Confiabilidad en los Sistemas Tecnológicos

Dependability of technological systems

B. M. González Contrerasa, E. H. Fernández Martínezaa, F. Martínez. Solísb, J.V. Galaviz Rodríguezca Facultad de Ciencias Básicas Ingeniería y Tecnología, Universidad Autónoma de Tlaxcala, Calzada deApizaquito s/n, C.P. 90300, Apizaco, Tlaxcala, México. E-mail de contacto: brian.m.g@ieee.orgb Universidad Juárez Autónoma de Tabasco, Av. Universidad s/n, Zona de la Cultura, Col. Magisterial, Vhsa, Centro, Tabasco, Mex. C.P. 86040. Tel (993) 358 15 00. E-mail: fsolis@cenidet.edu.mxc Ingeniería en Mantenimiento Industrial/Ingeniería en Procesos y Operaciones Industriales, UniversidadTecnológica de Tlaxcala, El Carmen Xalpatlahuaya s/n, C.P. 90500, Huamantla, Tlaxcala, México. E-mail: galaviz_4@hotmail.com

PALABRAS CLAVE:

Confiabilidad, seguridad, sistemas tecnológicos, diagnóstico y detección de fallas, tolerancia a fallas.

RESUMEN

El avance tecnológico reciente se fundamenta en el progreso científico de áreas específicas de la ingeniería aplicada hacia el desarrollo de sistemas, tanto computacionales como electrónicos. Estos sistemas se interrelacionan de forma que permiten desarrollar aplicaciones tecnológicas de vanguardia, como lo son los sistemas embebidos y mecatrónicos. Un requisito fundamental en estos sistemas tecnológicos, es proporcionar a los usuarios confiabilidad en su funcionalidad y servicio, y al mismo tiempo, seguridad en su utilización. Este artículo presenta la descripción de los elementos que permiten proporcionar confiabilidad y seguridad a los sistemas tecnológicos que utilizan sistemas computacionales y/o electrónicos de forma sinérgica. Asimismo, se presentan los conceptos comunes del área de ingeniería en el desarrollo de sistemas tecnológicos desde la perspectiva de la confiabilidad y, finalmente, una propuesta para evaluar la confiabilidad desde la etapa de diseño.

KEYWORDS:

Dependability, safety, technological systems, fault detection and diagnosis, tolerance to faults.

ABSTRACT

Recent technological advance is founded on the scientific progress of specific engineering areas applied on development of computational and electronic systems. These systems are related each other leading to state-of-the-art technological applications such as in the mechatronics and embedded systems. A fundamental requirement in these technological systems is to provide functionality and service dependability to users, and at same time, safe use. In this paper, a description of elements that provide technological system dependability and safety is presented, where computational and electronic systems are included synergically, also the common concepts used in the engineering domain related to system development are presented from the dependability point of view. Finally, a proposal of dependability evaluation is introduced in order to be capable of to evaluate dependability from the design stage.

Recibido: 31 de julio del 2015 Aceptado: 21 de noviembre del 2015 • Publicado en línea: 29 febrero 2016

1 INTRODUCCIÓN

Uno de los primeros sistemas que presentaron tolerancia a fallas en su misma funcionalidad, fue el protocolo de control de transmisión conocido como TCP por sus siglas en inglés (Transmission Control Protocol) [1, 2], y establece la forma en cómo se transmite la información entre computadoras debido a que controla el flujo de la información en red (Internet, por ejemplo) [1]. En este protocolo se cuenta con dispositivos de control especializados denominados gateways (routers), que se encargan de enviar los paquetes de información a las computadoras. La ventaja del protocolo es que es descentralizado, y sobre todo, es tolerante a fallas, ya que ninguna otra parte de la red puede evitar que la información sea transferida en otras partes de la red. El sistema es, además, confiable, pues es robusto a incertidumbres en el tiempo de retardo cuando se realizan envíos de información entre computadoras. Por último, es importante mencionar que el protocolo considera una forma de retroalimentación (un lazo cerrado), que también verifica la fiabilidad de la transferencia de datos al incluir una secuencia de números asociados a cada pieza de información, para asegurar que ésta sea colocada en el orden correcto en su destino y, al mismo tiempo, detectar falta de información. Así la computadora receptora envía un paquete de confirmación de datos, con lo cual se cierra el lazo de control, de esta forma a falta de la confirmación, se reenvía la información. La transferencia de datos se verifica finalmente a través de una pieza de información, conocida como checksum, que verifica la computadora receptora para determinar si cada pieza de información no tiene errores. Este protocolo incorpora tolerancia a fallas, lo que asegura que sea confiable, siendo aun vigente, además de formar parte de los sistemas tecnológicos que utilizan comunicaciones por red. De alguna manera este protocolo utiliza los principios sobre confiabilidad que se ilustrarán en lo que resta del artículo.

