CONTROL TOLERANTE A FALLOS (PARTE II): MECANISMOS DE TOLERANCIA Y SISTEMA SUPERVISOR [1]

Vicenç Puig, Joseba Quevedo, Teresa Escobet, Bernardo Morcego, Carlos Ocampo

Departament Enginyeria de Sistemes, Automàtica i Informàtica Industrial (ESAII) - Campus de Terrassa
Universitat Politècnica de Catalunya (UPC)
Rambla Sant Nebridi, 10. 08222 Terrassa (Spain)
e-mail: *{vicenc.puig, joseba.quevedo, teresa.escobet, bernardo.morcego, carlos.ocampo}@.upc.es*

Resumen: Los procesos industriales gobernados mediante controladores automáticos pueden presentar fallos. Una forma de aumentar su fiabilidad consiste en dotarlos de mecanismos de tolerancia frente a los mismos. El diseño de sistemas de control tolerante a fallos es una área emergente en control automático que aglutina diversas disciplinas y áreas teóricas que tienen como objetivo alcanzar esta nueva funcionalidad. La tolerancia a fallos se puede obtener mediante el diagnóstico en tiempo real de los mismos, y mediante el envío de una señal de tipo evento discreto a un sistema supervisor una vez el fallo ha sido detectado, aislado y estimada su magnitud. A su vez el sistema supervisor activará los mecanismos de acomodación/reconfiguración para continuar, si es posible, controlando el sistema en fallo. En este artículo se presentan los mecanismos de tolerancia que se pueden activar una vez se ha diagnosticado el fallo así como una arquitectura del sistema supervisor necesario para su implementación real. Finalmente, se presentará la aplicación de algunos de los mecanismos de tolerancia presentados en una aplicación real basada en el control global de la red de alcantarillado de Barcelona.

Keywords: Control tolerante, diagnóstico de fallos, detección de fallos, acomodación al fallo, reconfiguración del controlador.

1. INTRODUCCIÓN

El concepto de control tolerante (Zhang, 2003) nace hace unos 20 años de la mano del control tolerante a fallos de aviones (llamado en esa época "restructurable or self-reparing fligth control"), si bien a nivel científico aparece más tarde como un objetivo básico en el primer congreso de IFAC SAFEPROCESS de 1991 y sobretodo se desarrolla con gran fuerza desde el inicio del siglo XXI. El control tolerante trata del diseño e implementación de sistemas de control de procesos industriales proclives a que se produzcan funcionamiento incorrecto ya sea en sensores, actuadores, controladores, o componentes del procesos durante su operación. Para ello se trata de tener en cuenta

[1] Trabajo subvencionado por la CICYT del Ministerio de Ciencia y Tecnología Español (DPI2002-0350) y por la DGR de la Generalitat de Catalunya (grupo SAC2001/SGR/00236).

a la hora de diseñar e implementar el sistema de control una situación en que se produzcan fallos en el mismo. En un entorno industrial ésta es una situación realista ya que los procesos industriales crecen en complejidad, aumentan el número de variables y parámetros que se miden y de actuadores que se accionan automáticamente en tiempo real y en consecuencia aumenta el grado de probabilidad de aparición de fallos.

Tal como se ha presentado en un artículo anterior, en la bibliografía se consideran dos tipos de control tolerante a fallos: el ***control pasivo*** y el ***control activo***. El primero de ellos, utiliza la propiedad que tienen los sistemas realimentados de hacer frente a perturbaciones, cambios en la dinámica del sistema e incluso fallos en el mismo. Un cambio inesperado en el sistema crea un efecto sobre el mismo que se transmite al sistema de control que a su vez trata de compensarlo de forma más o menos rápida. En este sentido, el control tolerante pasivo consiste en un diseño robusto del sistema de control realimentado para hacerlo inmune a determinados fallos (Patton, 1997). Sin embargo, la teoría de control robusto muestra que sólo existen controladores robustos para una clase reducida de cambios en la dinámica del sistema provocados por los fallos. Además, un controlador robusto funciona de forma subóptima para la planta nominal puesto que sus parámetros se han obtenido mediante un compromiso entre prestaciones y robustez para toda la familia de plantas considerada, incluyendo los posibles fallos. Por otro lado, el ***control tolerante activo*** consiste en el ***diagnóstico*** en línea del fallo, es decir, en determinar el componente averiado, el tipo de avería, su tamaño e instante de aparición y, a partir de dicha información, activar algún mecanismo de acomodación del mismo o de reconfiguración del control o incluso dependiendo de la gravedad la parada el sistema. Este enfoque exige disponer de un sistema de diagnóstico de fallos que, en tiempo real, pueda dar información a un sistema ***supervisor*** para que active algún mecanismo de acción correctora (Blanke, 2003).

La estrategia de tolerancia a aplicar depende del componente del lazo de control que se vea afectado por el fallo. En primer lugar, si el proceso controlado dispone de redundancia física, más de un componente (sensor, actuador, elemento del proceso) para realizar la misma función, entonces la estrategia de tolerancia consistirá simplemente en sustituir el componente en fallo por otro igual que funcione bien. Esta estrategia es costosa ya que supone duplicar o triplicar los componentes críticos de un proceso controlado y no siempre es posible incorporarlos físicamente en un espacio reducido.

En el caso de que no exista redundancia física, distinguiremos entre fallos en sensores, actuadores y en la propia planta. Para acomodar fallos en sensores se suelen utilizar los denominados ***sensores virtuales*** que se basan en la estimación de la medida del sensor en fallo a partir del resto de sensores existentes en el sistema. Para acomodar fallos en actuadores y/o la propia planta se opta por el rediseño de controladores, utilizándose, principalmente, dos mecanismos: la ***acomodación al fallo*** y la ***reconfiguración***, según se cambie la ley o la estructura de control, respectivamente (Blanke, 2003).

La incorporación de mecanismos de control tolerante en el lazo de control depende fuertemente del tipo de control utilizado (Puig, 2001). Así, por ejemplo, existen estrategias de control como el control predictivo que, simplemente añadiendo nuevas restricciones al problema de optimización, permiten fácilmente incorporar mecanismos de tolerancia a fallos (Maciejowski, 2001).

Debido a que la aparición de fallos en el sistema y la activación de mecanismos de tolerancia se pueden modelar como eventos discretos en el tiempo que provocan cambios en el comportamiento dinámico continuo del sistema, los sistemas de control tolerantes son de naturaleza ***híbrida***. Por lo tanto, para el análisis y diseño de controladores tolerantes se deberán utilizar técnicas que se están desarrollando para sistemas híbridos (Cassandras, 1995), (Morari, 2003).

La estructura del artículo es la siguiente: en la *Sección 2* se presentará una revisión de los mecanismos de tolerancia a fallos existentes. En la *Sección 3* se presentará el sistema supervisor necesario para activar los mecanismos de tolerancia una vez ha sido diagnosticado el fallo. En la *Sección 4* se presentará una aplicación de algunas de los mecanismos de control tolerante a un sistema de control real: el sistema de control de la red de alcantarillado de Barcelona. Y, finalmente, en la *Sección 5* correspondiente a las conclusiones se presentarán las características más relevantes del control tolerante a fallos.

2. CLASIFICACION DE LOS MECANISMOS DE TOLERANCIA A FALLOS

Dentro de un lazo de control tolerante se puede considerar que existe tolerancia a fallo al contar con:

- Mecanismos que introducen redundancia en los sensores y/o actuadores.
- Estrategias de adaptación de la ley de control que gobierna el lazo.

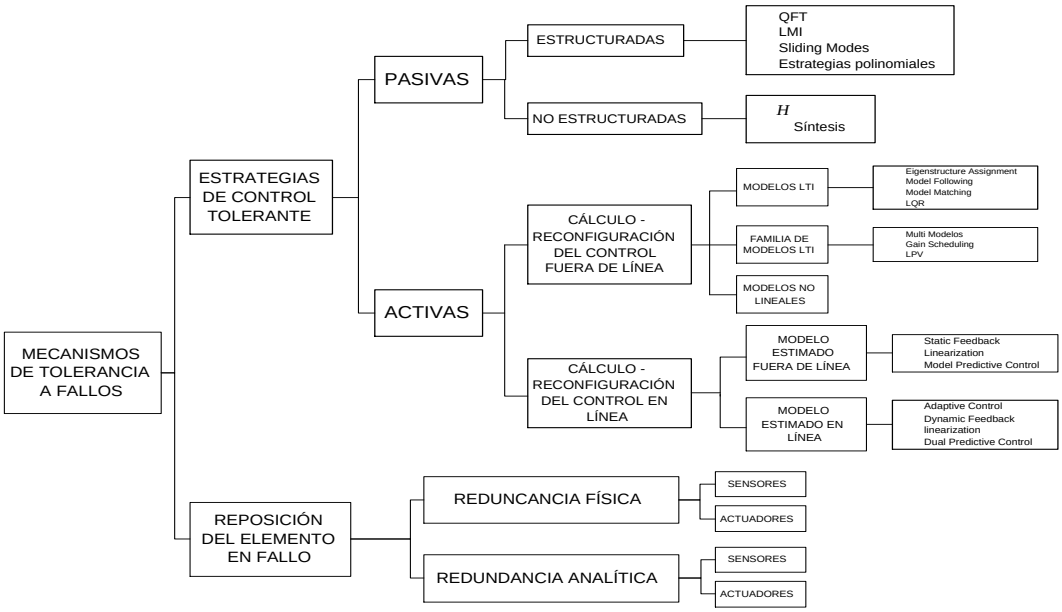


Figura 1. Clasificación de los mecanismos para control tolerante a fallos.

La Figura 1 presenta una posible clasificación de los mecanismos de tolerancia considerados en esta sección.

2.1 Tolerancia por adaptación de la estrategia de control

Desde el punto de vista de las estrategias de control, la literatura considera dos grupos principales: las técnicas activas y las pasivas. Las técnicas pasivas son leyes de control que tienen en cuenta la posible aparición de un fallo tratado como una perturbación al sistema. Así, dentro de ciertos márgenes de capacidad, la ley de control se acomoda de tal manera que el sistema admite la presencia del fallo sin tener en cuenta necesariamente el concepto de un sistema de diagnóstico. Esto las hace bastante restrictivas a soportar fallos de magnitud importante o fenómenos dinámicos no considerados dentro del diseño. Dentro de este documento no se realiza descripción alguna de estas técnicas ya que el tópico de interés centra en las técnicas activas que se apoyan en la información del fallo proporcionada por un sistema de diagnóstico. Sin embargo, en (Qu, 2001), (Qu, 2003), (Chen, 1998), (Liao, 2002) y (Liang, 2000), entre otros, se puede encontrar la descripción de técnicas pasivas de control tolerante a fallos.

