Detección y diagnóstico temprano de fallos para mejorar la seguridad de proceso y la confiabilidad: aplicación en un proceso de refinería

Early Fault Detection and Diagnosis to Process Safety and Reliability: Application in a Refinery Process

Carlos Agudelo*
Francisco Morant Anglada**
Eduardo Quiles Cucarella***
Emilio García Moreno****
Antonio Corredor Salvador*****

RESUMEN

En el presente artículo mostramos la integración de técnicas para la detección temprana y el diagnóstico de fallos en procesos industriales, con el propósito de hacer recomendaciones al personal de operaciones en un proceso industrial y evitar eventos de seguridad de proceso. La detección temprana y el diagnóstico de fallos permiten asistir al personal de operaciones en una planta industrial para tomar las mejores acciones durante el estado real del proceso, evitando que los fallos incipientes escalen a situaciones críticas donde existe el riesgo de pérdida de vidas humanas, daños al medio ambiente y pérdidas económicas. Se muestra un prototipo en una unidad de *Cracking Catalítico Fluidizado*.

Palabras clave: detección de fallos, diagnóstico, ingeniería del conocimiento, sistemas de alarmas, *cracking* catalítico fluidizado.

ABSTRACT

The present article shows the integration of techniques for the early fault detection and diagnosis in industrial processes, in order to make recommendations to the operations staff in an industrial process and avoid safety incidents. The early fault detection and diagnosis provides assistance to the operations team in an industrial plant in order to make the right decisions during the process. This prevents small faults from escalating to critical situations where risks such as loss of human lives, damages to the environment or economic loss may exist. The article presents a prototype in a fluidized catalytic cracking unit.

Keywords: Fault detection, knowledge engineering, alarm systems, fluidized catalytic cracking.

Fecha de recepción: 12 de junio del 2012 • Fecha de aprobación: 17 de septiembre del 2012

* Vinculado al Instituto Colombiano del Petróleo – Ecopetrol S.A., Bucaramanga, Colombia. Correo electrónico: carlos.agudelo@ecopetrol.com.co.
** Vinculado a la Universidad Politécnica de Valencia, Valencia, España. Correo electrónico: fmorant@isa.upv.es.
*** Vinculado a la Universidad Politécnica de Valencia, Valencia, España. Correo electrónico: equiles@isa.upv.es.
**** Vinculado a la Universidad Politécnica de Valencia, Valencia, España. Correo electrónico: emilio@isa.upv.es.
***** Vinculado a la Universidad Politécnica de Valencia, Valencia, España. Correo electrónico: ancorsal@ai2.upv.es.

Introducción

La seguridad de proceso tiene que ver con la prevención de eventos catastróficos de muy baja probabilidad de ocurrencia pero de un alto impacto en las organizaciones. Nombres como Chernobyl, Bhopal o Piper Alpha son muy conocidos en ambientes industriales, por las tragedias que significaron, no solo para los trabajadores involucrados sino para la comunidad circundante y el daño ecológico causado (Norman, 1986; Reason, 1987; Salge y Milling, 2006; Belke y Dietrich, 2001; Shrivastava, 1987; Drysdale y Sylvester-Evans, 1998; Paté-Cornell, 1993).

Estos nombres nos recuerdan que la seguridad siempre debe acompañar los avances tecnológicos. Estos accidentes (con la pérdida en vidas humanas, daño ambiental, pérdidas económicas, consideraciones éticas y morales) son incentivos para centrar nuestro trabajo en la seguridad de proceso y evitar que accidentes como estos ocurran en el futuro.

A través del uso de herramientas de *software* avanzadas se puede ayudar al personal de operaciones de una planta industrial a evitar que los fallos incipientes escalen a situaciones más graves. En el presente artículo se muestra el uso de técnicas para la detección temprana y el diagnóstico de fallos en procesos industriales, y cómo estas técnicas pueden generar recomendaciones al personal de operaciones.