Así como el ejemplo presentado anteriormente, los avances tecnológicos recientes dependen de la integración de sistemas complejos, los cuales resultan de una mezcla funcional de dispositivos dominados principalmente por la electrónica y el cómputo [2, 3, 4]. En el primer caso se habla de sistemas electrónicos: dispositivos que por su alto nivel de integración (de miles de transistores) permiten almacenamiento de información en un tamaño reducido para realizar acciones o funciones específicas complejas [5]. En el segundo caso, se consideran los sistemas computacionales: entidades de software y/o hardware que incluyen el procesamiento de la información de manera automática a través de ellos (la informática). De esta forma se integran los sistemas tecnológicos: aquellos que permiten realizar tareas automáticas, complejas y que facilitan la satisfacción de las necesidades del ser humano, produciendo bienes y servicios que mejoran su calidad de vida [3, 4, 5]. Los esfuerzos por lograr sistemas confiables y seguros inician en el área del cómputo electrónico a través de la eliminación de errores en el código, desde el inicio de la década de los 50s [6]. Por otro lado, el área electrónica también inicia tales esfuerzos para los componentes utilizados en sistemas de comunicaciones en la década de los 40s, enfocándose en aspectos de durabilidad de componentes [7]. Conforme convergen en el área computacional, los esfuerzos comienzan a ser comunes pues la sinergia entre ellos motiva mejoras de seguridad, costo, tiempo en el mercado, desempeño, tamaño, duración, consumo energético y flexibilidad, entre otros [8, 9].

El aumento en aplicaciones tecnológicas e industriales lleva al establecimiento de sistemas de seguridad crítica (donde la afectación a los seres vivos y el medio ambiente son los ejes principales), sistemas de costo crítico (donde el ahorro energético y por lo tanto económico es prioritario) y sistemas de volumen crítico (donde la capacidad y alta producción son prioridades) [7, 10, 11]. De entre los sistemas tecnológicos que han tenido mayor impulso, desarrollo, aplicación, avance y utilización destacan los denominados mecatrónicos [3] y embebidos [4, 5]. Si bien los sistemas mecatrónicos integran de manera sinérgica las disciplinas de ingeniería mecánica, eléctrica/electrónica, automatización y computación, los sistemas embebidos se refieren a los sistemas tecnológicos integrados por un sistema computacional (una computadora de propósito específico) que no es evidente para el usuario, pero que embebido en el sistema, gestiona la operatividad del mismo [4, 9].

En este artículo se presentan los atributos que permiten conferir de confiabilidad a un sistema tecnológico, haciendo hincapié en los de tipo embebido y mecatrónico por sus características de integración de dispositivos electrónicos y de cómputo, incluidos el software. Tomando en cuenta uno de los atributos, se propone una forma de evaluar la confiabilidad de un sistema tecnológico desde el punto de vista de control, considerando la fiabilidad de los macro componentes integrantes del sistema desde la etapa de diseño.

2 SISTEMAS TECNOLÓGICOS CONFIABLES

Las nociones presentadas en lo sucesivo son comunes en los sistemas tecnológicos indicados, debido a que se emplean los mismos conceptos, aunque en diferentes áreas, para describir los atributos de la confiabilidad. Las entidades componentes de tales sistemas pueden ser vistas como proveedoras de servicios y al mismo tiempo consideradas dentro de un lazo de control [2, 4, 12]. Esto es posible debido a que los sistemas mecatrónicos y embebidos funcionan en tiempo real por lo que, diferentes a un sistema de cómputo general, requieren retroalimentación bajo restricciones de tiempo de funcionamiento [12]. Asimismo, la metodología basada en el modelo-V [3, 4] que se muestra en la figura 1 a), se ha propuesto y se sigue utilizando muy a menudo en ambos tipos de sistemas. Este modelo proviene del área de computación siendo de utilidad para diseño de nuevas propuestas de software. En el caso de sistemas tecnológicos, se emplea para su diseño. Como se muestra, una vez definidos los requisitos, en cada una de las etapas subsecuentes de diseño (parte descendente del modelo) se considera el sistema completo y cada uno de los subsistemas; en la parte ascendente del modelo, la parte de integración, igualmente se considera el sistema global y los subsistemas. Teniendo esto en cuenta, las etapas diseño/integración toman en cuenta los subsistemas componentes del sistema, haciendo notar la importancia de inicio, en donde se definen los componentes principales del sistema visto como una integración de subsistemas o macro componentes que permitirán obtener un producto o servicio preliminar. El nivel de subsistemas será definido por los diseñadores dependiendo de las necesidades de fineza del sistema, así como la complejidad del mismo, como se ilustra en la figura 1 b).

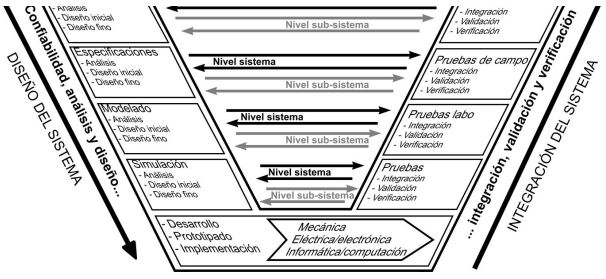
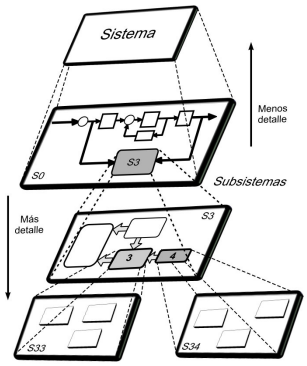


Figura 1. Fases de desarrollo para un sistema tecnológico: a) modelo v



b) definición de subsistemas.