Por otro lado, las técnicas de control tolerante activas consisten en reconfigurar la ley de control basándose en el uso de un diagnosticador que provee la información necesaria para realizar automáticamente los ajustes necesarios con el fin de cumplir los objetivos de control. De cara a entender las diferentes estrategias de tolerancia activa a fallos que se pueden aplicar, se ha de considerar el impacto de los fallos en el problema de control estándar $\langle O, C(\theta), U\rangle$ (ver Definición 1, (Puig, 2004)), donde $C(\theta)$ indica cómo dependen las restricciones de los parámetros que a su vez dependen de los fallos. El sistema de diagnóstico de fallos informa qué restricciones han cambiado y qué leyes de control ya no se pueden utilizar, debiéndose considerar dos casos, dependiendo de si el algoritmo de diagnóstico ha sido capaz de proporcionar:

- Una estimación $\hat{C}_f(\hat{\theta}_f)$y $\hat{U}_f$ del impacto del fallo de forma que el problema de control a resolver pasará a ser $\langle O, \hat{C}_f(\hat{\theta}_f), \hat{U}_f\rangle$.
- Sólo la detección y el aislamiento del fallo pero no estimación la magnitud de su impacto.

Existen dos formas principales de rediseño del sistema de control de cara a introducir tolerancia frente a sus efectos según si han producido o no cambios en la estructura del sistema. Esto es:

- Cambiando la ley de control sin cambiar los elementos del lazo de control mediante la ***acomodación al efecto del fallo***, en el caso de que haya sido posible estimar los cambios de estructura y parámetros introducidos por el fallo.

Definición 1 (Acomodación al fallo)
La acomodación al fallo consiste en resolver el problema de control $\langle O, \hat{C}_f(\hat{\theta}_f), \hat{U}_f\rangle$, *siendo* $\hat{C}_f(\hat{\theta}_f)$ *una estimación de las restricciones actuales proporcionadas por los algoritmos de diagnóstico de fallos.*

- Cambiando la ley de control y los elementos del lazo mediante su ***reconfiguración frente al fallo***, en el caso de que éste no haya

podido estimar los cambios de estructura y parámetros introducidos por el fallo. En este caso, se desconectarán los componentes en fallo localizados por el sistema de diagnóstico y se tratarán de alcanzar los objetivos de control utilizando sólo los componentes sin fallo.

Definición 2 (Reconfiguración del sistema)
La reconfiguración del sistema frente al fallo consiste en encontrar un nuevo conjunto de restricciones $C_f(\theta_f)$ tal que el problema de control $\langle O, C_f(\theta_f), U_f \rangle$ tenga solución, encontrarla y aplicarla.

La diferencia esencial entre ambas estrategias radica en que en el caso de la reconfiguración se utilizan diferentes señales de control y medidas entre el controlador y la planta, es decir, un cambio en su estructura, mientras que en la acomodación se pretende que sea la propia ley de control que compense el fallo. En esta categoría se pueden distinguir dos grupos:

- **Acomodación off-line** o de controlador precalculado (Figura 2(a)).
- **Acomodación on-line** o de controlador estimado en línea (Figura 2(b)).

En ambos esquemas se deberá adaptar el controlador teniendo en cuenta que el sistema en situación de funcionamiento normal viene representado por un modelo matemático al que se llamará ***Modelo Nominal*** y que en general será de la forma:

$$\begin{aligned} \dot{\mathbf{x}}_n(t) &= \mathbf{g}_n(\mathbf{x}_n(t), \mathbf{u}(t), \theta_n) \\ \mathbf{y}_n(t) &= \mathbf{h}_n(\mathbf{x}_n(t), \mathbf{u}(t), \theta_n) \end{aligned} \tag{1}$$

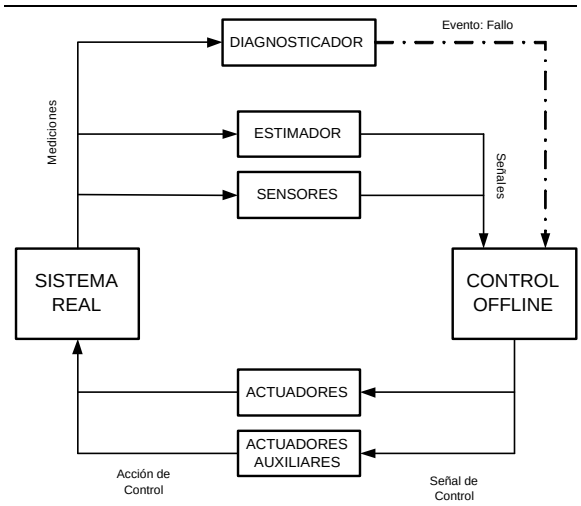
donde $\boldsymbol{x} \in \Re^{nx}$,$\boldsymbol{u} \in \Re^{nu}$ y $\boldsymbol{y} \in \Re^{ny}$ son los vectores de estado, entrada y salida de dimensión nx, nu y ny, respectivamente; $\boldsymbol{g}$ *y* $\boldsymbol{h}$ son las funciones de espacio de estado y medida respectivamente; θ es el vector de parámetros de dimensión p.

En caso de que el modelo sea lineal e invariante en el tiempo se considera de la forma: $\mathbf{g}_n(\mathbf{x}_n(t), \mathbf{u}(t), \theta_n) = \mathbf{A}_n(\theta_n)\mathbf{x}_n(t) + \mathbf{B}_n(\theta_n)\mathbf{u}(t)$ y $\mathbf{h}_n(\mathbf{x}_n(t), \mathbf{u}(t), \theta_n) = \mathbf{C}_n(\theta_n)\mathbf{y}_n(t)$.

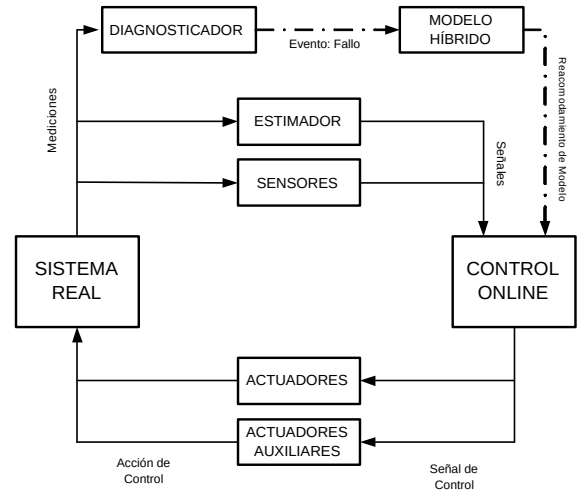
En situación de fallo, el modelo del sistema vendrá representado por el denominado ***Modelo en Fallo*** y que en general será de la forma:

$$\begin{aligned} \dot{\mathbf{x}}_f(t) &= \mathbf{g}_f(\mathbf{x}_f(t), \mathbf{u}(t), \theta_f) \\ \mathbf{y}_f(t) &= \mathbf{h}_f(\mathbf{x}_f(t), \mathbf{u}(t), \theta_f) \end{aligned} \tag{2}$$

donde el subíndice $f$denota la presencia del fallo, mientras que en caso particular de que el modelo sea lineal e invariante en el tiempo se considera de la forma: $\mathbf{g}_f(\mathbf{x}_f(t), \mathbf{u}(t), \theta_f) = \mathbf{A}_f(\theta_f)\mathbf{x}_f(t) + \mathbf{B}_f(\theta_f)\mathbf{u}(t)$ y $\mathbf{h}_f(\mathbf{x}_f(t), \mathbf{u}(t), \theta_f) = \mathbf{C}_f(\theta_f)\mathbf{y}_n(t)$.



(a) Fuera de Línea



(b) En Línea

Figura 2. Esquemas básicos del control tolerante activo.

Cabe agregar que se supone que no hay variación de la dimensión del espacio de estado entre el modelo nominal y el modelo en fallo y que no existe ninguna relación entre los dos modelos en los aspectos de controlabilidad y/o observabilidad.

2.2 Tolerancia por reposición de sensores y/o actuadores

Fallos graves en sensores o actuadores rompen los lazos de control. Para mantener el sistema controlado en funcionamiento es necesario utilizar un conjunto diferente de actuadores (entradas) y/o sensores (salidas). Para ello se propone utilizar un bloque de reconfiguración que junto con la planta en fallo, la planta reconfigurada se comporte igual que la planta sin fallo. Esta solución trata de aplicar los mínimos cambios al lazo de control, de tal manera que el controlador estándar pueda continuar controlando la planta como si no existiera fallo.

En cualquier caso, ya sea en sensores o actuadores, se maneja la idea de reconfiguración desde los siguientes puntos de vista:

- ***Mediante redundancia física:*** también llamada ***redundancia hardware***. Para el caso de sensores, este camino consiste en contar con un número generalmente impar de ellos, cuyas salidas se multiplexan dentro de un bloque de decisión. En este bloque se determina la medida correcta a partir de la salida más común producida por cada uno de los sensores**.** El caso de actuadores es más directo, pues de producirse una avería, la redundancia física implica contar con otro dispositivo alternativo listo para realizar la acción de control previa determinación de daño en el actuador principal.
- ***Mediante redundancia analítica:*** también conocida como redundancia mediante ***software*** o de ***elemento virtual***. Este caso consiste en la incorporación al lazo de un bloque que reconstruya las medidas mediante la estimación de las mismas (para sensores) o la aún teórica idea del reajuste de señales alternativas para llevar a cabo la acción de control requerida (para actuadores). Así se evita la incorporación de nuevo hardware en el sistema lo que se ve reflejado en costos de instrumentación.

En adelante se le dedica especial interés a los aspectos relacionados con la redundancia analítica.