La seguridad de proceso y el control automático

Bakolas y Saleh (2011) muestran cómo es necesario incrementar la observabilidad para evitar los eventos de seguridad de proceso. Un sistema se dice que es observable si se puede determinar el comportamiento de todo el sistema a partir de la medición de las salidas de este, en caso contrario los valores actuales de algunos de sus estados no podrán determinarse a partir de los sensores de salida, lo que implicará que su valor permanecerá desconocido para el controlador, y no se podrán cumplir las especificaciones de control de estas salidas.

En Saleh y Cummings (2011) se muestra cómo para mantener un control efectivo de los peligros y establecer un conjunto de defensas para bloquear los accidentes, es importante diagnosticar los indicios por los que una situación está creciendo hacia un escenario peligroso.

El sistema de control ayuda a evitar que las situaciones críticas se alcancen a través de las estrategias de control por sobremando (Smith y Corripio, 1997), pero se necesita un sistema que le indique al personal de operaciones qué fallos complejos se están empezando a presentar en la planta industrial, aumentando la observabilidad del proceso, aquí es donde entra en escena la detección y el diagnóstico de fallos.

El sistema de alarmas de la planta industrial

Hay normas y guías internacionales (ISA 18.2; EEMUA 191, entre otras) para enfrentar el problema de la inundación de alarmas (activación de demasiadas alarmas en el sistema de control electrónico). Una alarma es una indicación visual y auditiva de que una situación anormal está presente en el proceso, y el personal de operaciones debe implementar alguna acción inmediata, y cuyas implicaciones son bien conocidas por todo el personal involucrado. Las alarmas están asociadas a los límites aceptables para las variables del proceso, configuradas en el sistema de control electrónico para indicar violaciones por límite bajo y límite alto. También hay alarmas en el sistema de parada de emergencia para alertar al personal de operaciones acerca de una parada de emergencia inminente.

Las alarmas deben direccionar la atención del operador para evaluar apropiadamente las acciones que responden a las condiciones actuales del proceso, evitando información redundante, para reducir el riesgo en las personas, el medio ambiente y los equipos (Acero et ál., 2005a). Desafortunadamente es común encontrar alarmas que confunden al operador en lugar de ayudarlo, inundando el sistema con demasiados eventos, no solo durante las situaciones de emergencia sino también durante la operación normal. Por esto es urgente optimizar la información de las alarmas del proceso, priorizar aplicando una metodología para analizar operaciones peligrosas (Acero et ál., 2005b y 2005c). Para hacer esto hemos aplicado estándares internacionales (EEMUA Publication 191 "A guide to design, management and procurement of Alarms Systems") definiendo criterios para la optimización de las alarmas, criterios para la medición del desempeño y puntos de referencia durante operación normal y durante escenarios de fallo.

Hemos aplicado esta metodología para muchas plantas en las refinerías de Barrancabermeja y Cartagena (Colombia). Hemos dividido esta metodología en fases: fase 1, tiene que ver con los "malos actores" de alarmas, que son las alarmas que más

se activan en la planta. Detectamos estos "malos actores" utilizando herramientas estadísticas sobre los reportes históricos de alarmas del sistema de control electrónico. Con un equipo interdisciplinario (integrado por el ingeniero electrónico responsable del sistema de control, el ingeniero químico responsable del proceso, operador y supervisor experto de la planta, y el facilitador de alarmas), se analiza por qué estas alarmas se están activando. Algunas veces es por problemas de configuración del sistema de control (como ajuste erróneo de parámetros), algunas veces es por problemas de sintonía de lazos de control, algunas veces es por problemas de límites. La fase 2 es racionalización de alarmas, realizando el análisis a todas las alarmas de la planta, eliminando alarmas redundantes, y alarmas que no son realmente alarmas sino actividades de mantenimiento. La fase 3 es gerenciamiento inteligente de alarmas, que es la aplicación de herramientas de *software* avanzadas para realizar detección temprana y diagnóstico de fallos. El monitoreo del desempeño de la planta, la detección temprana y el diagnóstico de fallos pueden ser asistidos por herramientas de *software* avanzadas para incrementar la confiabilidad.