En la fase de diseño se establecen los objetivos, aplicaciones, requisitos, funciones, estructura funcional, forma y comportamiento del sistema global. Para conferir al sistema de estos atributos, se requiere conocer también las amenazas a los mismos y la manera de manejarlas. Para ello se definen los conceptos siguientes que aplican para sistemas o subsistemas, si es que se consideran dentro de una sistema global realizando funciones específicas dentro del mismo (considere la figura 1 b)).

2.1 AMENAZAS DE LOS SISTEMAS TECNOLÓGICOS

Un error es una desviación entre el valor medido (o calculado) y el verdadero (especificado o teóricamente correcto). Se trata de una desviación del valor normal de lo esperado en el estado del sistema. Sólo ocurre en sistemas que procesan información (señales o datos). Suele asociársele a los equipos de cómputo y también ser de carácter software. Su causa es una o varias fallas, mientras que su consecuencia probable es provocar una avería cuando alcanza la interfaz del servicio.

Una falla es una desviación no permitida, a partir de una condición normal, de al menos una propiedad característica de un sistema (o subsistema) de manera que éste ya no puede satisfacer la función para la cual ha sido diseñado. Es por lo tanto una condición anormal que provoca la reducción o la pérdida de la capacidad de funcionamiento del sistema para realizar su función. La falla es el origen de los errores, las averías y los malos funcionamientos. Suele provocarse por medios físicos y propiciada por efectos ambientales así como el uso dado, de esta manera se conoce como falla interna. Si se trata de fallas provocadas por mal uso, defectos de diseño o desarrollo, se trata de fallas externas.

Un mal funcionamiento (o mal función) es una irregularidad intermitente de la capacidad de un sistema para realizar una función solicitada bajo condiciones específicas de operación, en consecuencia la entrega del servicio es intermitente.

El fallo o avería se refiere a la interrupción permanente de la capacidad de un sistema para realizar una función solicitada bajo condiciones específicas de operación. Es una desviación del valor normal de lo esperado, pero sobre todo impide la realización de la función del sistema y con ello ausencia del servicio.

Mayores detalles acerca de las amenazas pueden encontrarse en [2, 6, 7]. En sistemas tecnológicos tanto mecatrónicos como embebidos, al momento de integrar software con hardware, la probabilidad de presencia de errores y fallas se incrementa, por lo que debe de buscarse una manera de disminuir o atenuar esta probabilidad considerando los subsistemas antes y después de la integración de éstos. Debido a que los sistemas tecnológicos tienen una perspectiva orientada a productos [3, 4, 7], se consideran atributos que, al estar agregados en las etapas de desarrollo del producto/servicio, buscan disminuir las probabilidad de ausencia de servicio y con ello lograr un sistema tecnológico confiable.

2.2 CONFIABILIDAD EN SISTEMAS TECNOLÓGICOS: ATRIBUTOS

Cualitativamente descrita, la confiabilidad de un sistema tecnológico determina la propiedad/habilidad para proporcionar el servicio para el cual fue diseñado/construido y que al entregarse sea justificablemente de confianza, pues el usuario depende del servicio que se entrega para la realización de una actividad o función [2, 6, 7, 11]. El aseguramiento cuantitativo de la confiabilidad de un sistema tecnológico requiere tener valores adecuados de cantidades medibles denominadas atributos [2, 6, 11]: fiabilidad, disponibilidad, preservabilidad y seguridad. Los tres primeros son valores probabilísticos, mientras que el último es una propiedad relacionada al uso del sistema sin que provoque (o sea el mínimo) daño al usuario y el medio ambiente.

Se considera S=Sp P E P como el conjunto de todos los posibles estados que puede tener el sistema. Los conjuntos disjuntos Ss, Sf son respectivamente los estados en donde el sistema funciona correcta e incorrectamente, por lo que S=S U S con S={sp p E P} y S {s p pE Pf} con y . Igualmente se considera que los sistemas tienen un tiempo en funcionamiento definido como el tiempo de misión tm.Tomando en cuenta estas consideraciones se presentan los atributos de la confiabilidad.

Fiabilidad. Habilidad/propiedad de un sistema para realizar su función solicitada bajo ciertas condiciones, dentro de un alcance dado, durante un tiempo específico . Es un valor probabilístico dado por:

$$R(t) = Pr\left\{ s(t) \in S_s \middle| s(\tau) \in S_s \right\},\ \tau \in [0,t) \quad (1)$$

y se expresa como la probabilidad de que un sistema proporcione el servicio correcto en un tiempo >0. En términos prácticos su utiliza la función de tasa de fallo (o tasa de riesgo), , que representa la tasa instantánea de elementos que se averían respecto a los que siguen funcionando, así la fiabilidad queda expresada como:

$$R(t) = e^{\int_0^t \lambda(t)dt} \quad (2)$$

Apoyándose en la denominada distribución de Weibull [8] y considerando una tasa de fallo constante [7, 9], lo que es común en las especificaciones de software, equipo y componentes [10, 11], se tiene una representación de la fiabilidad regida por una ley exponencial de fallo , notándose que es un atributo que se pierde conforme pasa el tiempo y es afectada por las amenazas (fallas, errores, fallos). Debido a que se aplica también a los componentes o elementos integrantes de un sistema, indica el número de elementos que sobreviven respecto a un total inicial durante un periodo de tiempo. La forma de medir la fiabilidad es a través del recíproco de la tasa de fallo, el tiempo promedio de fallo (MTTF, en inglés), visto como el recíproco de la tasa de fallo (siempre y cuando sea constante):

$$MTTF = \int_0^\infty R(t)\,dt = \frac{1}{\lambda} \quad (3)$$

Esta medida aplica para elementos que no son reparables. Para el caso de elementos reparables se tiene el tiempo promedio entre fallos (MTBF, en inglés), esto permite utilizar (2) y (3) de forma alternativa.

Preservabilidad. Es la probabilidad de poder reparar el sistema. Incluye las diferentes funciones o actividades necesarias para mantener o restaurar un sistema a un estado aceptable u operacional. Supone la entrega del servicio en t>0 siempre que no se haya entregado el servicio en t=0.

$$M(t) = Pr\left\{ s(t) \in S_s \middle| s(\tau) \in S_f \right\},\ \tau \in [0,t) \qquad (3)$$

Al tener un alto valor de preservabilidad se tendrá un tiempo muerto bajo de operación del sistema. Se relaciona al tiempo esperado para que se recupere el sistema de una falla o fallo y está definido por el tiempo promedio de reparación o recuperación (MTTR en inglés), siendo también un valor probabilístico dado por

$$MTTR = \int_0^\infty \left(1 - M(t)\right) dt$$

Disponibilidad. Es la probabilidad de encontrar el sistema en su estado operacional en algún tiempo en cualquier momento. Es un valor que es de mayor importancia para el usuario del sistema. Se calcula a través de

$$A(t) = Pr\left\{ s(t) \in S_s \middle| s(\tau) \in S \right\},\ \tau \in [0,t) \qquad (5)$$

Pero puede obtenerse a través de los atributos precedentes como

$$A(t) = \frac{MTTF}{MTTF + MTTR} \qquad (6)$$

Seguridad. Habilidad de un sistema para evitar daño a las personas, los equipos o el ambiente en presencia de una falla (y sus consecuencias). La seguridad puede considerarse como un estatus donde el riesgo es mínimo y es una consecuencia de utilizar valores altos de los anteriores.

3 TOLERANCIA A FALLAS

La tolerancia a fallas (TF) define la capacidad del sistema tecnológico a seguir proporcionando el servicio aun en presencia de fallas, es decir, mantener funcional el sistema mientras contiene las consecuencias de fallas/fallos [13, 14, 15]. La tolerancia a fallas requiere y explota la redundancia y mientras mejor se gestione ésta, será más efectiva. Puede denominarse una técnica de ejecución que permite proveer de confiabilidad al sistema, pues incrementa su fiabilidad global. La tolerancia puede lograrse a través de dos formas: incorporando arquitecturas tolerantes a fallas o incorporando un sistema de control tolerante a fallas (SCTF). La primera se fundamenta en proporcionar el servicio replicando operaciones/funciones, mientras que la segunda se fundamenta en mantener márgenes de estabilidad del sistema en presencia de fallas y, al mismo tiempo, mantener un desempeño aceptable del sistema. En ambos casos se busca lograr un sistema confiable a través de la integración de unidades tolerantes a fallas (UTFs) [2, 15]. Las UTFs requieren de métodos superiores de monitoreo para poder establecer la condición funcional en la que se encuentran.

Los métodos superiores (avanzados) de monitoreo son aquellos métodos que aprovechan las mediciones del sistema (entradas y salidas) para incorporarlos en descripciones analíticas que permitan determinar fallas en los componentes del sistema [8, 10, 11]. A través de ellos se procesa información para definir acciones sobre el sistema. En estos métodos se considera el uso de un módulo denominado de detección y aislamiento/diagnóstico de fallas (FDI/FDD, por sus siglas en inglés) [10, 11, 13]. Este módulo determina si un componente del sistema está fallando, de esta forma, se activan las acciones de mantenimiento en cuanto a reemplazo/corrección de componentes (sistemático o correctivo según sea el caso, en donde interviene un agente externo al sistema).

Las fallas afectan a los tres componentes principales de todo sistema tecnológico, sea tangible o intangible [12, 13, 14]:

1.- Sensores: son los componentes del sistema que le permiten percibirse y percibir el entorno.

2.- Actuadores: son los componentes del sistema que le permiten interactuar con su entorno.

3.- Estructura del sistema: el comportamiento del sistema en términos de entradas-salidas.

Todo sistema que incorpore acciones en tiempo real puede trasladarse a una forma funcional de tipo retroalimentada para realizar un análisis desde el punto de vista de control [12, 15], así los atributos presentados pueden tomarse en cuenta en la fase de diseño para el análisis de componentes y considerar niveles de fiabilidad que puedan mejorar la fiabilidad del sistema global final. Tomando en cuenta lo anterior, una UTF consiste de un sub-sistema que proporciona uno de los tres niveles de tolerancia a fallas que se describen a continuación.