3. MECANISMOS DE TOLERANCIA A FALLOS EN LA LEY DE CONTROL

3.1 Técnicas de acomodación del control off-line.

En este caso se obtiene un controlador fuera de línea parametrizado en función de los fallos, llegándose a determinar una ley de control $U(f)$ donde f corresponde al fallo diagnosticado. Así, la arquitectura del sistema contiene un bloque en el cual el sistema supervisor determina el modo de operación cuando se produce el fallo para posteriormente determinar $U(f)$. El esquema básico de funcionamiento de este grupo se muestra en la Figura 2(a). Una posible caracterización de las técnicas que incorporan este grupo según la naturaleza de la planta que integra el lazo de control se da en (Theilliol, 2003) de la siguiente manera:

- ***Modelos LTI:*** técnicas aplicadas sobre una planta de modelo lineal invariante en el tiempo, tales como *Model Matching, Model Following, LQR* y *EA (eigenstructure assigment)*, entre otras.
- ***Familia de modelos LTI:*** técnicas aplicadas sobre una planta cuyo modelo matemático es no lineal y ha sido descompuesto en varios modelos, los cuales corresponden a linealizaciones alrededor de ciertos puntos predefinidos de tal manera que se cubra la zona de interés en el espacio de estado, tales como *Multimodelos*, *Gain-Scheduling y LPV.*
- ***Modelos no lineales:*** técnicas de control que se aplican sobre sistemas cuyo modelo es directamente no lineal. En este caso se hace uso de técnicas de *soft-computing* para realizar la implementación de los controladores. A este grupo pertenecen las técnicas como *control Difuso*, *Neuronal* y *Neuro-difuso*, entre otras (Diao, 2001a).

A continuación se realizará una breve descripción de algunas de las técnicas propuestas para realizar acomodación fuera de línea.

3.1.1. Model matching (Kung, 1992). Puesto que el modelo nominal del sistema en lazo cerrado es conocido, dicho modelo se puede utilizar como una especificación de las propiedades dinámicas que el controlador tolerante debe mantener en presencia de un fallo. Si consideramos que el sistema de control estándar es del tipo realimentación de estado, la dinámica del sistema controlado se puede expresar como:

$$\begin{aligned}\dot{\mathbf{x}}(t) &= (\mathbf{A}_n - \mathbf{B}_n\mathbf{K}_n)\mathbf{x}(t)\\ \mathbf{y}(t) &= \mathbf{C}_n\mathbf{x}(t)\end{aligned} \tag{3}$$

Cuando aparece un fallo, la dinámica del sistema controlado vendrá dada por la ecuación (2). El sistema controlado con el nuevo controlador $\boldsymbol{K}_f$ a utilizar vendrá descrito por:

$$\begin{aligned}\dot{\mathbf{x}}(t) &= (\mathbf{A}_f - \mathbf{B}_f\mathbf{K}_f)\mathbf{x}(t)\\ \mathbf{y}(t) &= \mathbf{C}_f\mathbf{x}(t)\end{aligned} \tag{4}$$

lo que permite obtener la ecuación de diseño del mismo. Si se desea que el sistema controlado presente las mismas prestaciones (modelo de lazo cerrado) que el sistema controlado sin fallo debe cumplirse:

$$\mathbf{A}_n - \mathbf{B}_n\mathbf{K}_n = \mathbf{A}_f - \mathbf{B}_f\mathbf{K}_f \tag{5}$$

Una solución aproximada a esta ecuación de diseño se obtiene empleando la matriz pseudoinversa de $\mathbf{B}_n$, $\mathbf{B}_n^+$

$$\mathbf{K}_f = \mathbf{B}_n^+(\mathbf{A}_n - \mathbf{A}_f + \mathbf{B}_n\mathbf{K}_n) \tag{6}$$

Por este motivo a este método se le conoce también como ***método de la pseudoinversa***.

3.1.2. Model following (Jiang, 1994). Si se dispone del modelo nominal del sistema (1), de su

modelo en fallo (2) y suponiendo que todos los estados son accesibles, se considera el esquema de control que se presenta en la Figura 3.

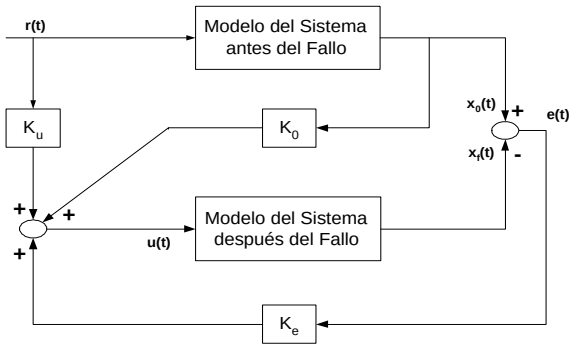


Figura 3. Esquema de control Model Following.

El diseño del control tolerante consiste en determinar $\boldsymbol{K}_0$, $\boldsymbol{K}_u$ y $\boldsymbol{K}_e$. El error entre ambos modelos viene dado por el error del sistema expresado como $\mathbf{e}(t) = \mathbf{x}_0(t) - \mathbf{x}_f(t)$, de donde:

$$\dot{\mathbf{e}}(t) = \mathbf{A}_f\mathbf{e}(t) + (\mathbf{A}_0 - \mathbf{A}_f)\mathbf{x}_0(t) + \mathbf{B}_0\mathbf{r}(t) - \mathbf{B}_f\mathbf{u}(t) \quad (7)$$

Si se define como ley de control:

$$\mathbf{u}(t) = \mathbf{K}_e\mathbf{e}(t) + [\mathbf{K}_0\mathbf{x}_0(t) + \mathbf{K}_u\mathbf{r}(t)] \quad (8)$$

entonces la ecuación de la dinámica del error se transforma en:

$$\dot{\mathbf{e}}(t) = [\mathbf{A}_f - \mathbf{B}_f\mathbf{K}_e]^{\mathbf{e}}(t) + (\mathbf{A}_0 - \mathbf{A}_f - \mathbf{B}_f\mathbf{K}_0)\mathbf{x}_0(t) + (\mathbf{B}_0 - \mathbf{B}_f\mathbf{K}_u)\mathbf{r}(t) \quad (9)$$

$\mathbf{K}_0$ y $\mathbf{K}_u$ se determinan a partir de los valores que minimizan la norma:

$$\|(\mathbf{A}_0 - \mathbf{A}_f - \mathbf{B}_f\mathbf{K}_0)\mathbf{x}_0 + (\mathbf{B}_0 - \mathbf{B}_f\mathbf{K}_u)\mathbf{r}\|_2$$

con $\mathbf{K}_0 = \mathbf{B}_f^+(\mathbf{A}_0 - \mathbf{A}_f)$ y $\mathbf{K}_u = \mathbf{B}_f^+\mathbf{B}_f$, respectivamente. Para este caso, $\mathbf{B}^+$ representa la matriz pseudo-inversa de $\boldsymbol{B}$. El valor de $\mathbf{K}_e$ se determina de forma que los valores propios de la matriz $\mathbf{A}_f - \mathbf{B}_f\mathbf{K}_e$ cumplan la condición de estabilidad.

3.1.3. Eigenstructure Assignment (EA) (Jiang, 1994). Ya que la estabilidad y la dinámica del sistema controlado dependen de sus valores y vectores propios, un mecanismo de acomodación de cara a obtener tolerancia a fallos consiste en forzar a que la estructura de vectores y valores propios del sistema en fallo sea la misma que la del sistema nominal sin fallo. Si se dispone del modelo nominal del sistema (1) y del modelo en fallo (2), la ley de acomodación del controlador se obtendrá a partir de:

$$(\mathbf{A}_f + \mathbf{B}_f\mathbf{K}_f)\mathbf{v}_i^f = \lambda_i^f\mathbf{v}_i^f \quad (10)$$

donde λ_i^f y $\mathbf{v}_i^f$ para *i=1,...,n* representan respectivamente los vectores y valores propios del sistema acomodado, debiéndose de cumplir que:

$$\lambda_i^f = \lambda_i \quad (11)$$

para *i=1,...,n* , donde $\lambda_i$son los valores propios del sistema sin fallo, así como que los vectores propios del sistema sin fallo $\boldsymbol{v}_i$ sean lo más próximos a los del sistema acomodado $\mathbf{v}_i^f$.

Esta técnica es usualmente implementada en sistemas de múltiple entrada y múltiple salida y tiene como ventaja a destacar la manipulación de la expresión explícita de la estructura dinámica requerida, lo cual permite alcanzar teóricamente la estabilidad y los objetivos de control deseados. Las condiciones fundamentales para la aplicación de esta técnica son en primer lugar que exista un número suficiente de actuadores y de sensores disponibles dependiendo de la aplicación (Zhang, 2002) y que los vectores propios deseados residan en subespacios alcanzables (Murray Wonham, 1978). Sin embargo, sus limitaciones son que los objetivos de control no podrán ser óptimos en ningún sentido y que los requerimientos del sistema no pueden ser expresados fácilmente en términos de su estructura. Por esto, Zhang y Jiang (1999) proponen combinar la técnica EA y el control LQR, argumentando un mejor desempeño cuando las ventajas de ambas estrategias son asociadas, haciendo que el EA se encargue de las tareas de acomodación mientras que el LQR actúa como controlador nominal.

La estrategia presentada en (Zhang, 2002) consiste en el uso de EA, el cual utiliza la información de los estados proveniente de un Filtro de Kalman Adaptativo (FKA). El controlador se divide en dos bloques: la parte *feedback*, en la cual se usa el EA y la parte *feedforward*. Dicho controlador es modificado convenientemente por un bloque de acomodación. Así, el bloque *feedback* se encarga de la adecuación de la estructura y el bloque *feedforward* se ocupa de que el sistema realice el seguimiento a consignas. Esto último se logra mediante una estrategia conocida como CGT (Command Generador Tracker), la cual está basada en el principio de Model Following. La Figura 4 muestra la estructura del lazo de control descrito. La señal de control tendrá una expresión de la forma:

$$\mathbf{u}(t) = \mathbf{K}_{ff}\mathbf{w}(t) + \mathbf{K}_{fb}\mathbf{x}(t) \quad (12)$$

donde $\boldsymbol{K}_{ff}$y $\boldsymbol{K}_{fb}$ son las ganancias de los controladores y $\boldsymbol{w}(t)$ es la señal de consigna.

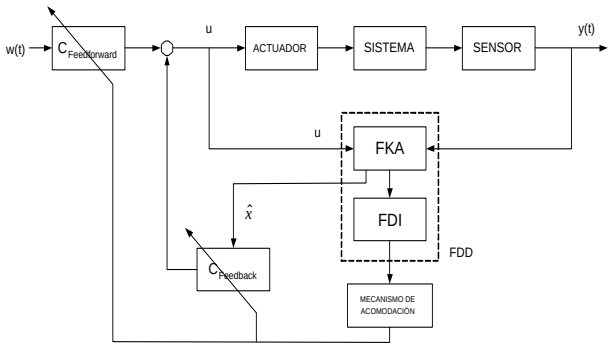


Figura 4. Acomodación usando EA.