Muchas técnicas para la detección y el diagnóstico de fallos han sido desarrolladas y comprobadas en ambientes industriales, mostrando sus fortalezas y debilidades. Hemos estudiado la integración de técnicas para la detección temprana y el diagnóstico de fallos para incorporar lo mejor de cada una de ellas para detectar situaciones anormales en procesos complejos. Las técnicas para la detección temprana y el diagnóstico de fallos asisten al personal de operaciones en la toma de las mejores decisiones, evitando que fallos incipientes escalen a situaciones críticas. Las técnicas para la detección temprana y el diagnóstico de fallos integradas utilizan la información disponible en ambientes industriales. Hemos desarrollado una herramienta prototipo en una unidad de *cracking* catalítico fluidizado (FCC).

Integracion de técnicas

Pérdida de vidas e impacto económico se ha registrado en la industria petroquímica debido al manejo inapropiado de situaciones anormales (Venkatasubramanian et ál., 2003; Marsh Risk Consulting, 2001). Los atributos deseados para un sistema de detección y diagnóstico de fallos han sido definidos previamente (Venkatasubramanian et ál., 2003): detección temprana y diagnóstico de fallos; discriminación entre diferentes fallos; robustez en presencia de ruido e incertidumbre; identificación de nuevos fallos; identificación de múltiples fallos; facilidad de explicación

de resultados y adaptabilidad. Comparando diferentes métodos para la detección y el diagnóstico de fallos, de acuerdo con estos criterios, ninguna de las técnicas usadas hasta ahora cubre todos los atributos de evaluación (Dash y Venkatasubramanian, 2003; Biswas et ál., 2004). Como resultado de esta comparación, una nueva aproximación se necesita para utilizar estas técnicas. Proponemos una posible solución utilizando una arquitectura integrada combinando tres métodos, utilizando herramientas de inteligencia artificial.

Revisamos las técnicas existentes para realizar detección y diagnóstico de fallos. Pusimos especial interés en aquellas técnicas que usan información disponible en procesos industriales: las alarmas asociadas a los límites operacionales de las variables de proceso; la experiencia del personal de operaciones en fallos comunes y registradas en forma de reglas; un modelo simplificado de la planta (respuesta escalón unitario) que permite predecir el comportamiento dinámico durante la operación normal y los escenarios de fallo. Hemos desarrollado un diccionario extendido de fallos e implementado un sistema de inferencia lógica para integrar los síntomas y los resultados de cada técnica de detección y diagnóstico de fallos.

Un sistema de inferencia lógica ha sido utilizado para incorporar la mejor de las técnicas utilizadas, compilando el conocimiento experto en reglas que tienen la forma: si "antecedente" es verdadero entonces "consecuente" es verdadero, capturando las relaciones causales en el proceso.

El proceso de inferencia para validar las hipótesis de fallo se realiza a través del encadenamiento hacia atrás. El modelo utilizado para detectar perturbaciones (una forma temprana en la que los fallos se muestran en el proceso) es un modelo respuesta escalón unitario, utilizado en el control multivariable de la planta para predecir el comportamiento de las variables controladas basado en los movimientos calculados para las variables manipuladas.