3.1 NIVELES DE TOLERANCIA A FALLAS

Para definir la capacidad tolerante a fallas de un sistema, se tienen tres niveles de TF [2, 14, 15]:

a)Nivel de fallo-operacional (FO): la UTF mantiene el sistema en operación y proporcionando el servicio a pesar de la falla (o error) que pudiera derivar en un fallo. Mantiene de esta forma la fiabilidad y seguridad del sistema. El objetivo es mantener la funcionalidad aun con un desempeño degradado, pues el servicio del sistema no debe interrumpirse.

b)Nivel de fallo-seguro (FS): en presencia de una o más fallas/fallos, la UTF busca alcanzar un estado de seguridad del sistema y así seguir funcionando de forma nominal hasta culminar la entrega del servicio antes de aplicar mantenimiento correctivo.

c)Nivel de fallo-apagado (FA): se refiere a cesar el funcionamiento del sistema en presencia de una o más fallas/fallos para evitar daños irreparables o afectaciones a la seguridad: es preferible que no haya servicio. Igualmente, a nivel componente, éste se apaga o desactiva antes de que influya sobre otro(s).

El uso de las UTFs se explota en esquemas denominados tolerantes a fallas que pueden definirse en arquitecturas o en sistemas de control, como se explican enseguida.

3.2 ARQUITECTURAS TOLERANTES A FALLAS

Las arquitecturas manejan la redundancia de los componentes, unidades o sub-sistemas que integran a los sistemas tecnológicos, a estos se les denomina módulos. Los módulos son redundantes pues se conectan uno o más en paralelo. La ventaja de hacer esto es explotar la fiabilidad que se logra para sistemas en paralelo [2, 6, 16]. Para el caso de qS subsistemas conectados en serie se obtiene una fiabilidad total por medio de (7):

$$R_S(t) = \prod_{i=1}^{q_S} R_i(t). \tag{7}$$

Para el caso de qP subsistemas en paralelo, la fiabilidad total se obtiene con el uso de (8):

$$R_P(t) = \prod_{j=1}^{q_P} (1 - R_j(t)) \tag{8}$$

Los esquemas redundantes normalmente requieren subsistemas en paralelo y pueden diseñarse para hardware, software, procesamiento de información y dispositivos mecánicos y eléctricos, es decir, los que integran a los sistemas tecnológicos. Tales esquemas proporcionan al sistema de niveles FS y FO. En la etapa de diseño debe considerarse alguna de estas arquitecturas para preparar el prototipo del sistema hacia lo que será un funcionamiento continuo y listo para pruebas (parte de prototipado) [3]. Mayores detalles acerca de los tipos de arquitecturas tolerantes a fallas se presentan y explican en [6, 7, 11].

3.3 SISTEMAS DE CONTROL TOLERANTE A FALLAS (CTF)

Los SCTF incorporan un control avanzado que permite reaccionar ante las fallas presentes en un sistema tecnológico. Según la forma en que reaccionan ante las fallas, pueden ser activos o pasivos.

3.3.1 TOLERANCIA ACTIVA

La TF en estos sistemas se logra considerando un ajuste en tiempo real del lazo de control. Se trata de una UTF que se compone principalmente de tres elementos [12, 14, 15]:

- Un control reconfigurable
- Un módulo FDI o un módulo FDD
- Un mecanismo de reconfiguración

Pueden proporcionar los tres niveles de TF pues son capaces de reaccionar a una gran cantidad de fallas de ciertas magnitudes, que, al ser sobrepasadas, entran en el nivel FA.

3.3.2 TOLERANCIA PASIVA

La UTF en este caso no requiere monitoreo continuo del sistema para determinar el estado de las fallas, es decir, los módulos FDD/FDI no son necesarios, por lo que tienen un nivel de autonomía mayor respecto a un SCTF activo. La TF en estos SCTF se logra considerando un conjunto de fallas bien definido ante las cuales un controlador general define una ley de control robusta con suposición de efectos de las fallas en el sistema. Los niveles que logra son FO y FS de forma global.

3.3.3 ESQUEMAS FUNCIONALES

En la etapa de diseño se requiere, en muchas ocasiones, un modelo funcional del sistema que represente su dinámica. Una manera apropiada y relativamente sencilla es conforme a la perspectiva de control. Un sistema en tiempo real (un sistema tecnológico, como se ha indicado) siempre puede ser considerado bajo esta forma. Es conveniente bajo esta descripción definir la forma en que se gestionan las fallas en componentes de tipo sensores y de tipo actuadores. Se considera el siguiente modelo lineal continuo de parámetros constantes que refleja el estado y dinámica del sistema:

$$\begin{cases} \dot{x}(t) &= Ax(t) + \sum_{i \in I} B_i u_i(t) \\ y(t) &= \sum_{j \in J} C_j \hat{x}_j(t), \end{cases} \qquad (9)$$

donde A E [] xn es la matriz de estado, B E [] es la matriz de entrada asociada a los actuadores u (t) y C E [] xn es la matriz de salida asociada a los sensores y(t) E [] m , es por ello que se define el estimado del estado x(t) E[]n como x(t) , que puede provenir de un observador. En el caso de que las señales de interés estén disponibles a través de mediciones x(t)= x(t). El conjunto I caracteriza el conjunto de actuadores disponibles de forma nominal, donde u(t)=E[] es la entrada del actuador i E I con

$$r = \sum_{i \in I} r_i \quad .$$

En el caso de los sensores se tiene similarmente un conjunto J que caracteriza el conjunto de sensores disponibles de forma nominal, x j (t) E [] es la salida del sensor j E J con $m = \sum_{j \in J} m_j$.