3.1.4. Additive fault compensation (Noura, 2001). En el caso de fallos aditivos en sensores o actuadores, una forma de acomodar el fallo se puede conseguir mediante la ley de control siguiente:

$$\mathbf{u}(t) = \mathbf{u}_0(t) + \mathbf{u}_f(t) \tag{13}$$

donde $\mathbf{u}_0(t)$ es la componente nominal del ley de control obtenida a partir de los estimadores que no están afectados por el fallo, mientras que $\mathbf{u}_f(t)$ es la ley de control obtenida a partir de la estimación del fallo de cara a cancelar su efecto según:

$$\mathbf{B}\mathbf{u}_f(t) + \mathbf{B}_j\hat{\mathbf{f}}_a(t) = 0 \tag{14}$$

por ejemplo, para el caso de un fallo en el j-ésimo actuador, de donde:

$$\mathbf{u}_f(t) = -\mathbf{B}^+\mathbf{B}_j\hat{\mathbf{f}}_a(t) \tag{15}$$

siendo $\hat{\mathbf{f}}_a(t)$ la estimación del fallo y $\mathbf{B}^+$ representa la matriz pseudo-inversa de $\boldsymbol{B}$.

3.1.5. Multicontroladores y gain-scheduling . El control de sistemas no lineales y/o variantes con el punto de operación se puede realizar mediante el uso de alguno de los siguientes métodos:

- ***Multicontroladores*** (bancos de controladores): basado en el diseño de un conjunto de controladores lineales para distintos puntos de operación. En tiempo real mediante la medición del punto de operación del sistema se realiza una fusión/conmutación entre los mismos.
- ***Gain-Scheduling***: basado en el diseño de controladores paramétricos con el punto de operación. En tiempo real mediante la medición del punto de operación se modifica la ley de control ya sea mediante una expresión analítica o una tabla de valores predeterminados.

La incorporación en esta estrategia de control de mecanismos de acomodación frente al fallo consiste en ver el fallo como un nuevo punto/modo de operación para el cual se habrá diseñado un controlador lineal, al cual se conmutará en presencia del fallo, garantizando la estabilidad y una degradación aceptable de las prestaciones. El sistema de diagnóstico es el encargado de medir el modo de operación en fallo de forma que el sistema supervisor active o adapte el controlador correspondiente (Huzmezan, 1998), (Zhang, 2001).

3.2 Técnicas de acomodación del control on-line

En este caso se obtiene en línea una ley de control U a partir una estimación de las restricciones actuales $\hat{C}_f(\hat{\theta}_f)$ después de la aparición del fallo. El esquema básico de funcionamiento de este grupo se muestra en la Figura 2(b). A su vez, para la estimación del efecto del fallo sobre las restricciones existen dos alternativas:

- **Estimación off-line**. Previamente se ha estudiado el efecto de los fallos sobre las restricciones parametrizándose las mismas en función del fallo. Al diagnosticarse el fallo se cambiarán dichas restricciones de acuerdo con el fallo, lo que afectará también al controlador puesto que también se calcula en línea a partir de las mismas. A este grupo corresponden las técnicas de *Control Predictivo basado en Modelo* y de *Linealización Estática por Realimentación*.
- **Estimación on-line.** El efecto del fallo sobre las restricciones se estima en línea de forma que el controlador, que también se calcula en línea a partir de las mismas, se adaptará a los cambios que se produzcan. A este grupo corresponden técnicas como el *Control Adaptativo*, la *Linealización Dinámica por Realimentación* y el *Control Predictivo Dual*.

3.2.1. Control adaptativo. El control adaptativo proporciona la forma más natural de diseñar un control tolerante puesto que el efecto de los fallos se manifiesta como un cambio en los parámetros estimados en línea. La ley de control se acomoda automáticamente a partir de los nuevos valores de los parámetros. La literatura reporta trabajos explícitos básicos en el tema como la redundancia de controladores propuesta por Cho (1990), las aplicaciones conjuntas con redes neuronales presentadas como sistemas robustos y adaptables en tareas de tolerancia a fallos (Wasser, 1989) y

la consideración de técnicas de control como el Backstepping para analizar el sistema en modo de fallo y lograr hacer que se adapte de manera adecuada a las nuevas condiciones de funcionamiento, trabajo propuesto por Ikeda y Shin (1995).

De manera más reciente, Diao y Passino (2001a, 2001b, 2002) proponen en el tema la aplicación de estrategias neuro/difusas adaptables al fallo del sistema debido a la capacidad de aprendizaje en línea de las dinámicas desconocidas causadas por los fallos que puedan presentarse. La efectividad de su método ha sido estudiada en un caso de estudio real. Su propuesta se ve inmersa en la reciente teoría del control tolerante al realizar el diagnóstico del fallo de manera robusta implementando los métodos propuestos e integrando la adaptación a la arquitectura del sistema tolerante. El esquema de la Figura 5 propone una estrategia adaptativa de múltiples modelos donde se tienen en cuenta los elementos de diagnóstico y supervisión y engloba la filosofía de control activo a través de las técnicas neurodifusas.

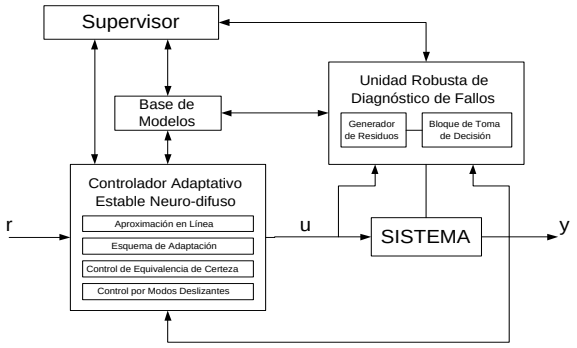


Figura 5. Esquema de lazo de control tolerante adaptativo basada en técnicas neurodifusas.

3.2.2. Control predictivo (Maciejowski, 1993; 2001). Las leyes de control predictivo permiten incluir de forma fácil estrategias de control tolerante, puesto que la acción de control se determina a cada instante resolviendo un problema de optimización en un horizonte temporal utilizando como restricción el modelo del sistema. Si dicho modelo se actualiza a partir de la información proporcionada por el sistema de diagnóstico acerca del fallo, las nuevas acciones de control se calcularán teniendo en cuenta el efecto del fallo sobre el sistema. La información acerca del fallo se puede incluir mediante:

- La redefinición de las restricciones para representar determinados tipos de fallo, siendo especialmente adecuada para fallos en actuadores. Así, por ejemplo, el rango de operación puede quedar reducido a un nuevo rango, o prefijado a un determinado valor.
- El cambio del modelo de la dinámica para reflejar cambios en la planta real bajo fallo.
- El cambio de los objetivos de control para reflejar limitaciones debido a la operación bajo condiciones de fallo, eliminando, por ejemplo, el control de una variable a raíz de un fallo en el sensor que la medía, en el caso de que ésta no pueda ser reconstruida mediante otros mecanismos.

Una extensión de esta técnica al caso de multimodelos ha sido propuesta por Gopinathan (1998), en la cual aparecen ciertos interrogantes de operación y desempeño cuyas respuestas son particulares para cada aplicación (Aufderheide, 2001). Cuestiones abiertas pueden ser citadas como el número requerido de modelos, la estabilidad de cada uno de ellos en el lazo cerrado, la transición entre ellos y los tiempos de retardo más la consideración del retardo del FDI, entre otras.

De otro lado, una variante de la técnica de control predictivo consiste en la utilización del denominado *Control Predictivo Dual* propuesto por Veres (1998), el cual que puede ser usado cuando ocurren cambios dinámicos inesperados y se requiere mantener un compromiso razonable entre el comportamiento de la planta y la rápida valoración de los efectos producidos por la estimación probablemente desviada. Básicamente, esta estrategia se basa en el control predictivo agregando además una componente que consiste en usar entradas con una acción de prueba para obtener más información de la planta con el fin de beneficiar un control futuro. Este tipo de ley de control tiene en cuenta tres aspectos:

- Precaución del controlador: Significa que se tiene en cuenta la incertidumbre del modelo del sistema. Esto se logra incluyendo un modelo de la incertidumbre en la función de costo del controlador.
- Prueba del controlador: Significa que tiene en cuenta el efecto de la entrada de control en la precisión del modelado basada en la estimación en línea.
- Inclusión de restricciones: La cual se realiza en el proceso de optimización de la función de costo predictiva. Dichas restricciones pueden ser de naturaleza “hard” o “soft”.

4. MECANISMOS DE TOLERANCIA A FALLOS EN SENSORES Y ACTUADORES

4.1 Tolerancia en sensores

En el caso de sensores, el bloque de reconfiguración consiste en utilizar un observador que permita reconstruir las medidas del sistema a partir de

otros sensores existentes, por lo que se denomina ***sensor virtual*** o ***software***. Las técnicas de reposición de medidas basadas en filtros de Kalman no sólo tienen validez en el ámbito de fallos sino también en la idea de optimizar el proceso de medición de variables dentro de un control industrial moderno. La posibilidad de estimar variables se encuentra estrechamente ligada con las especificaciones particulares del sistema y con la disponibilidad de elementos de medida. El diseño de una red de sensores teniendo en cuenta los criterios de tolerancia a fallos, observabilidad del sistema, costos y robustez es tema de amplio estudio actualmente en la literatura (Hoblos, 2000)(Attouche, 2001). Staroswiecki y sus colaboradores (2004) proponen la estimación de la tolerancia a fallos asociada al diseño de redes de sensores, analizando el tiempo de utilidad del conjunto de sensores, evaluando su capacidad de tolerancia y conjunto mínimo necesario considerando la redundancia. En el campo de las aplicaciones en este tema se pueden citar los trabajos basados en fallos de sensores en aeronáutica (Lyshevski, 1999), (Huo, 2001), en sistemas AC (Bennett, 1999), entre otros.

4.2 Tolerancia en actuadores

Análogo a la tolerancia en sensores, la tolerancia en actuadores consiste en la capacidad que tiene el lazo de control de soportar la influencia de un fallo originado en la etapa de ejecución de las acciones determinadas por el controlador. Estas acciones, por estar relacionadas con actuadores físicos, pueden ser irremplazables y un fallo originaría la incapacidad del sistema para ejecutar cualquier acción, lo que implicaría en la práctica una necesidad casi inminente de incorporar al menos otro actuador redundante. Sin embargo y en el área del análisis teórico, se ha propuesto recientemente una estrategia que se muestra como el dual del sensor virtual conocida como ***actuador virtual***(Lunze, 2003). Esta estrategia supone, de nuevo, un modelo nominal del proceso (1) y un modelo de la planta cuando se presenta fallo en el actuador (2). Mediante la inclusión de un observador y un controlador por realimentación de estados se pretenden cumplir los siguientes objetivos:

- Que el controlador haga que el lazo de control reconfigurado se comporte como el modelo nominal del sistema, o lo que es lo mismo $\boldsymbol{x}_f(t) = \boldsymbol{x}_n(t)$ (*Strong Reconfiguration Goal*).
- Que la salida del sistema reconfigurado tienda al valor de la salida del modelo nominal en presencia de una señal de consigna constante, es decir $\boldsymbol{y}_f(t) \rightarrow \boldsymbol{y}_n(t)$ (*Weak Reconfiguration Goal*).

