v. 2, n. 5, 2022

Journal of
Engineering
Research

LA FIABILIDAD DINÁMICA Y LA SEGURIDAD DE FUNCIONAMIENTO DE UN SISTEMA

Gabriel Antonio Pérez Castañeda
Profesor de Ingeniería Mecatrónica en el Tecnológico Nacional de México campus Instituto Tecnológico de Tehuacán

Jesús Raymundo Flores Cabrera
Profesor de Ingeniería Mecatrónica en el Tecnológico Nacional de México campus Instituto Tecnológico de Tehuacán

Enrique Bravo Cruz
Profesor de Ingeniería Mecatrónica en el Tecnológico Nacional de México campus Instituto Tecnológico de Tehuacán

Oscar Leopoldo Pérez Castañeda
Profesor de Ingeniería Electrónica en el Tecnológico Nacional de México campus Instituto Tecnológico de Tehuacán

Martín Guadalupe Carrera Sánchez
Estudiante de Ingeniería Mecatrónica en el Tecnológico Nacional de México campus Instituto Tecnológico de Tehuacán

Resumen: Los aspectos de seguridad, disponibilidad, fiabilidad y mantenabilidad constituyen la Seguridad de Funcionamiento de un sistema. Si éste es dinámico, las herramientas tradicionales no pueden ser aplicadas eficazmente para evaluar los parámetros o cantidades antes mencionados, pues, suponen una estructura invariante en el tiempo para el sistema. Es necesario recurrir a la fiabilidad dinámica la cual tiene por objeto tomar en cuenta las interacciones entre el comportamiento funcional dinámico y determinista de un sistema y el comportamiento estocástico de sus componentes. Este artículo presenta las características y problemas que plantea la fiabilidad dinámica, así como la simulación, como herramienta de evaluación, pues se integran en ella las evoluciones discretas y continuas del sistema y los aspectos probabilísticos como las fallas.
Palabras clave: Seguridad de funcionamiento, fiabilidad dinámica, simulación de Monte Carlo, autómata estocástico híbrido.

INTRODUCCIÓN

Las preocupaciones relacionadas a la seguridad están muy presentes en el mundo de las máquinas y herramientas, del transporte o de las petroquímicas. En las instalaciones de producción manufacturera o por lotes, las preocupaciones están más bien ligadas a la disponibilidad. Desde que la que la seguridad o la disponibilidad de un sistema están en entredicho, se involucra la fiabilidad. En fin, en caso de disfuncionamiento, conviene poner al sistema en condiciones de funcionamiento inicial: es aquí que interviene la mantenabilidad. Estas cuatro características constituyen la Seguridad de Funcionamiento (SdF) de un dispositivo.

Uno de los grandes méritos del concepto de SdF es la integración de métodos y técnicas destinadas a garantizar la aptitud de un sistema a proporcionar un servicio en el cual se pueda tener confianza y asegurar que esta confianza esté justificada.

LA SEGURIDAD DE FUNCIONAMIENTO

La SdF es definida por (Villemeur, 1988) como la ciencia de las fallas. En un sentido más estricto, la SdF es la aptitud de una entidad a asumir una o varias funciones requeridas en condiciones dadas (CEI 50-191, 1990). Según (Laprie *et al.* 1995) la SdF de un sistema es la propiedad que permite a sus usuarios de colocar su confianza justificada en el servicio que él proporciona. Esta noción de confianza es fundamental, dado que todo sistema material/software contiene errores. La gran mayoría de estos errores son introducidos desde la fase de concepción del sistema.

Para practicar la SdF, es importante, primeramente, identificar las fuentes que originan las fallas de la forma más exhaustiva posible. Enseguida, por cada una de éstas, conviene evaluar su importancia con respecto a otras o con respecto a una escala de medidas absolutas (calculando su probabilidad de aparición). Además, buscar prevenir las fallas es también un objetivo primordial. Para esto, se debe observar y utilizar los modelos de evolución. Posteriormente, a toda observación de una falla, se asociarán medidas con el fin de enriquecer los modelos utilizados para la evaluación y la prevención. Finalmente, el último objetivo es controlar las fallas con la reducción de sus ocurrencias, la prevención contra las consecuencias o por su tolerancia.