Considerando fallas en los actuadores (el caso de sensores es similar y por ello se omite), cuando aparecen después del tiempo tf (tiempo de aparición de la falla) se tienen dos sub-conjuntos: el de los actuadores sin falla I N y con falla IF . Por lo tanto I= IN U IF . Bajo la nomenclatura propuesta, se tiene que sin falla en el conjunto

$$I(t) = I_N(t), I_F(t) = \varnothing, \qquad (10)$$

sY al momento de aparición de una falla, para elementos del conjunto I se transfieren al conjunto , en $I_F, I_F(t) \neq \varnothing$ consecuencia.

$$I(t) = I_N(t) \rightarrow I(t) = I_N(t) \cup I_F(t). \qquad (11)$$

La TF puede integrarse al sistema de control como una reacción contra las fallas o bien, como otra condición/restricción que debe considerarse al inicio como una situación extrema de funcionamiento (desde la etapa de diseño). Enseguida se presenta una forma de incluir los conjuntos (10) y (11) dentro de las posibles configuraciones que se pueden tener considerando que algunos de los actuadores puede fallar, de forma que se determine la fiabilidad global considerando las opciones según la redundancia dada al sistema.

3.3.4 ANÁLISIS PARA DIAGRAMA DE BLOQUES DE FIABILIDAD

En este trabajo se considera que la estructura del sistema puede modelarse como indica (9) con atención especial a los actuadores, pues la redundancia es sobre las acciones sobre el sistema. El caso de sensores puede trabajarse utilizando redundancia analítica o virtual, lo que no puede hacerse con actuadores [9, 10, 15]. La propuesta presentada toma en cuenta el modelo (9), donde la matriz B se describe como B=[b1,b2,b...] bi E Rn. Como se trata con redundancia, los macro componentes del sistema global se consideran como la fiabilidad de cada uno de ellos para obtener la fiabilidad global Rg (t)=f(R1(t)R2(t)...R(T) formándose las siguientes sub-estructuras Lk k=1....n, , siendo nL las estructuras válidas diferentes de cero. La controlabilidad se obtiene para cada combinación de componentes en donde intervienen los actuadores como indica (12):

$$\mathsf{L}_k = \{R_i\} : rank\left[ctrl\left(A, [\rho_1 b_1, \rho_2 b_2, \ldots, \rho_r b_r] \right) = n \right], \; i = 1, \ldots, r \qquad (12)$$

Donde ctrl indica que se debe encontrar la matriz de controlabilidad de la dupla indicada considerando los factores:

$$\begin{cases} \rho_1 = 0, \text{ el } i\text{-ésimo actuador no se considera en } \mathsf{L}_k \\ \rho_1 = 1, \text{ el } i\text{-ésimo actuador se considera en } \mathsf{L}_k \end{cases} \qquad (13)$$

para poder conformar la dupla necesaria de la matriz B modificada sin considerar las columnas indicadas para la obtención de tal matriz. Como puede observarse, las estructuras obtenidas definen los conjuntos válidos en términos de mantener controlable el sistema. Considerando arreglos en serie, paralelo y sus combinaciones [17], las estructuras se ordenan de forma que se obtiene la fiabilidad global utilizando la fórmula de Poincaré para fiabilidad de redes de sistemas complejos [17]:

$$R_g(t)=\sum_{j=1}^{n_L}\prod_{i\in L_j}R_i(t)-\sum_{j=2}^{n_L}\sum_{k=1}^{j-1}P(L_k\cap L_j)+\cdots+(-1)^r P(L_1\cap\cdots\cap L_r),\ P(L_k\cap L_j)=\prod_{i\in(L_k,L_j)}R_i(t) \tag{14}$$

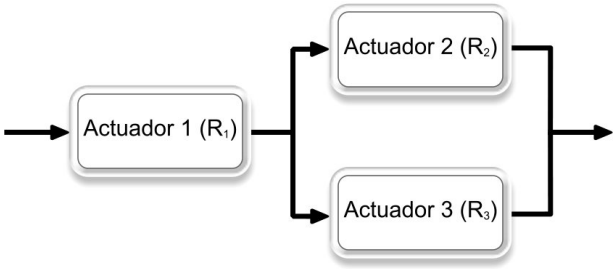
Con (13) se calcula la fiabilidad global del sistema manteniendo la controlabilidad del sistema según la redundancia de la que esté provisto el sistema a través de los subsistemas, vistos desde la perspectiva de los actuadores. De esta forma se tiene una manera de calcular la fiabilidad global del sistema en términos de mantener la controlabilidad del sistema según la redundancia de la que esté provisto el sistema a través de los subsistemas, en este caso vistos desde la perspectiva de los actuadores.