La condición fundamental para el empleo de la técnica descrita y para asegurar la estabilidad del sistema reconfigurado es que este modelo del sistema en fallo (2) sea controlable. En estas condiciones, dado un modelo en fallo como el de la ecuación (2) (contemplada la restricción anterior), un controlador nominal y un punto de equilibrio se diseña el actuador virtual (observador y realimentación de estados) para incorporarlo al lazo de control y obtener el sistema reconfigurado capaz de tolerar fallos en actuadores.

Sin embargo, esta estrategia deja cuestiones abiertas en cuanto a sus limitaciones de implementación. Entre otras se puede citar el conocimiento necesario de los efectos del fallo sobre el actuador y su modelado para obtener el modelo del sistema necesario a usar en el cálculo del actuador virtual. Tópicos abiertos se plantean en este campo como son la parametrización automática del bloque de reconfiguración, la evaluación del comportamineto de la técnica en escenarios reales, el diseño de la instrumentación previendo las influencias de los fallos, las restricciones dadas por la estimación del fallo y la incertidumbre dada por el cálculo del punto de equilibrio del sistema y la posterior obtención tanto del modelo nominal como del modelo en fallo, entre otras. Nótese que estas técnicas heredan todos los problemas considerados en las estrategias de modelado dinámico y control clásico.

Una manera más implícita de plantear la tolerancia a fallos en actuadores consiste en utilizar la información del diagnosticador para realizar las consideraciones necesarias que puedan ser incorporadas en los criterios de modificación del controlador o en su ley de ajuste (Zhang, 2000), (Tao, 2002), (Wang, 2000). De esta manera el fallo ocurre en el actuador pero quien asume la función de tolerancia y reposición es la ley de control, pudiéndose suponer la existencia de redundancia física (Maki, 2001) o una disposición apropiada de actuadores y una combinación adecuada de comandos que, mediante relaciones indirectas, hagan que se cumpla el objetivo de control predefinido (Dardinier-Maron, 1999). Estas técnicas se acercan más a la filosofía de acomodación, ligada a la ley de control, que a la reconfiguración.

Otras estrategias se basan en la detección de la magnitud del fallo y el aprovechamiento de esta información utilizando el modelo nominal, el modelo en fallo y una relación definida entre ambos (Zhou, 2002), (Zhao, 1998), para generar el modelo del sistema tal como se expresa en la ecuación (2). Es así como la expresión:

$$\mathbf{B}_f = \mathbf{B}_n(\mathbf{I} - \mathbf{\Gamma}(t)) \tag{16}$$

donde $\mathbf{\Gamma}(t) = diag\left[\gamma_1\ \gamma_2\ \cdots\ \gamma_m\right]$, realiza la menciona relación entre modelos. Los términos $\gamma_i(t)$, con *i=1,...,m*, denotan el estado de cada actuador, siendo 1 si el actuador está completamente averiado, 0 si el actuador está en perfectas condiciones y $0 < \gamma_i < 1$ si el actuador presenta pérdida parcial de efectividad. Por lo tanto, la estimación de la matriz $\Gamma(t)$ se realiza en línea con el fin de determinar la influencia del fallo en el proceso y el modelo resultante se encuentra listo para aplicar alguna de las técnicas de acomodación anteriormente mencionadas.

5. EL SISTEMA SUPERVISOR

El sistema supervisor es un sistema basado en eventos discretos, mientras que el sistema supervisado es un sistema a tiempo continuo. El nivel supervisor intercambia información con el sistema supervisado mediante el diagnosticador, el cual le proporciona información sobre la existencia de fallos y sus características, y actúa sobre el mismo mediante la activación de los mecanismos de acomodación y reconfiguración frente a los fallos. Debido a la naturaleza híbrida de los sistemas de control tolerante, su análisis y diseño se puede abordar mediante la teoría de sistemas híbridos (Cassandras, 1995)(Morari, 2003), siendo actualmente ésta una tarea pendiente de desarrollar en la literatura existente.

El sistema supervisor debe realizar el conjunto de funciones que se detalla a continuación para que el sistema de control alcance la tolerancia a fallos:

- Monitorización de la planta controlada.
- Diagnóstico de los fallos mediante su detección, aislamiento y estimación de su tamaño.
- Evaluación de la situación después de que un fallo ha sido diagnosticado a partir de la información acerca del mismo, valorando la posibilidad de activar o no mecanismos de tolerancia a fallos.
- Ejecución de las acciones correctoras que acomoden el sistema controlado al fallo, permitiendo su funcionamiento con un grado de degradación aceptable mientras sea posible.
- Comunicación con el resto de subsistemas y la propia planta para intercambiar información.

La implementación del nivel de supervisión en un sistema de control requiere de una arquitectura apropiada que deberá de ser capaz de acomodar la implementación de las funcionalidades anteriormente mencionadas.

5.1 Arquitectura del sistema de control tolerante

La Figura 6 muestra una posible arquitectura para un sistema de control tolerante que engloba los tres niveles descritos por Blanke (1999): la parte del lazo tradicional de control (nivel 1), el sistema diagnosticador y de acomodación/reconfiguración del fallo (nivel 2) y el nivel de supervisión (nivel 3) que cierra el lazo exterior y añade la tolerancia frente al fallo.

El esquema de la Figura 6 muestra el lazo de control realimentado que consta de una ***ley de control***, un ***actuador***, la ***planta*** y un ***sensor***. En paralelo con los bloques del actuador y el sensor se encuentran elementos de hardware o software que se encargan de proporcionar ***redundancia*** tanto en la medición de señales como en la ejecución de acciones de control. Dicha redundancia se puede introducir de forma física (sensores o actuadores redundantes), o bien de forma analítica (mediante modelos) tal como se ha visto en la Sección correspondiente a mecanimos de tolerancia a fallos. A partir de las medidas de las entradas y salidas del actuador, sensor y planta, el diagnosticador realiza la detección y aisamiento del fallo y, de ser posible, la cuantificación de su magnitud además de discriminar el elemento que se encuentra implicado. Cuando el diagnosticador ha detectado, aislado y estimado el fallo, comunica al sistema ***supervisor automático (SA)*** lo ocurrido y éste se encarga de tomar las decisiones de recuperación del lazo de control frente al fallo reportado, evaluando una serie de criterios y realizando, de ser posible, un conjunto de acciones que se resumen en la Figura 7. Este supervisor automático es configurado por el ***supervisor humano (SH)***, que es aquel operario que impone las consignas para el lazo de control y analiza la posible información que el supervisor automático pueda ofrecer en cuanto a estadísticas de fallos o desempeño del sistema.

5.2 Sistemas de supervisión automática

El sistema de supervisión automática comercial más parecido al descrito en el apartado anterior es un *SCADA*, acrónimo de *Supervisory Control And Data Acquisition*. Un SCADA es una aplicación informática de ejecución típica en equipos de sobremesa, que incluye adquisición de datos, almacenamiento de datos, interfase de comunicaciones, interfase de operación y explotación de datos.

Los SCADA más modernos han evolucionado hacia una compleja base de datos que alimenta y es alimentada por aplicaciones interrelacionadas de gestión de procesos batch, análisis de históricos, generación de informes, etc. Una de las aplicaciones (o módulos) que actualmente cualquier SCA-

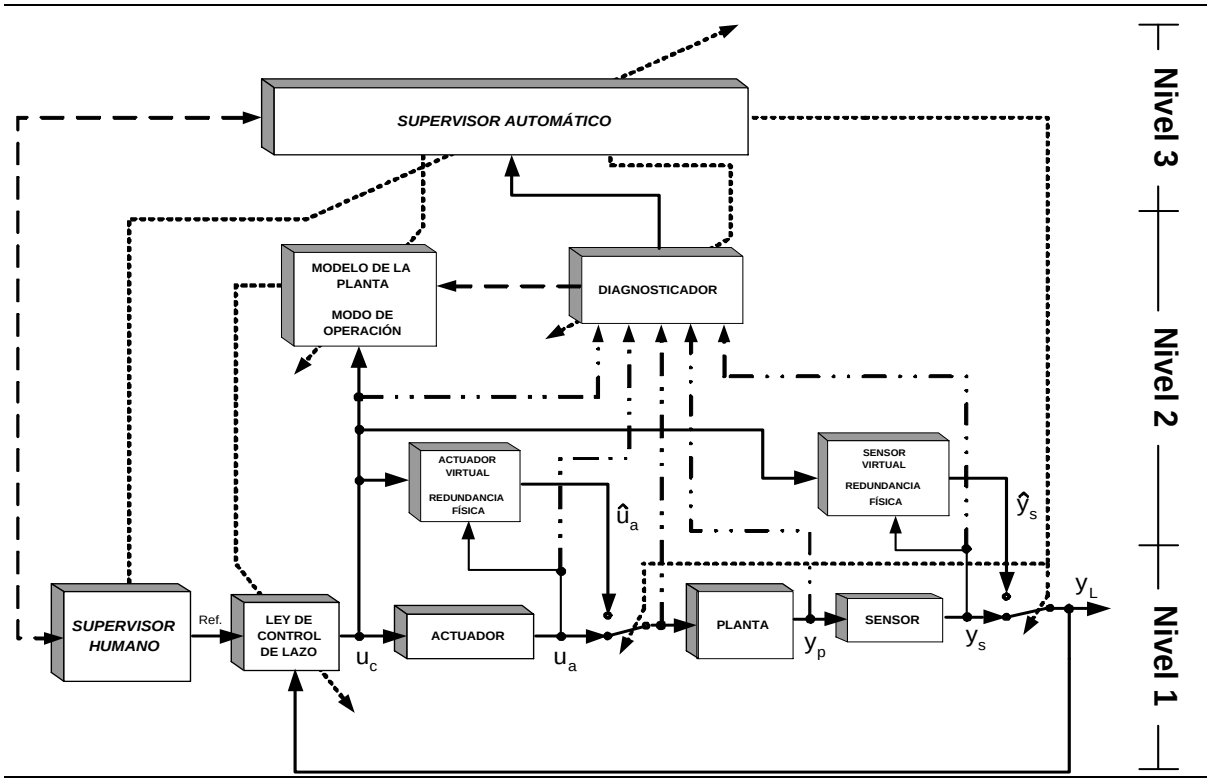


Figura 6. Arquitectura propuesta para un sistema de control tolerante a fallos.