En 1995, (Laprie *et al.*, 1995), definen el árbol de la SdF (figura 1). Este árbol muestra los obstáculos, los medios y los atributos asociados a la SdF. Los obstáculos están ligados a las circunstancias no deseables, pero no inesperadas. Los medios corresponden a los métodos y técnicas que permiten garantizar la aptitud del sistema a proporcionar un servicio conforme al cumplimiento de su función y

Figura 1. Relación entre la falla y el estado de un componente (Chevalier *et al.*, 2004).

dar confianza en esta aptitud. Finalmente, los atributos permiten expresar las propiedades que son esperadas del sistema y apreciar la calidad del servicio proporcionado.

La SdF cubre los conceptos de fiabilidad, mantenabilidad y disponibilidad (FMD). El equivalente anglosajón es el término dependability (reliability, maintainability, availability) frecuentemente designado por el acrónimo RAM. La seguridad es muchas veces tratada aparte. Sin embargo, el acrónimo RAMS es utilizado para designar el conjunto de actividades ligadas a estos cuatro conceptos.

La fiabilidad es definida por (Laprie *et al.*, 1995) como la medida de la continuidad de la concesión de un servicio correcto o de manera equivalente, medida también del tiempo hasta la falla. (CEI 50 (191), 1990) y (Villemeur, 1988) expresan que la fiabilidad es la aptitud de una entidad para cumplir una función requerida en condiciones dadas durante un tiempo dado. Esta aptitud se mide (Smith, 2001) por la probabilidad que una entidad realice una función requerida en condiciones dadas durante un período de tiempo dado. La fiabilidad puede ser parafraseada como la probabilidad de la no falla de la entidad en un período de tiempo dado. En el instante t, la fiabilidad se mide entonces por la probabilidad que la entidad E cumpla una función requerida en condiciones dadas durante el intervalo de tiempo $[0 ; t]$ (CEI 50 (191), 1990). Así, $R(t) = P[E \text{ soit non défaillante sur } [0 ; t]]$.

Por otro lado, la disponibilidad es la aptitud de una entidad a estar en el estado de cumplir una función requerida en condiciones dadas y en un instante dado [Villemeur, 1988]. La disponibilidad es generalmente medida por la probabilidad de que una entidad E esté en estado de cumplir una función requerida en condiciones dadas en el instante t.

También, la mantenabilidad es la aptitud de una entidad a ser reparada en un estado en el cual se pueda cumplir una función requerida, (Villemeur, 1988). La mantenabilidad es medida por la probabilidad que el mantenimiento de una entidad E cumpla en condiciones dadas con procedimientos y medios prescritos, sea terminar en el tiempo t sabiendo que la entidad falla en el tiempo $t = 0$.

Si bien la norma (CEI 50 (191), 1990) no integra la seguridad como componente de la SdF, se considera que es importante tomarla en cuenta dado que la ocurrencia de un evento catastrófico pone en peligro la vida humana. Por lo tanto, la norma (EN 292-1, 1991) la define como la aptitud de una máquina a cumplir su función, a ser transportado, instalado, puesta en marcha, mantenida, desmontada y puesta de nuevo en servicio en las condiciones de utilización normales especificadas de acuerdo con las instrucciones del fabricante, esto sin causar lesiones o efectos negativos sobre la salud. En términos de una probabilidad la seguridad es la probabilidad que el sistema evite hacer aparecer, en condiciones dadas, eventos críticos o catastróficos (Villemeur, 1988).

Es importante también hablar, desde luego, de fallas, pues de éstas se ocupa la Sdf. Una falla es un evento. Un evento está presente o no, así las fallas. El evento puede combinarse con otros eventos para producir eventos compuestos. La falla de una entidad es la consecuencia de la imperfección de ésta (imperfección intrínseca o debida a la de sus componentes). Según (CEI 50 (191), 1990) y (Villemeur, 1988]) una falla es: la cesación de la aptitud de una entidad a cumplir una función requerida. La figura 2 muestra la relación entre la falla y el estado de un componente o entidad (Chevalier *et al.*, 2004). Particularmente, los componentes electrónicos están sometidos a un estrés importante del ambiente que constituye la principal causa de fallas: humedad, vibración, temperatura, campo electromagnético, etc. El conocimiento de la fiabilidad o bien mejor dicho del índice de falla de los componentes es primordial para poder evaluar la SdF de una arquitectura material con la ayuda de métodos de análisis cuantitativo.

