Probabilidades e procesos estocásticos*. John Wiley, 1979.
- Kapur, K.C., L.R. Lamberson y L.R. *Reliability in engineering design*. New York, John Wiley, 1977.
- Lewis, E.E., *Introduction to reliability engineering*. New York, John Wiley, 1987.
- Military Handbook, *Reliability prediction of electronic equipment*. Mil-Hdk-217f, 2 December 1991.
- Ramakumar, R. *Engineering reliability: fundamentals and applications*. Englewood Cliffs, Prentice-Hall, 1993.
- Reibman, A. L., Veeraraghavan, M. *Reliability modeling: an overview for system designers*. IEEE, 1991. p.49-57
- Tejada, M.G. *Comparação entre uma arquitetura distribuida e arquitetura centralizada no nível de instrumentação*. São Paulo, SP, 1998. Dissertação (Mestrado) - Escola Politécnica, Universidade de São Paulo.