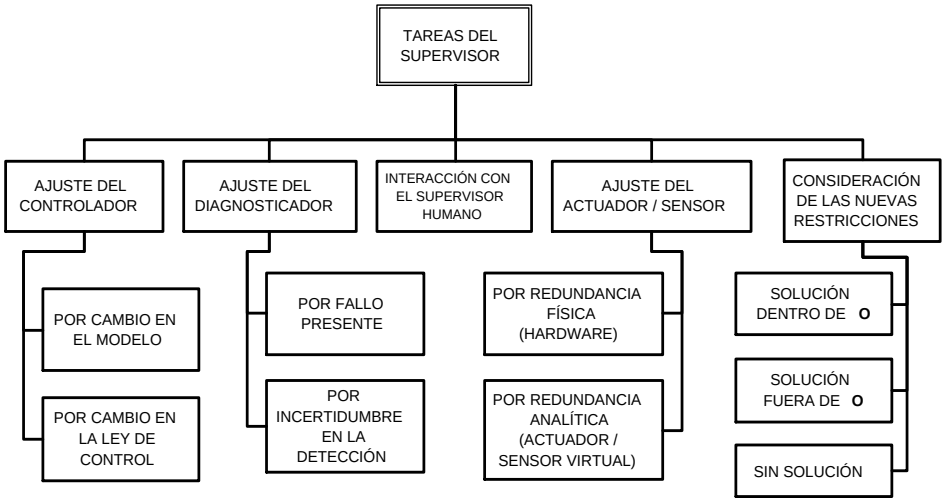


Figura 7. Tareas del supervisor automático.

DA incorpora es el de programación, entendiendo ésta como la posibilidad de diseño de cualquier algoritmo de control y/o supervisión de la planta. Los lenguajes más extendidos son C/C++, Visual Basic y otros propios de cada paquete. Esto puede permitir al usuario la programación de sistemas de control tolerantes a fallos pero la mayor parte del trabajo, en este sentido, está por hacer.

De los 51 productos analizados en Ayza (2002), solamente 1 declara tener un módulo de gestión de fallos. En realidad, la mayoría de ellos incorpora el concepto de alarma y su gestión, pero en general se trata de la mera detección de una situación concreta, basada normalmente en la superación de umbrales o la activación de señales binarias.

Sin embargo, el mismo informe describe las últimas herramientas incorporadas en los más modernos SCADA que son, precisamente, las que permiten a un operario humano determinar el funcionamiento correcto/incorrecto de la planta y tomar las medidas correctoras necesarias. Si esta tendencia que están siguiendo los SCADA comer-

ciales continua, el próximo paso será incorporar módulos de control tolerante a fallos para asistir al operario en sus tareas.

5.3 Aplicaciones en la industria

En la actualidad puede encontrarse referencias en la literatura de la aplicación de las técnicas de tolerancia a fallos en:

- aerodinámica (Lyshevski, 1999) (Huo, 2001) (Ganguli, 2002) (Wu, 2004),
- aplicaciones con motores/generadores de inducción (Hao, 2002) (Zidani, 2003) (Bonivento, 2004),
- robótica (Meng Ji, 2003) (Notash, 2003),
- procesos químicos (Bao, 2003)

entre otros temas.

6. CASO DE ESTUDIO: CONTROL TOLERANTE RED DE ALCANTARILLADO DE BARCELONA

La aplicación que se describe a continuación es la misma que se ha presentado en el primer artículo de control tolerante (Puig, 2004) y trata del control global de la red de alcantarillado de Barcelona que tiene como objetivo minimizar las inundaciones y vertidos al mar actuando sobre los elementos activos de la red de alcantarillado (depósitos de retención, compuertas de derivación, estaciones de bombeo) en caso de lluvia intensa.

Tal como se describe en (Cembrano, 2004), el control global requiere conocer el estado actual de la red proporcionada por sensores conectados a un SCADA y disponer de los actuadores (compuertas y bombeos) operativos. En este artículo se enfatizará el la necesidad de mantener en funcionamiento el sistema de control global en condiciones meteorológicas muy adversas dotando tanto a los más de 100 sensores (pluviómetros y limnímetros) que dispone la red de Barcelona y/o actuadores de los depósitos de retención, compuertas de derivación o estaciones de bombeo de mecanismos de tolerancia a fallos (Figueras, 2004).

Los resultados que se presentan a continuación corresponden a una parte representativa de la red de alcantarillado de la ciudad de Barcelona compuesta por varias subcuencas, con un depósito de retención (Escola Industrial) que dispone de dos compuertas de entrada y de salida y una compuerta de derivación (Tarragona), 11 depósitos virtuales que contienen todo el volumen que almacena la red de alcantarillado en esta zona, 12 pluviómetros que miden la intensidad de lluvia y 10 limnímetros que proporcionan los niveles de los colectores principales (Figura 8).

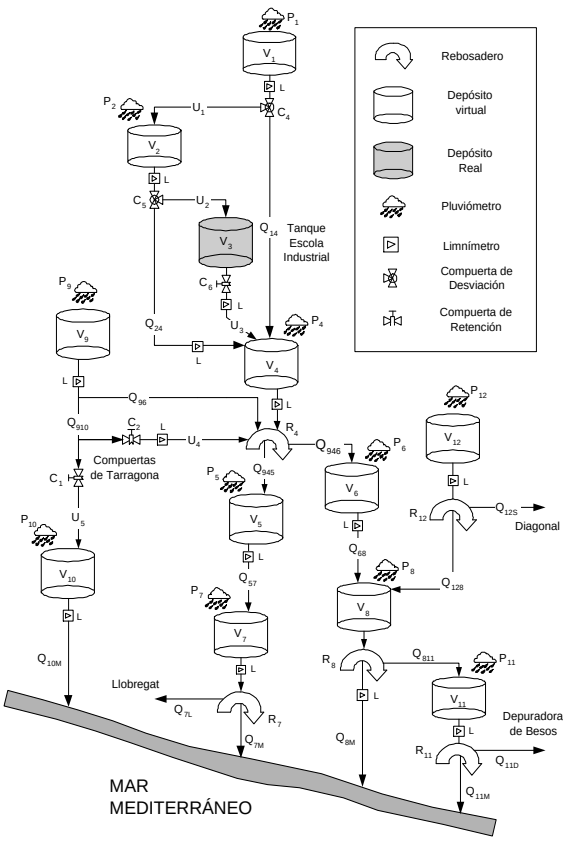


Figura 8. Modelo de la cuenca piloto de Barcelona.

6.1 Tolerancia a fallos en sensores

La Figura 9 presenta la estrategia de tolerancia que se ha llevado a cabo para todos los sensores de la red. En primer lugar, se ha detectado, aislado y repuesto los pluviómetros en fallo y a continuación suponiendo que las mediciones de los pluviómetros son correctas, se han detectado, aislado y repuesto los limnímetros en fallo.

Como ya se ha dicho anteriormente, la estrategia utilizada como mecanismo para la tolerancia de los limnímetros es la de reposición de la estimación mediante su modelo. Ahora bien, el modelo utilizado para la detección no puede ser utilizado directamente para remplazar el limnímetro en fallo ya que el modelo utiliza medidas anteriores del mismo sensor en fallo. Por ello se ha optado por diseñar un banco de observadores de todos los limnímetros donde cada observador utiliza diversas medidas reales (Staroswiecki, 2004).

En la Figura 10 se presentan los resultados de la reconstrucción del limnímetro L80 utilizando un observador basado en el la medida del limnímetro L16:

$$\hat{L}_{80}(k+1) = a_{80}\hat{L}_{80}(k) + b_{47}L_{47}(k) + K(L_{16}(k) - \hat{L}_{16}(k)) \quad (17)$$

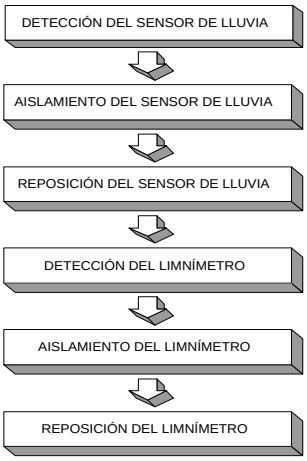


Figura 9. Ciclo de detección, aislamiento y reposición de fallos.

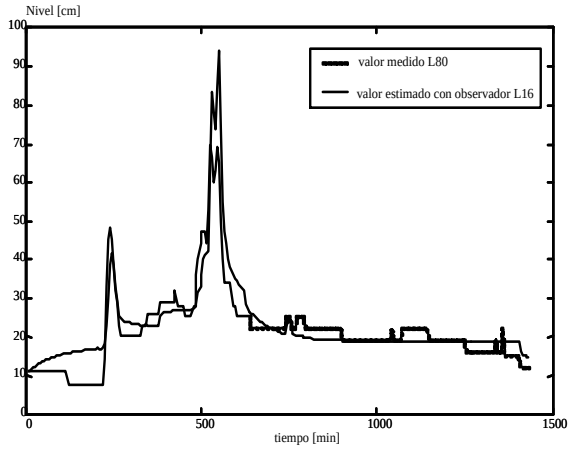


Figura 10. Reconstrucción limnímetro L80.

utilizando para ello el modelo de depósitos virtuales presentado en (Cembrano, 2004).

6.2 Tolerancia a fallos en actuadores

La tolerancia a fallos en los actuadores (compuertas de retención y desviación) se basa en primer lugar en el diagnóstico de fallo utilizando modelos y a continuación la reconfiguración de la ley de control. Los modelos utilizados para el diagnóstico son modelos estáticos no lineales que relacionan la posición de la compuerta con el nivel aguas arriba y aguas abajo medido mediante los correspondientes limnímetros de acuerdo con:

$$L_{down}(k) = f(L_{up}(k), u(k)) \qquad (18)$$

donde$L_{up}(k)$ y $L_{down}(k)$ son los niveles antes y después de la compuerta y $u(k)$ es la posición de la compuerta. Esta ecuación permitirá definir una relación de redundancia analítica para cada compuerta que junto con las relaciones de redundancia analítica del resto de limnímetros permitirán detectar y aislar fallos en las compuertas.