La información disponible (de las alarmas y de las otras técnicas) es incorporada en el diccionario extendido de fallos (Agudelo et ál., 2007). Esta información es perturbaciones detectadas utilizando el modelo respuesta escalón del proceso; similitud entre la secuencia de alarmas observada y secuencias identificadas previamente durante escenarios de fallo; síntomas observados durante escenarios de fallo (de la base de conocimiento experto en detección y diagnóstico de fallos). Los síntomas de los que hablamos son los antecedentes de las reglas de la base de

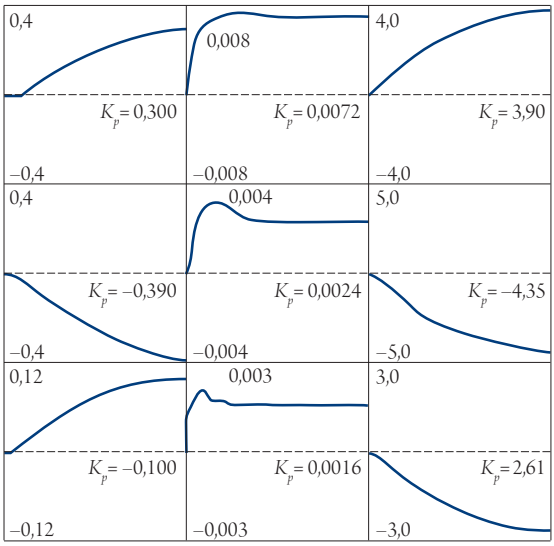

Figura 1. **Modelo respuesta escalón unitario utilizado para detectar perturbaciones en el proceso**

Fuente: Process dynamics and control (2010).

conocimiento experto, que replican el mecanismo de inferencia utilizado por el personal de operaciones en detección y diagnóstico de situaciones anormales.

Las alarmas deben ser vistas como herramientas para la detección y el diagnóstico de fallos. En la figura 2 las secuencias de alarmas para los fallos principales del proceso se han representado. Estas secuencias fueron construidas a partir de un análisis FMEA (análisis de efectos y modos de fallo) realizado en el proceso (Suttinger et ál., 2005).

La ingeniería del conocimiento tiene metodologías para construir la base de conocimiento con la experiencia del personal de operaciones (Russell y Norvig, 1996): definición de términos que se van a incluir en el modelo, variables influenciándolo; codificación cualitativa y cuantitativa de la dependencia de variables; casos especiales; consulta a procedimientos de inferencia para validar las respuestas de los expertos; y análisis de sensibilidad para establecer la robustez en presencia de perturbaciones.

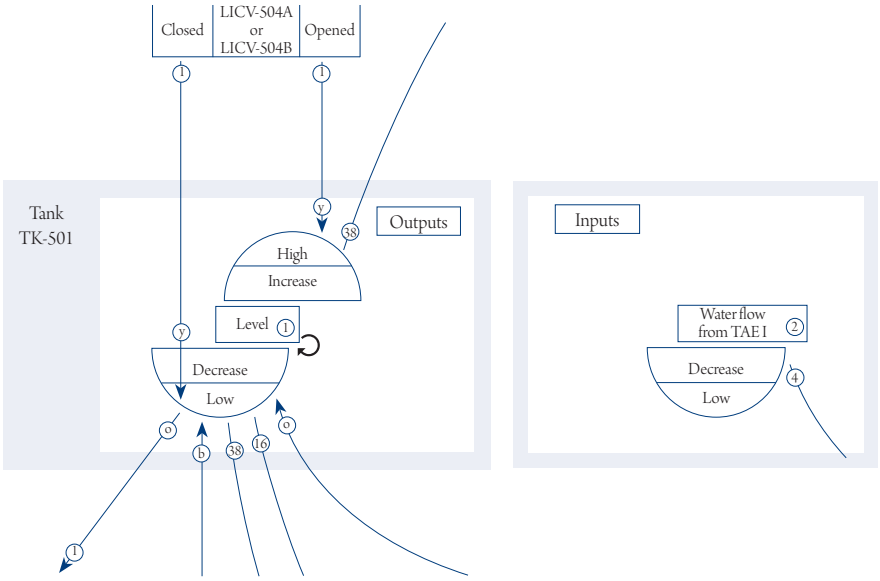

Figura 2. **Secuencias de alarmas de los fallos principales del proceso**

Fuente: elaboración propia.