4. EJEMPLO ACADÉMICO

Considere el sistema definido por las matrices dadas en (15) correspondientes al modelo (9):

$$A=\begin{bmatrix} -3 & 0.1 & 0.1 & 0 & -10 & 0 & 0\\ 0 & -1 & 0 & -20 & 0 & 0 & 0\\ 0.1 & 0.2 & -0.2 & 0 & 2 & 0 & 0\\ 0 & 1 & 0 & -1 & 0 & 0 & 0\\ 0.02 & 0 & -1 & 0 & -1 & 0.3 & 0\\ 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},\ B=\begin{bmatrix} -50 & 0 & 1\\ 0 & -30 & 4\\ -0.9 & 0 & 0\\ 0 & -0.1 & 0\\ 0.1 & 0 & 0\\ 0 & 0 & -2\\ 0 & 0 & 1 \end{bmatrix},\ C=I_7 \tag{15}$$

Usando (12)-(13) se obtienen los subconjuntos:L1={R1,R2,R3} L1={R1,R2} L1={R1,R2,} con nL=3. La fiabilidad global queda definida, usando (14), como Rg(t)= R1(t)R3(t)+ R1(t)r2(t)-R1(t)R2(t)R3(t). El diagrama de bloques de fiabilidad que muestra la conexión entre subsistemas, obtenido a partir del uso de (7)-(8) y el resultado para Rg, se muestra en la figura 2.



m Figura 2. Diagrama de bloques de fiabilidad para el ejemplo

El diagrama de bloques de fiabilidad muestra claramente que hay redundancia en las acciones realizadas por los actuadores 2 y 3, por lo que si alguno de ellos llegará a fallar, el otro realizaría la actividad solicitada.

5 DISCUSIÓN Y CONCLUSIONES

5.1 DISCUSIÓN

La evaluación de la fiabilidad desde la etapa de diseño, tomando como metodología de desarrollo el modelo-V (Fig. 1), permite incorporar uno de los atributos que permiten definir la confiabilidad del sistema tecnológico por desarrollar. Esto incrementa la seguridad del mismo, además de asegurar que el funcionamiento del prototipo soporte la realización de mayores pruebas de funcionamiento para definir su pertinencia en la etapa final de desarrollo. El ejemplo presentado muestra una forma sencilla de evaluar la fiabilidad cuando se cuenta con una descripción dinámica del sistema a través del espacio de estados, si no fuera el caso, se utilizan las técnicas clásicas de fiabilidad para sistemas serie-paralelo [7, 13].

5.2 CONCLUSIONES

Se presentó en este artículo, un panorama general acerca de la confiabilidad de los sistemas tecnológicos, entre los que destacan los embebidos y los mecatrónicos.

Todo sistema tecnológico puede ser visto como una entidad que genera un servicio al usuario final y el garantizar que el servicio se tenga en tiempo y forma cumpliendo específicas características es el objetivo de la confiabilidad. Al asegurar la confiabilidad de un sistema tecnológico se mejora al mismo tiempo la seguridad en el uso del mismo. Se propuso una forma de determinar la forma en que se conectan los subsistemas, considerando una representación en el espacio de estados del sistema con redundancia material de tipo actuadores. A través de esta propuesta puede determinarse la redundancia estructural del sistema global y la fiabilidad que se tendría. Se presentó un ejemplo para ilustrar una forma de determinar la fiabilidad de un sistema visto como un sistema de control a través del modelo en el espacio de estado, para obtener el diagrama de fiabilidad y poder determinar su fiabilidad global.

REFERENCES

1. Richard D. Braatz. The "Nobel Prize in Engineering" Awarded for the Design of a Feedback Control System. IEEE Control Systems Magazine. 2013, 33 (5), 6-7.
2. Buja, G., Menis, R. Dependability and Functional Safety, IEEE Industrial Electronics Magazine. 2012, 18, 4-12.
3. Bradley, D. Mechatronics – More questions than answers. Mechatronics. 2010, 20, 827–841.
4. Ibrahim, A.M. Fuzzy Logic for Embebbed Systems Applications. New Yotk, USA: Newnes, 2004.
5. Tummala, R. R. SOP: what is it and why? A new microsystem-integration technology paradigm-Moore's law for system integration of miniaturized convergent systems of the next decade. Advanced Packaging, IEEE Transactions on. 2004, 27(2): 241-249.
6. Avizienis, A., Laprie, J.-C., Randell, B., Landwehr, C. Basic Concepts and Taxonomy of Dependable and Secure. Computing. IEEE Transactions on Dependable and Secure Computin., 2004, 1 (1), 11-33.
7. Murthy, D., Østerås, T., Rausand, M. Component reliability specification. Reliability Engineering and System Safety. 2009, 94, 1609-1617.
8. Isermann, R., Fault-diagnosis applications. Model-based condition monitoring: Actuators, drives, machinery, plants, sensors, and fault-tolerant systems. USA: Springer, 2006.
9. M. Schlett, Trends in Embedded Microprocessor Design. IEEE Computer. 1998, 31(8), 44-49.
10. Ding, S. X. Model-based Fault Diagnosis Techniques. Design Schemes, Algorithms, and Tools. Berlin: Springer, 2008.
11. Isermann, R., Fault-diagnosis systems: An introduction from fault detection to fault tolerance. Berlin: Springer, 2006.
12. Kopetz, H. Real-Time Systems: Design Principles for Distributed Embedded Applications, New York: Springer, 2011.
13. Zhang, Y., Jiang, J. Bibliographical review on reconfigurable fault-tolerant control systems. Annual Reviews in Control. 2008, 32, 229-252.
14. Jiang, J. Fault-tolerant control systems. An introductory overview. Acta Automatica Sinica, 2005, 31 (1), 160-174.
15. Blanke, M., Kinnaert, M., Lunze, J., Staroswiecki, M. Diagnosis and Fault-Tolerant Control, Berlin: Springer, 2006.
16. Li, H.; Zhao, Q. & Yang, Z. Reliability modeling of fault tolerant control systems, International Journal of Applied Mathematics and Computer Sciences. 2007, 17, 491-504.
17. Fateh Guenab, Contribution aux systems tolerant aux défauts : Synthèse d'une méthode de reconfiguration et/ou de restructuration intégrant la fiabilité des composants, Tesis de doctorado, Nancy Université, 2007.