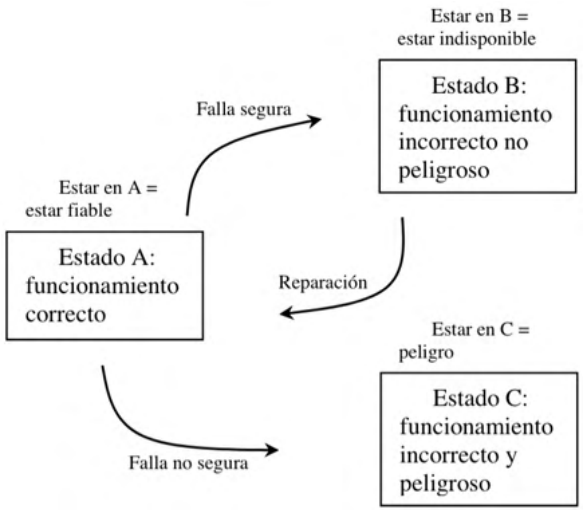

Figura 2. Relación entre la falla y el estado de un componente (Chevalier *et al.*, 2004).

Finalmente, los principales métodos desarrollados para evaluar la SdF de sistemas son: el árbol de eventos y el árbol de causas, árbol de fallas, el diagrama y redes de fiabilidad, la función de estructura de un sistema, los modelos de Markov, las redes de Petri, entre otros (Pérez, 2009).

LA FIABILIDAD DINÁMICA

Las herramientas clásicas de la SdF antes mencionadas no pueden tomar en cuenta los problemas que plantea la fiabilidad dinámica debido a que soportan, en general, una estructura invariante en el tiempo para el sistema y, además, no toman en cuenta el orden de ocurrencia de los eventos que conducen al estado de peligro (Labeau *et al.*, 2000). La complejidad matemática de la evaluación analítica de la SdF es tal que sólo es posible bajo ciertas hipótesis o cuando el sistema no es demasiado complejo. Otros métodos han sido propuestos, pero bajo ciertas hipótesis o restricciones: discretización de las variables físicas (Marseguera, 1995) o discretización de la variable tiempo (Kermisch, 2000). Éstas presentan dificultad en integrar en un solo proceso metodológico las interacciones entre las variables físicas continuas y la

ocurrencia de eventos debido a las fallas de los componentes o el cruce del umbral por las variables físicas continuas. En (Pérez *et al.*, 2015) se presenta una más amplia información sobre estos métodos, su tipo o clasificación.

La Simulación de Monte Carlo (SdMC) sería el único medio de evaluar la SdF de los sistemas híbridos complejos si herramientas informáticas adecuadas existieran. No hay, al menos que se tenga conocimiento, herramientas capaces para simular de manera simultánea la evolución discreta del sistema y su evolución continua tomando en cuenta los aspectos probabilísticos. En este contexto, se ha introducido el concepto del autómata estocástico híbrido y se ha desarrollado un método de simulación de Monte Carlo en el ambiente informático Scicos de Scilab. A la herramienta informática que permite efectuar una simulación de Monte Carlo con el fin de evaluar la fiabilidad de sistemas, modelados por el autómata estocástico híbrido, en contexto dinámico se le ha dado el nombre de *Dyrela* (Dynamic Reliability and Assessment, por sus siglas en inglés) (Pérez, 2010).

La *fiabilidad dinámica* es un concepto que ha sido necesario definir con el fin de evaluar de manera predictiva la SdF de sistemas dinámicos híbridos cuya estructura de fiabilidad evoluciona o cambia con el tiempo como consecuencia del cambio de estado continuo por la parte de control o por la naturaleza propia del sistema o por cambios externos al sistema, como fallas o errores humanos.

El principal objetivo de la fiabilidad dinámica es tomar en cuenta e integrar los siguientes aspectos:

- ✓ Las interacciones dinámicas existentes entre los parámetros físicos (representadas generalmente por variables continuas) y el comportamiento nominal o disfuncional de los componentes (representado generalmente por la ocurrencia de eventos).
- ✓ El carácter determinista o estocástico de los eventos y de las variables físicas.
- ✓ La estructura de fiabilidad que cambia en el tiempo (reconfiguración del modelo).
- ✓ Los modos de envejecimiento múltiples de los componentes según el estado discreto del sistema.
- ✓ Los modelos no binarios del comportamiento de los componentes.