Puesto que el algoritmo de control global de la red de alcantarillado se basa en un control óptimo predictivo (Cembrano, 2004), la incorporación la reconfiguración de la ley de control es relativamente simple una vez el fallo en la compuerta ha sido diagnosticado (Maciejowski, 2001). Una posible reconfiguración de la ley de control consiste en modificar el programa de optimización modificando la restricción que define los límites operativos de la compuerta a los nuevos límites operativos estimados por el operador o por el sistema de diagnóstico. De esta forma el modelo de la planta incorporará el cambio de la restricción debido al fallo en la compuerta y la tendrá en cuenta de cara a la generación de las futuras estrategias de control.

Para demostrar el funcionamiento de esta estrategia de reconfiguración frente a fallos en las compuertas se van a presentar los resultados del control sobre el escenario de lluvia correspondiente al 14 de septiembre de 1999 en dos situaciones de la compuerta de salida del depósito real u_3:

- Funcionamiento sin fallo.
- Funcionamiento con fallo con bloqueo de la compuerta de retención del depósito de la Escuela Industrial de forma que sólo puede operar en el rango de apertura del 0 % al 50 %.

En la Figura 11 se muestra la intensidad de la lluvia en dicho escenario medida por el pluviómetro P16.

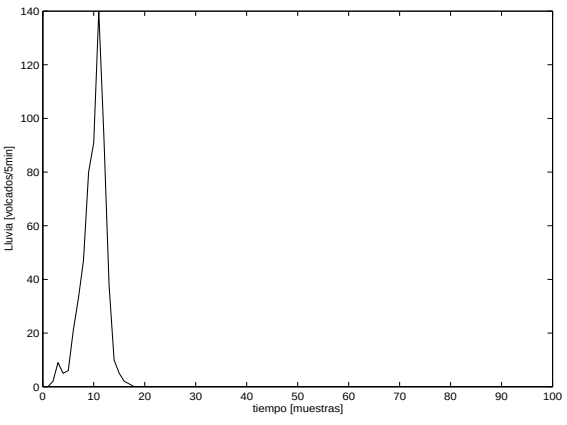


Figura 11. Medida del pluviómetro P16 para el escenario de lluvias 14/09/1999.

En la Figura 12 se presenta el volumen del depósito de regulación de la "Escuela Industrial" cuando el control óptimo de la red está operando con normalidad o con un fallo operativo en la compuerta u_3 respectivamente. Se puede observar, que en la situación normal se utiliza hasta el límite de la

capacidad total del depósito y en consecuencia retiene más agua que en la situación de fallo.

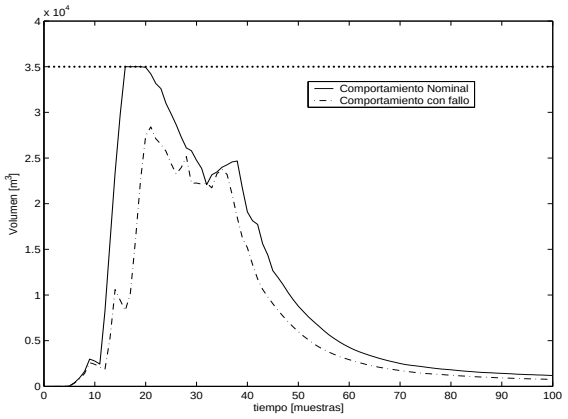


Figura 12. Volumen del depósito real.

La Figura 13 representa el volumen de agua vertido al mar (polución) en los dos casos estudiados y se puede observar que el control óptimo busca una alternativa al control de las compuertas que mantiene prácticamente igual la polución en el mar a pesar de que en el segundo caso, el depósito de retención no ha acumulado tanta agua como en el primer caso. Sin embargo, la estrategia de control óptimo en caso de fallo (control degradado) tiene un efecto negativo lógicamente en el incremento de volumen que se vierte a la calle (inundación), como se puede ver en las Figuras 14 y 15, que corresponden al volumen de agua a la calle en la cuenca asociada al depósito virtual 2 (V_2) y al volumen de agua a la calle del colector q_{24} respectivamente.

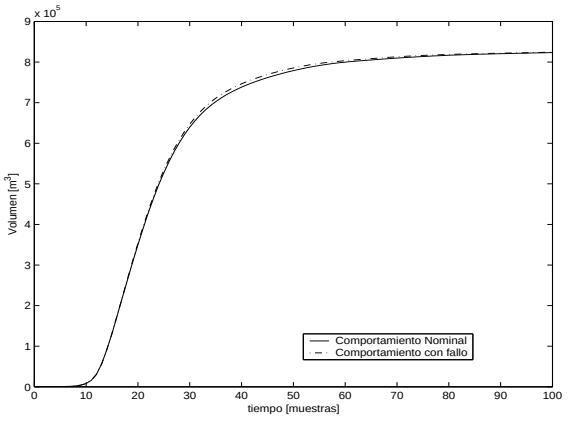


Figura 13. Volumen de agua vertido al mar.

7. CONCLUSIONES

Como se ha visto en este trabajo, una vez se ha diagnósticado el fallo existe la posibilidad de activar un conjunto de mecanismos de tolerancia

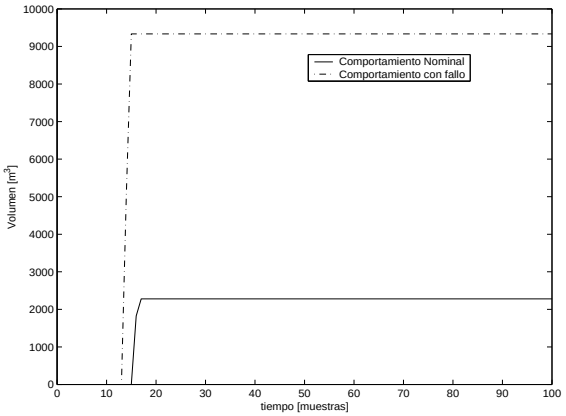


Figura 14. Volumen de agua a la calle en la cuenca asociada al depósito virtual 2 (V_2).

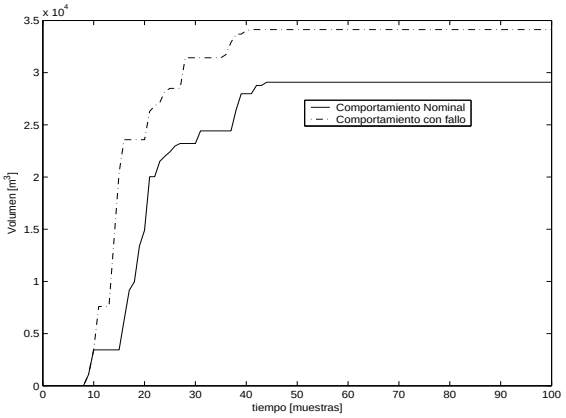


Figura 15. Volumen de agua a la calle del colector q_{24}.

a fallos de forma que el sistema de control pueda continuar operando. Estos mecanismos van desde el resideño de la ley de control (off-line o on-line) hasta la reposición/substitución de sensores y/o actuadores. El diseño de los mecanismos de tolerancia a fallos abre una serie de problemas teóricos no tratados habitualmente en la literatura de control como: la evaluación de la capacidad de recuperabilidad y la degradación del proceso controlado en fallo, diseño de instrumentación pensando en la reposición después de un fallo, rediseño de leyes de control parametrizadas en función del fallo, estimación de la magnitud de fallo y su compensanción mediante el reajuste de la ley de control, entre otras. El diseño de sistemas de control tolerante integra, pues, un conjunto de técnicas a aplicar de forma metodológica como son detección y diagnóstico de fallos, análisis estructural, reposición de sensores y actuadores, la acomodación al fallo o la reconfiguración del sistema, que actualmente aún son motivo de investigación y desarrollo.

Otro aspecto importante no resuelto es el diseño de supervisores basados en eventos discretos. El sistema supervisor realiza de forma integrada y en tiempo real todas las tareas del control tolerante a fallos. Su implementación se puede realizar utilizando paquetes comerciales ya existentes como los bien conocidos SCADA's con capacidad para programar estas funcionalidades o bien pueden ser realizados mediante módulos específicos de control tolerante con funciones distribuidas mediante agentes y con gran capacidad de comunicación en tiempo real y cumpliendo estándares informáticos que permitan una reutilización de los módulos diseñados y una fácil comunicación entre ellos.

Por otro lado, el modelado completo del sistema supervisor (sistema discreto) junto con el sistema controlado (sistema continuo) se puede realizar como un sistema híbrido. La teoría de sistemas híbridos actualmente se encuentra en fase de desarrollo siendo su aplicación al análisis y diseño de sistemas de control tolerante por desarrollar.

En la parte final del artículo, se ha presentado una aplicación de control: el control global de la red de alcantarillado que debido a que su funcionamiento requiere la disponibilidad de un gran número de sensores y actuadores que deben de funcionar en condiciones adversas (episodios de lluvia) es normal la aparición de fallos en los mismos o en los equipos de comunicaciones. Para garantizar que a pesar de la presencia de dichos fallos el control global pueda continuar operando se hace indispensable dotar la sistema de mecanismos de tolerancia tanto en los sensores como en la propia ley de control.

Tal como se ha comentado, en la primer artículo de control tolerante, dada la juventud e interés teórico y aplicado del tema, existe un importante colectivo de grupos de investigación muy activos a nivel internacional que cooperan entre ellos (DAMADICS, BRIDGE, CHEM, IFATIS, FTCOSY, DEFTAC) para dar respuestas teóricas y aplicadas a los problemas descritos lo que permite augurar soluciones reales fiables de control tolerante en los próximos años.

8. AGRADECIMIENTOS

Este trabajo ha sido subvencionado por la CICYT del Ministerio de Ciencia y Tecnología Español (DPI2002-0350) y por la DGR de la Generalitat de Catalunya (grupo SAC 2001/SGR/00236). Los autores también desean agradecer el apoyo recibido por la empresa CLABSA S.A. en la aplicación de este trabajo.

REFERENCIAS

Attouche, S., Hayat S. y Staroswiecki M. (2001). An efficient algorithm for the design of fault tolerant multi-sensor system. *Proceedings of the 40th IEEE Conference on Decision and Control* **2**, 1891–1892.

Aufderheide, B., Prasad V. y Bequette B.W. (2001). A comparison of fundamental model-based and multiple model predictive control. *Proceedings of the 40th IEEE Conference on Decision and Control* **5**, 4863–4868.

Ayza, J. (n.d.). Núcleo de los sistemas integrados de automatización de la empresa.

Bao, J., Zhang W. y Lee P. (2003). Decentralized fault-tolerant control system design for unstable processes. *Chemical Engineering Science* **58**, 5045–5054.