Acerca de los autores

Brian Manuel González Contreras es Ingeniero Eléctrico, con Maestría en Ciencias en Ingeniería Electrónica con especialidad en control automático (CENIDET, Morelos, México). Es Doctor en Control Automático, Procesamiento de Señales e Ingeniería Informática (Universidad Henri Poincaré – Université de Lorraine, Nancy, Francia). Es profesor-investigador del Programa Educativo de Ingeniería en Sistemas Electrónicos de la Universidad Autónoma de Tlaxcala. Ha participado en diversos proyectos nacionales e internacionales, entre los que destacan: diseño de alimentación eléctrica en alta y baja potencia para subestaciones eléctricas de CFE en Minatitlán, Veracruz; diseño del SCADA para PEMEX de la red nacional de refinación, en ciudad de México; diseño de sistemas de control seguros y confiables para la compañía Neste-Jacobs Oy, en Finlandia. Sus líneas actuales de investigación consideran: el modelado de sistemas, la detección y diagnóstico de fallas, el control tolerante a fallas, sistemas confiables y seguros, así como la identificación/modelado de sistemas industriales.

Fermín Martínez Solís, es Ingeniero en Electrónica egresado del Instituto Tecnológico de Apizaco, Maestro en Ciencias de la Electrónica egresado de la Benemérita Universidad Autónoma de Puebla, y con Doctorado en Ciencias en Electrónica realizado en el Centro Nacional de Investigación y Desarrollo Tecnológico (CENIDET). Actualmente es profesor investigador en la Universidad Juárez Autónoma de Tabasco. Tiene experiencia en investigación y diseño de sistemas electrónicos para medición, control y automatización de procesos industriales. Además de modelado, simulación y control de sistemas robóticos y mecatrónicos ha trabajado en diseño de prótesis inteligentes, biomecánica de extremidades inferiores y cinemática de la marcha humana. Sus áreas de interés son: diseño e implementación de tarjetas de adquisición de datos, sistemas robóticos y mecatrónicos; automatización industrial y control de procesos, así como la investigación y desarrollo de equipos para rehabilitación.

E. H. Fernández Martínez, es profesora de la licenciatura en Ingeniería Química en la Facultad de Ciencias Básicas Ingeniería y Tecnología de la Universidad Autónoma de Tlaxcala desde el año 2009 a la fecha; algunas de las materias impartidas son: operaciones unitarias, ingeniería química i, mecánica de fluidos, programación y métodos numéricos, fisicoquímica I, II y III. Candidato a doctor por la Universidad Autónoma de Tlaxcala en el área de procesos de separación, específicamente en el diseño de columnas de destilación. Estudios de maestría en el Instituto Tecnológico de Celaya y de licenciatura en ingeniería química por la Universidad Veracruzana. Presentaciones de trabajos internacionales, de trabajos en extenso a nivel nacional en el AMIDIQ (Asociación Mexicana de Investigación y Docencia en Ingeniería Química) y publicaciones nacionales. Presidente de la sección Tlaxcala del Instituto Mexicano de Ingenieros Químicos.

José V. Galaviz Rodríguez, realizó estudios de Ingeniería industrial en producción y tiene un Doctorado en planeación estratégica y dirección de tecnología por parte de la Universidad Popular Autónoma del Estado de Puebla (UPAEP), así como una Maestría en Ingeniería administrativa. Es evaluador del RCEA-07-26884-2013 en el área 7 de Ingeniería e Industria del Sistema Nacional de Evaluación Científica y Tecnológica del CONACYT. Es responsable del cuerpo académico "Ingeniería en Procesos en Consolidación" UTTLAX-CA-2, así como integrante de la Red Temática Modelado y Automatización de Procesos. Poseedor del Perfil Deseable por tres convocatorias consecutivas del PRODEP. Ha publicado artículos científicos arbitrados/indexados a nivel internacional (India, Colombia, Polonia, EUA y Austria). Es autor y coautor de cuatros libros a nivel internacional editados por Palibrio. Actualmente es profesor investigador de T.C. Titular "B" en la Carrera de Ingeniería en Mantenimiento Industrial e Ingeniería en Procesos y Operaciones industriales en la Universidad Tecnológica de Tlaxcala.