El instante y el orden de ocurrencia de los eventos asociados a los cambios del estado discreto, los cuales están relacionados a las fallas de los componentes o al cruce de los umbrales de las variables continuas.

Se entiende por fiabilidad dinámica la evaluación previsional de la fiabilidad de un sistema en el cual la estructura fiabilista (lo que expresa cómo la falla del sistema depende de las fallas de sus componentes) evoluciona en el tiempo. Se puede decir en general que la "fiabilidad dinámica" es el problema de la evaluación probabilista de la falla de un sistema dinámico híbrido. Se le puede representar bajo la forma siguiente:

$$R_S(t) = P[S(X(T),Q(T),V(T)) = 1]_{0 \le T \le t} \quad (1)$$

Esta expresión (Pérez *et al.*, 2009) expresa que la fiabilidad $R_s(t)$ de un sistema no reparable se mide por la probabilidad que el sistema funciona durante un intervalo de tiempo *[0,t]*. *S* es la función de estructura del sistema que vale "1" si el sistema funciona y, "0", en caso contrario. $X(t)$ y $Q(t)$ son los vectores de estado continuo y discreto respectivamente, $V(t)$ es el vector de las variables aleatorias "estado de funcionamiento" de las componentes.

Con el fin de integrar los aspectos que demanda la fiabilidad dinámica y acceder, por simulación, a la evaluación predictiva de la SdF, un Autómata Estocástico Híbrido (AEH) ha sido formalmente definido sobre la base de

la teoría de los autómatas de estados finitos y sobre la teoría de los autómatas híbridos (Alur *et al.,* 1993), (Henzinger, 1996).

El Autómata Estocástico Híbrido (AEH) se define como (Pérez, 2009):

$$\text{AEH} = (\mathcal{X}, \mathcal{E}, \mathcal{A}, X, A, \mathcal{H}, \mathcal{F}, p, \mathcal{X}_o, \mathrm{x}_o, p_o) \quad (1)$$

en donde

X es un conjunto finito de estados discretos $\{x^1, x^2, \ldots, x^m\}$,

E es un conjunto finito de eventos $\{e_1, \ldots, e_r\}$ deterministas o estocásticos,

X es un conjunto finito de variables reales que evolucionan en el tiempo $\{x_1, \ldots, x_n\}$,

A es un conjunto finito de arcos de la forma *(x,e,*G,R,*x')* donde:

x y *x'* son los estados discretos origen y final del arco k, e_j es el evento asociado al arco, G_k la condición de guarda sobre *X* en el estado discreto x y R_k es la función de reinicio de *X* en el estado x',

$A: \mathcal{X} \times X \rightarrow (¡^{n+} \rightarrow ¡)$ es una función de "actividades", que asocia a un elemento de *X* x X una función definida sobre $¡^{n+}$ y a valores en ¡,

H es un conjunto finito de relojes sobre sur $¡^{n+}$,

$\mathcal{F}: \mathcal{H} \rightarrow (¡ \rightarrow [0,1])$ es una aplicación que asocia a cada reloj una función de repartición,

p_i^l es una distribución de probabilidades de transición de estado $p(x^i | x^l, e)$ sobre la ocurrencia de un mismo evento hacia dos estados discretos diferentes.

x^0, X_0 y p_i^0 corresponden respectivamente al estado discreto inicial, al valor inicial del vector de estado continuo en el estado inicial discreto y a la distribución inicial de probabilidades de transición en el estado inicial discreto.

La duración de buen funcionamiento y de reparaciones de los componentes son materializados por los relojes H. Estas duraciones son obtenidas por tiros aleatorios a partir de las funciones de repartición de probabilidad F. Los elementos *X, E* y *A* del AEH corresponden al autómata a estados finitos que definen su parte discreta. Por otro lado, *X, A,* R y G definen su parte continua. H corresponde a su aspecto temporal y finalmente F y *p* expresan su aspecto estocástico.