Bennett, S. M., Patton R. J. y Daley S. (1999). Sensor fault-tolerant control of a rail traction drive. *Control Engineering Practice* **7**, 217–225.

Blanke, M. (1999). Fault-tolerant control systems. In: *New Trends in Advanced Control*. Springer-Verlag.

Blanke, M., Kinnaert M. Lunze J. y Staroswiecki M. (2003). *Diagnosis and fault-tolerant control*. Springer-Verlag. Germany.

Bonivento, C., Isidori A. Marconi L. y Paoli A. (2004). Implicit fault-tolerant control: application to induction motors. *Automatica* **40**, 355–371.

Cassandras, C.G., Lafortune S. y Olsder G.J. (1995). Introduction to the modelling, control and optimisation of discrete event systems. In: *Trends in Control* (A. Isidori, Ed.). Springer-Verlag.

Cembrano, G., Quevedo J. Salamero M. Puig V. Figueras-J. y Martí J. (2004). Optimal control of urban drainage systems: a case study. *Control Engineering Practice*.

Chen, J., Patton R.J. y Chen Z. (1998). An lmi approach to fault-tolerant control of uncertain systems. *Held jointly with IEEE International Symposium on Computational Intelligence in Robotics and Automation (CIRA), Proceedings of the 1998 IEEE International Symposium on Intelligent Systems and Semiotics (ISAS)* pp. 175–180.

Cho, Y., Kim K. y Bien Z. (1990). Fault tolerant control using a redundant adaptive controller. *Proceedings of the 29th IEEE Conference on Decision and Control* **3**, 1467–1468.

Dardinier-Maron, V., Hamelin F. y Noura H. (1999). A fault-tolerant control design against major actuator failures: application to a three-tank system. *Proceedings of the 38th IEEE Conference on Decision and Control* **4**, 3569–3574.

Diao, Y. y Passino, K.M. (2001a). Stable fault-tolerant adaptive fuzzy/neural control for a

turbine engine. *IEEE Transactions on Control Systems Technology* **9**, 494–509.

Diao, Y. y Passino, K.M. (2001b). Intelligent fault tolerant control using adaptive schemes and multiple models. *Proceedings of the 2001 American Control Conference* **4**, 2854–2859.

Diao, Y. y Passino, K.M. (2002). Intelligent fault-tolerant control using adaptive and learning methods. *Control Engineering Practice* **10**, 494–509.

Figueras, J., Puig V. Quevedo J. (2004). Contribution to the optimal control of sewage networks including fault-tolerant capabilities. *1ª Jornada de Investigación en Automática, Visión y Robótica. Universidad Politécnica de Cataluña.*

Ganguli, S., Marcos A. y Balas G. (2002). Reconfigurable lpv control design for boeing 747-100/200 longitudinal axis. *Proceedings of the American Control Conference.*

Gopinathan, M., Boskovic J.D. Mehra R.K. y Rago C. (1998). A multiple model predictive scheme for fault-tolerant flight control design. *Proceedings of the 37th IEEE Conference on Decision and Control* **2**, 1376–1381.

Hao, C., Xianjun M. Fang X. Tao S. y Guilin X. (2002). Fault tolerant control for switched reluctance motor drive. *IEEE 28th Annual Conference of the Industrial Electronics Society* **2**, 1050–1054.

Hoblos, G., Staroswiecki M. y Aitouche A. (2000). Optimal design of fault tolerant sensor networks. *Proceedings of the 2000 IEEE International Conference on Control Applications* pp. 467–472.

Huo, Y., Ioannou P. y Mirmirani M. (2001). Fault-tolerant control and reconfiguration for high performance aircraft: Review. *CATT Technical Report 01-11-01. University of Southern California Dept. of Electrical Engineering-Systems Los Angeles, CA 90089 California State University, Los Angeles Dept. of Mechanical Engineering.*

Huzmezan, M. y Maciejowski, J. (1998). Reconfiguration and scheduling in flight using quasi-lpv high-fidelity models and mbpc control. *Proceedings of the 1998 American Control Conference* **6**, 3649–3653.

Ikeda, K. y Shin, S. (1995). Fault tolerant decentralized adaptive control systems using backstepping. *Proceedings of the 34th IEEE Conference on Decision and Control* **3**, 2340–2345.

Jiang, J. (1994). Design of reconfigurable control systems using eigenstructure assignment. *International Jounal of Control* **59**, 395–410.

Kung, Chung-Chun (1992). Optimal model matching control for mimo continuous-time systems. *Proceedings of Singapore International Conference on Intelligent Control and Instrumentation* **1**, 42–47.

Liang, Y., Liaw D. y Lee T. (2000). Reliable control of nonlinear systems. *IEEE Transactions on Automatic Control* **45**, 706–710.

Liao, F., Wang J. y Yang G. (2002). Reliable robust flight tracking control: an lmi approach. *IEEE Transactions on Control Systems Technology* **10**, 76–89.

Lunze, J. y Steffen, T. (2003). Control reconfiguration by means of a virtual actuator. *In Proceedings of IFAC Symposium on SAFEPROCESS* pp. 133–138.

Lyshevski, S., Dunipace K. y Colgren R. (1999). Identification and reconfigurable control of multivariable aircraft. *Proceedings of the American Control Conference.*

Maciejowski, J.M. (2001). Predictive methods in fault-tolerant control. In: *Control of Complex Systems* (K.J Aström et al., Ed.). Springer-Verlag.

Maciejowski, J.M. y Ramirez, W.F. (1993). Controlling systems in the face of faults. *IEE Colloquium on Fault Diagnosis and Control System Reconfiguration.*

Maki, M., Jiang J. y Hagino K. (2001). A stability guaranteed active fault-tolerant control system against actuator failures. *Proceedings of the 40th IEEE Conference on Decision and Control* **2**, 1893–1898.

Meng Ji, Zhang, Z. Biswas G. y SarkarÑ. (2003). Hybrid fault adaptive control of a wheeled mobile robot. *IEEE/ASME Transactions on Mechatronics* **8**, 226–233.

Morari, M., Baotic M. y Borrelli F. (2003). Hybrid systems modeling and control. *European Journal of Control* **9**, 177–189.

Murray Wonham, W. (1978). *Linear Multivariable Control: A Geometric Approach.* Springer Verlag. 2nd edition.

Notash, L. y Huang, L. (2003). On the design of fault tolerant parallel manipulators. *Mechanism and Machine Theory* **38**, 85–101.

Noura, H., Sauter D. Hamelin F. y Theilliol D. (2001). Fault-tolerant control in dynamic systems: application to a winding machine. *IEEE Control Systems Magazine* **20**, 33–49.

Patton, R. J. (1997). Fault-tolerant control: the 1997 situation. *Proceedings of IFAC Symposium on SAFEPROCESS* pp. 1033–1055.

Puig, V., Quevedo J. Escobet T. Moncego B. y Ocampo C. (2004). Control tolerante a fallos (parte i): Fundamentos y diagnóstico. in press.

Puig, V. y Quevedo, J. (2001). Fault-tolerant pid controllers using a passive robust fault-detection approach. *Control Engineering Practice* **9(11)**, 1221–1234.

Qu, Z., Ihlefeld C.M. Yufang J. y Saengdeejing A. (2001). Robust control of a class of nonlinear uncertain systems. fault tolerance against sensor failures and subsequent self re-

covery. *Proceedings of the IEEE Conference on Decision and Control* **2**, 1472–1478.

Qu, Z., Ihlefeld C.M. Yufang J. y Saengdeejing A. (2003). Robust fault-tolerant self-recovering control of nonlinear uncertain systems. *Automatica* **39**, 1763–1771.

Staroswiecki, M., Hoblos G. y Aitouche A. (2004). Sensor network design for fault tolerant estimation. *International Journal of Adaptive Control and Signal Processing* p. in press.

Tao, G., Chen Sh. y Joshi S.M. (2002). An adaptive control scheme for systems with unknown actuator failures. *Automatica* **38**, 1027–1034.

Theilliol, D. (2003). Contribution à l'étude et au développement des systèmes tolérants aux defaults: diagnostic et accommodation à base de modèles linéaires et au-delà. *Habilitation à Diriger des Recharches*.

Veres, S.M. y Xia, H. (1998). Dual predictive control for fault tolerant control. *International Conference on Control UKACC (Conf. Publ. No. 455)* **2**, 1163–1168.

Wang, J. y Shao, H. (2000). Delay-dependent robust and reliable h_∞ control for uncertain time-delay systems with actuator failures. *Journal of the Franklin Institute* **337**, 781–791.

Wasser, D.J., Hislop D.W. y Johnson R.N. (1989). Evaluation of a neural network for fault-tolerant real-time adaptive control. *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biologu Society. Images of the Twenty-First Century* **6**, 2027–2028.

Wu, X. y Campion, G. (2004). Fault detection and isolation of systems with slowly varying parameters: simulation with a simplified aircraft turbo engine model. *Mechanical Systems and Signal Processing* **18**, 353–366.

Zhang, Y. y Jiang, J. (2000). Design of proportional-integral reconfigurable control systems via eigenstructure assignment. *Proceedings of the American Control Conference* **6**, 3732–3736.

Zhang, Y. y Jiang, J. (2001). Integrated active fault-tolerant control using imm approach. *IEEE Transactions on Aerospace and Electronic Systems* **37**, 1221–1235.

Zhang, Y. y Jiang, J. (2002). Active fault-tolerant control system against partial actuator failures. *IEE Proceedings on Control Theory and Applications* **149**, 95–104.

Zhang, Y. y Jiang, J. (2003). Bibliographycal review on reconfigurable fault-tolerant control systems. *Proceedings IFAC SAFEPROCESS* pp. 265–276.

Zhang, Y.M. y Jiang, J. (1999). Design of integrated fault detection, diagnosis and reconfigurable control systems. *Proceedings of the IEEE Conference on Decision and Control* **4**, 3587–3592.

Zhao, Q. y Jiang, J. (1998). Reliable state feedback control system design against actuator failures. *Automatica* **34**, 1267–1272.

Zhou, Yu-guo, Zhang Ying-wei y Wang Fu-li (2002). A new type of reconfigurable control against actuator faults. *Proceedings of the 4th World Congress on Intelligent Control and Automation* **4**, 2710–2713.

Zidani, F., Benbouzid M. Diallo-D. y Benchaib A. (2003). Active fault-tolerant control of induction motor drives in ev and hev against sensor failures using a fuzzy decision system. *IEMDC'03. IEEE International Conference in Electric Machines and Drives* **2**, 677–683.