El diccionario extendido de fallos

La integración de técnicas para la detección y el diagnóstico de fallos deben resolver conflictos cuando los resultados de cada técnica no coinciden. Cada una de las técnicas no detecta todos los fallos posibles. La información de diagnóstico proveniente de diferentes fuentes debe ser fusionada correctamente (estampas de tiempo ordenadas para los eventos del sistema, resultados actualizados de cada técnica de diagnóstico, monitoreo del desempeño de equipos para validar hipótesis, etc.). La información disponible (de las alarmas y de las otras técnicas) es incorporada en el diccionario extendido de fallos (Agudelo et ál., 2007) (figura 3).

La herramienta de *software* imita el proceso de inferencia que realizan los operadores al analizar una situación anormal, realizando encadenamiento hacia atrás de las reglas de la base de conocimiento. Estas reglas registran las hipótesis de fallo posibles y son construidas a partir del diccionario extendido de fallos. La regla *ij* será:

$$S_{ij} \wedge Mode(m) \Rightarrow f_j \qquad (1)$$

	t_1	t_2	t_3	$\cdots$	t_r	*Mode*
f_0	S_{10}	S_{20}	S_{30}		S_{r0}	m_0
f_1	ϕ	S_{21}	S_{31}		S_{r1}	$m_1.m_2$
f_2	S_{12}	S_{22}	ϕ		S_{r2}	m_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	
f_n	S_{1n}	S_{2n}	S_{3n}	$\cdots$	S_m	m_m

Figura 3. Diccionario extendido de fallos

Fuente: elaboración propia.

Donde:

La hipótesis de fallo (f_j) está en el lado consecuente.
Los síntomas de validación (S_{ij}) están en el lado antecedente junto con el modo de operación en el que la hipótesis de fallo es válida.

Hay cinco modos utilizados para representar las condiciones del proceso: modo de arrancada, producción normal, producción con defectos, modo de parada y modo de emergencia. La transición entre los modos es estimada monitoreando las condiciones operacionales del proceso, tal como se muestra en Cáceres y Ropero (2006).

Prototipo

Una herramienta inteligente de *software* que realiza detección y diagnóstico de fallos ha sido construida a partir de los conceptos anteriores en una unidad de FCC, localizada en la refinería de Barrancabermeja (Colombia). La base de conocimientos requerida para construir la aplicación se recopiló a través de entrevistas con los operadores, supervisores e ingenieros, expertos en el proceso, utilizando la metodología apropiada (Brulé, 1989). La herramienta de *software* ha sido construida utilizando C++ Builder.[1] Una herramienta prototipo para conectarse con la base de datos en tiempo real de la refinería también fue construida. La conexión entre estas dos plataformas se logra a través de una base de datos en SQL Server.[2]

1 Builder es marca registrada de Borland.

2 SQL Server es marca registrada de Microsoft Corporation.

Los fallos detectables por la herramienta de *software* incluyen (pero no están limitados a): problemas en la circulación del catalizador; pérdidas de catalizador; formación de coke/ensuciamiento; flujo inverso; alta temperatura del regenerador; poscombustión; problemas con la calidad y cantidad de productos. Las razones principales de estos fallos son: condiciones de operación; problemas mecánicos; características de la carga; y características del catalizador, tal y como se describe en Sadeghbeigi (2000).

Una de las reglas para detectar y diagnosticar el fallo "Circulación de catalizador limitada y flujo inverso" debido a fallas mecánicas, en la herramienta inteligente tiene los siguientes síntomas:

- Decrementa PDIC27149
- Decrementa ZI27100
- Decrementa ZI27101
- Incrementa PIC27116
- Decrementa ZI27103
- Incrementa ZI27104

Donde PDIC27149 es el *tag* para la presión diferencial entre reactor y regenerador, síntoma que indica que una baja presión diferencial entre reactor y regenerador ha sido causada (debido a taponamiento en las tomas de presión diferencial del reactor-regenerador).