El AEH, implementado en un ambiente informático, está constituido de tres componentes: un autómata, un generador aleatorio y un descriptor de modos (figura 3). El AEH está constituido de *i* entradas situadas al lado izquierdo del bloque y sólo dos salidas ubicadas al lado derecho (figura 4). El autómata tiene tantas entradas como estados discretos existen en el sistema. La salida superior derecha del autómata proporciona el vector que contiene el estado discreto corriente x_i y el anterior $x_{[i-1]}$. La salida inferior aporta el vector de las variables de estado continuo *X* y sus derivadas. En la parte inferior del bloque del autómata se tiene una salida correspondiente a los eventos discretos *e*. Esta salida es activada cada vez que una transición se produce implicando un cambio de estado discreto en el sistema.

Con la ayuda del AEH se podrá realizar una SdMC del comportamiento funcional y disfuncional del sistema con el fin de acceder a la evaluación de los indicadores de la SdF. Para lograr esto, primeramente, se debe describir el comportamiento del sistema a través del AEH determinando los parámetros concernientes del autómata. Enseguida, se implementa el autómata en el ambiente informático creado para este fin. Posteriormente se efectúa la simulación de Monte Carlo. Finalmente, se efectúa el tratamiento estadístico con los datos obtenidos con el fin de determinar los parámetros correspondientes de la SdF.

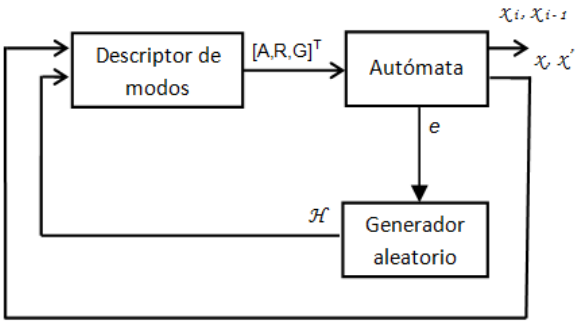

Figura 3. Estructura del autómata estocástico híbrido.

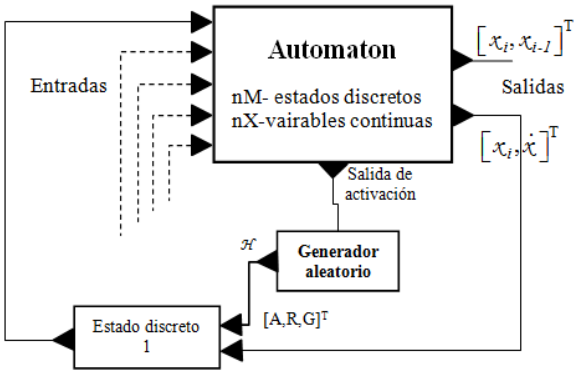

Figura 4. Implementación del AEH.

Dyrela ha sido aplicada a diferentes casos. Por citar algunos: evaluación de la seguridad de funcionamiento del sistema de regulación de la temperatura de un horno (Pérez et al., 2010), evaluación de la fiabilidad del mismo sistema, pero con variables dependientes (Pérez et al., 2009), por citar algunos.

Por último, la SdMC es un método basado en el tiraje de números aleatorios. La cantidad que se desea estimar corresponde a la esperanza matemática de una variable aleatoria. El principio consiste en estudiar la evolución de un sistema simulando un modelo genérico, representando el comportamiento del sistema en el curso de lo que se llamará escenario o historia. La cuantificación de la cantidad buscada, por ejemplo, la fiabilidad o la probabilidad de aparición de un evento no deseado está, entonces, basado sobre el estudio de un cierto número de escenarios diferentes, permitiendo extraer resultados estadísticos (estimadores). Par efectuar una estimación de la probabilidad de aparición de un evento no deseable, se puede asociar un estimador del tipo binario a esta probabilidad e incrementar un contador de una unidad por cada historia en la cual el evento se produce. La estimación de la probabilidad es, entonces, obtenida realizando el cociente entre el número de historias que han conocido un evento no deseable y el número total de historias (Labeau y Kermisch, 2001).