ZI27100 y ZI27101 son las posiciones de las válvulas de corredera del regenerador, síntomas que indican que el sistema de control quiere presionar el regenerador.

PIC27116 es el controlador de presión del regenerador.

ZI27103 y ZI27104 son las válvulas de corredera del catalizador regenerado y gastado (entre el reactor y el regenerador) respectivamente.

Estos son síntomas que indican que el sistema de control decrementa la posición de la válvula ZI27103 para descender la presión del reactor, debido a una baja en la temperatura. La causa del fallo es "Taponamiento en la toma de presión del reactor PDIC27149". Si hay un taponamiento en las tomas del transmisor de presión diferencial, el sistema de control va a cerrar las válvulas de corredera para presionar el regenerador, incrementando la presión diferencial entre regenerador y reactor, incrementando el riesgo de que el soplador de aire baje su flujo. La recomendación al operador es poner en manual el PDIC27149 y ajustar la señal de salida de operación normal en el valor que venía antes de presentar el disturbio.

Una vez la herramienta de *software* detecta un fallo, alarma al operador, y le da las recomendaciones necesarias para prevenir que un incidente ocurra, o para ayudarle al operador a que la planta se recupere del estado de fallo de la mejor forma posible.

Al comienzo desarrollamos una conexión directa al sistema de control (para descargar en línea los valores de los instrumentos de medición de la planta y hacer la estimación de síntomas), pero luego nos dimos cuenta que esta conexión podría sobrecargar el sistema de control electrónico, lo que no es permisible en ningún caso. Por eso migramos nuestro desarrollo a una conexión con la base de datos en tiempo real de la refinería. La arquitectura del *software* se muestra en la figura 4.

Muchas pruebas se realizaron utilizando un Sistema de Entrenamiento a Operadores (OTS) de la planta, y la instalación en el proceso real en la refinería ya se hizo. Nos encontramos evaluando el impacto de la herramienta en el proceso de FCC, y la herramienta de *software* ya ha detectado y diagnosticado varios fallos en el proceso.

Mejora de la confiabilidad

La fiabilidad en ingeniería se define como la capacidad de un sistema o componente para realizar sus funciones requeridas bajo las condiciones establecidas por un periodo determinado de tiempo.

En Aranguren y Tarantino (2006) se plantean las mejoras por el uso de la detección temprana y el diagnóstico de fallos:

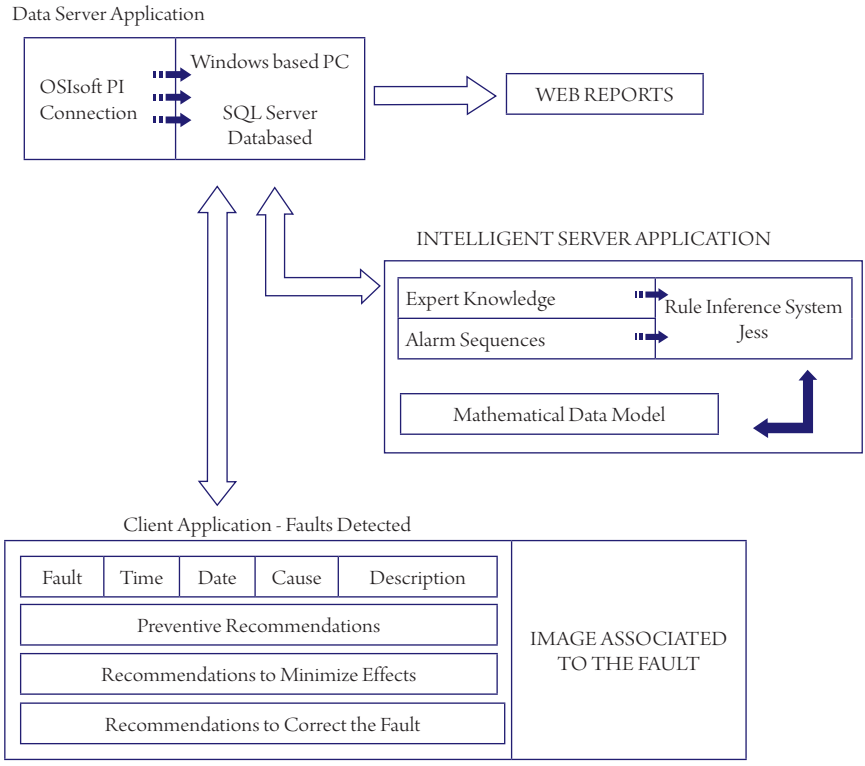

Figura 4. **Arquitectura de la herramienta de software**

Fuente: elaboración propia.

- Maximizar la vida útil del equipo
- Eficiencia en el momento de las intervenciones de los equipos
- Confiabilidad del equipo
- Seguridad de proceso
- Protección del medio ambiente
- Costos de la minimización

El uso de técnicas para la detección temprana y el diagnóstico de fallos permiten las mejoras anteriores, debido a que pueden detectar la presencia de fallos incipientes

en los sistemas bajo estudio. Esta información es necesaria para la planificación, mantenimiento basado en condiciones y la toma de decisiones. Con base en la información proporcionada por las técnicas de detección temprana y diagnóstico de fallos pueden ser definidos los modos de fallo y escenarios de fallo para el taller de mantenimiento centrado en la confiabilidad (RCM).

El uso de la detección temprana y el diagnóstico de fallos permite planificar el mantenimiento en lugar del mantenimiento no-planificado. También busca reducir el riesgo en el proceso, a través de la prevención de que las situaciones anormales incipientes escalen a situaciones más críticas.

Conclusiones

En este artículo se muestra la integración de tres técnicas para la detección y diagnóstico de fallos: alarmas en el sistema de control electrónico, la base de conocimientos en fallos del proceso basado en la experiencia del personal de operaciones y un modelo simplificado para detectar perturbaciones en las variables controladas del proceso. Este artículo sustenta el uso de herramientas de *software* avanzadas para ayudar a la detección temprana y el diagnóstico de fallos. Se muestra un prototipo de herramienta en un proceso de FCC. Se muestra cómo la detección temprana y el diagnóstico de fallos ayudan a mejorar la seguridad del proceso y la confiabilidad operacional.

Referencias

Acero, C.; Riascos, F.; Agudelo, C. y Torres, E. (2005a). *Gerenciamiento de alarmas: documento filosófico para el manejo de alarmas en la Gerencia Refinería de Cartagena*. Piedecuesta (Colombia): Instituto Colombiano del Petróleo - Ecopetrol.

Acero, C.; Riascos, F.; Agudelo, C. y Torres, E. (2005b). *Gerenciamiento de Alarmas en GRC: Diagnóstico preliminar Unidad de Ruptura Catalítica-Fase I*. Piedecuesta (Colombia): Instituto Colombiano del Petróleo - Ecopetrol.

Acero, C.; Riascos, F.; Agudelo, C. y Torres, E. (2005c). *Gerenciamiento de Alarmas en GRC: Informe de medición Post-Fase I Unidad de Ruptura Catalítica*. Piedecuesta (Colombia): Instituto Colombiano del Petróleo (Ecopetrol).

Agudelo, C. (2010). *Integración de técnicas para la detección y el diagnóstico de fallos. Aplicación a un proceso de Cracking Catalítico Fluidizado* [documento Diploma de Estudios Avanzados]. Valencia: Universidad Politécnica de Valencia.

Agudelo, C.; Quiles, E. y Morant, F. (2007). Uso de sistemas expertos en el diagnóstico de fallos en procesos complejos. *XIII Convención de Ingeniería Eléctrica*. Universidad Central María Abreu de las Villas. Villa Clara (Cuba).

Aranguren, S. y Tarantino, R. (2006). Approaches and directives for the development and application of fault detection and diagnosis systems. *Revista Colombiana de Tecnologías de Avanzada, 2*(8).

Bakolas, E. y Saleh, J. (2011). Augmenting defense-in-depth with the concepts of observability and diagnosability from Control Theory and Discrete Event Systems. *Reliability Engineering and System Safety, 96,* 184-193.

Belke, JC, Dietrich DY. (2001). Chemical accident risks in US industry-a preliminary analysis of accident risk data from US hazardous chemical facilities. *Paper presented at the 10th international symposium on loss prevention and safety promotion in the process industries*.Stockholm, Sweden.

Biswas, Cordier, Lunze, Travé-Massuyès, Staroswiecki. (2004). Diagnosis of Complex Systems: Bridging the Methodologies of the FDI and DX Communities. *IEEE Transactions on Systems, Man, and Cybernetics - Part B: Cybernetics, 34*(5), 2159-2162.

Brulé, J. (1989). *Knowledge acquisition*. Nueva York: McGraw-Hill.

Cáceres, L. y Ropero, A. (2006). *Desarrollo de un modelo de simulación para el análisis de fallos en la unidad de ruptura catalítica de la refinería de Cartagena - ECOPETROL.* [Tesis]. Bucaramanga (Colombia): Universidad Pontificia Bolivariana.

Dash y Venkatasubramanian (2003). Integrated Framework for Abnormal Event Management and Process Hazards Analysis. *AIChe Journal, 49*(1).

Drysdale, D. (1998). Sylvester-Evans R. The explosion and fire on the PiperAlpha platform, 6 July 1988. A case study. *Philosophical Transactions of the Royal Society of London Series, a Mathematical Physical and Engineering Sciences, 356*(1748), 2929-51.

Ghariani, A. K. A.; Toguyéni, E. y Craye, A. (2002). Functional Graph Approach for Alarm Filtering and Fault Recovery for Automated Production Systems, WODES. *Sixth International Workshop on Discrete Event Systems* (WODES'02).

Hamscher, W.; Console, L. y De Kleer, J. (1992). Readings in Model-based Diagnosis. California: Morgan Kaufmann Publishers Inc.

Marsh Risk Consulting. (2001). Large Property Damage Losses in the Hydrocarbon Industries, *A Third Year Review*.

Norman, C. (1986). Chernobyl-errors and design flaws. *Science, 233*(4768), 1029-31.

Paté-Cornell, M. (1993). Learning from the Piper Alpha accident. A postmortem analysis of technical and organizational factors. *Risk Analysis,13*(2), 215-232.

Reason, J. (1987). The Chernobyl errors. *Bulletin of the British Psychological Society*, 40, 201–20–>206.

Russell, S. y Norvig, P. (1996). *Artificial Intelligence: A modern approach*. New York: Prentice Hall.

Sadeghbeigi, R. (2000). *Fluid Catalytic Cracking Handbook. Gulf Professional Publishing Company* (2ª. ed.). Houston.

Saleh, J. y Cummings, A. (2011). Safety in the mining industry and the unfinished legacy of mining accidents: Safety levers and defense-in-depth for addressing mining hazards. *Safety Science, 49*, 764-777.

Salge, M. y Milling, PM. (2006). Who is to blame, the operator or the designer? Two stages of human failure in the Chernobyl accident. *System Dynamics Review, 22*(2), 89-112.

Shrivastava, P. (1987). *Bhopal: anatomy of a crisis*. Cambridge, Mass: BallingerPub.

Smith, C. y Corripio, A. (1997). *Principles and Practice of Automatic Process Control* (2ª. ed.). New York: Wiley.

Suttinger, L. et ál. (2005). *FMEA and the Installed SIS. ISA EXPO 2005 Technical Conference*. Westinghouse Savannah River Company.

Venkatasubramanian, V. et ál. (2003). A review of process fault detection and diagnosis. Part I: Quantitative model-based methods. *Computers and Chemical Engineering, 27*.