CONCLUSIÓN

La modelación de un sistema dinámico con el AEH permite evaluar los parámetros de la SdF aplicando una simulación de Monte Carlo. Se toman en cuenta las interacciones entre el funcionamiento y mal funcionamiento para una evaluación fina de estos parámetros del SdF. El AEH puede "pilotear" la simulación a pesar del comportamiento determinístico y estocástico. Faltan todavía tomar en cuenta varios aspectos: la influencia del tiempo en las leyes de probabilidad (envejecimiento, por ejemplo), leyes de control más complejas, la probabilidad de error del diagnóstico, la no linealidad en los modelos continuos, la dependencia entre variables continuas y estocásticas (fiabilidad del sensor vs. temperatura). Esto es el objeto de trabajos actuales.

REFERENCIAS

Alur, R., Courcoubetis C., Henzinger T. A., Ho P. H. (1993). Hybrid automata: an algorithmic approach to the specification and verification of hybrid systems. In Grossman R. L., Nerode A., Ravn A. P., Rischel H., editors, Hybrid Systems I, Lecture Notes in Computer Science 736, p. 209 – 229. Spinger-Verlag.

Campbell, S. L., Chancelier, J. P. and Nikoukhah, R. (2006). Modeling and Simulation in Scilab/Scicos. Springer.

CEI 50 (191) CEI 50 191. Vocabulaire Electrotechnique International, Chapitre 191 – Sûreté de fonctionnement et qualité des services – 1990.

Chevalier M., Garnier R., Chang P., Lusson B. La Sûreté de Fonctionnement. Intersections, le magazine Schneider Electric de l'enseignement technologique et professionnel. Novembre 2004.

EN 292 – 1, 1991. Sécurité de machines – Notions fondamentales, principes, généraux de conception – Partie 1 : Terminologie de base – Méthodologie – 1991.

Henzinger, T. A. (1996). The theory of hybrid automata. Proceedings of the 11th Annual IEEE Symposium on Logic in Computer Science (LICS), pp. 278 – 292.

Kermish, C. y P.E. Labeau. Approche dynamique de la fiabilité des systèmes. Projet 6/2000 de l'ISdF. *Tâche n°1 : établissement de l'état de l'art en fiabilité dynamique*. Université Libre de Bruxelles, 2000.

Labeau, P. E., C. Smidts y S. Swaminathan. Dynamic reliability: towards an integrated platform for probabilistic risk assessment. *Reliability Engineering and System Safety* 68, pp. 219-254, 2000.

Laprie J.-C., Arlat J., Blanquart J.-P., Costes A., Crouzet Y., Deswarte Y., Fabre J.-C., Guillermain H., Kaâniche M., Kanoun K., Mazet C., Powell D., Rabéjac C., Thévenod P. Guide de la Sûreté de fonctionnement. Cépaduès Éditions. 1995.

Marseguerra, M. and Zio, E. (1995). The cell-to-boundary method in Monte Carlo-based dynamic PSA. Reliability Engineering and System Safety 48, pp. 199-204.

Najafi, M. and Nikoukhah, R. (2007). Modeling Hybrid Automata in Scicos. Multi-conference on Systems and Control (MSC), Singapore, 1 – 3 October.

Perez, C. (2009). Evaluation par simulation de la sûreté de fonctionnement de systèmes en contexte dynamique hybride. Institut National Polytechnique de Lorraine – INPL. Thèse doctorale.

Pérez C., G. A., J.-F. Aubry y N. Brinzei. Modélisation d'un système par automate stochastique hybride pour l'évaluation de la fiabilité dynamique. *Journal européen des systèmes automatisés*, pp. 231-255, 2010.

Pérez, C., Aubry, J.-F. et Brinzei, N. (2010). DyRelA (Dynamic Reliability and Assessment. In 1st Workshop on DYnamic Aspects in DEpendability Models for Fault-Tolerant Systems, DYADEM-FTS 2010 in conjunction with European Dependable Computing Conference EDCC 8. Espagne.

Pérez, C., Méndez, G., Villano, A., Morales. Métodos para la evaluación de la fiabilidad de sistemas en contexto dinámico. Journal Academic Celaya 2015.

Smith D. J. Reliability, maintainability and risk. Practical methods for engineers. Sixth Edition. Butterworth Heinemann, 2001.

Villemeur, A. Sûreté de fonctionnement des systèmes industriels. Edition Eyrolles. 1988.