

Title

Sistemas de control de plantas químicas en situaciones de emergencia

Propuesta de proyecto de Investigación para la convocatoria de becas de Iniciación a la I+D+i de la Cátedra Repsol ETSII-UPM

Author

Laura Lanchas Fuentes
Santos Galán Casado (tutor)

Reference R-2008-B01
Release 1.0 Edición
Date 2 de junio de 2008

Address

Autonomous Systems Laboratory
UPM - ETS Ingenieros Industriales
José Gutierrez Abascal 2
28006 Madrid
SPAIN

Sistemas de control de plantas químicas en situaciones de emergencia

ASLab R-2008-B01 v 1.0 Edición de 2 de junio de 2008

Resumen

El proyecto pretende desarrollar nuevas técnicas y arquitecturas para sistemas de control de plantas químicas que en situaciones de emergencia mantengan la continuidad operativa o al menos mitiguen los daños de forma automática o colaborando con los operadores.

Área de trabajo

Sistemas avanzados de control de procesos químicos y de refino

Índice general

1. Introducción y motivación	6
1.1. Seguridad en plantas químicas	6
1.2. Sistemas de control en situaciones anormales	8
2. Propuesta	10
2.1. Identificación del área de trabajo	10
2.2. Objetivos	10
2.3. Estado de la técnica	10
2.4. Metodología	12
2.5. Plan de trabajo	12
2.5.1. Aplicación a una unidad de REPSOL-YPF	13
2.5.2. Sistemas de control en situaciones de emergencia	14
2.5.3. Banco de ensayos	15
2.5.4. Programación	16
2.6. Firma y aval del tutor	17
Bibliografía	18

Introducción y motivación

La industria química se ocupa de la transformación de materias primas en una multitud de productos que, bien directamente o bien abasteciendo a otros sectores productivos, satisfacen las principales necesidades de nuestras sociedades, tales como salud, energía o comunicaciones. Desde esta perspectiva funcional, y con el horizonte de beneficio que estructura la organización económica, la operación de una planta química está también sujeta a unas restricciones de seguridad, calidad y salubridad. El marco de competitividad mundial ha hecho que el nivel de interacción de materia y energía en las plantas haya aumentado considerablemente, lo que conduce a procesos cada vez más próximos a los límites y bajo condiciones de operación más difíciles.

Al considerar la operación de un sistema complejo de la magnitud de, por ejemplo, una refinería, hay que tener en cuenta una enorme variedad de componentes que colaboran para el correcto funcionamiento de la misma. Uno de ellos es el sistema automático de control y seguridad, que por los motivos citados viene tomando cada vez más importancia. Aquí nos interesan el funcionamiento de estos sistemas en las ocasiones en que las condiciones de la planta desbordan los límites. Nos encontramos con lo que en la literatura técnica anglosajona se está denominando «situación anormal» y que incluye desde las pequeñas perturbaciones que se pueden controlar, devolviendo la operación a su estado normal, hasta los accidentes graves.

1.1. Seguridad en plantas químicas

La seguridad en las plantas químicas está intrínsecamente relacionada con la seguridad del personal, de los equipos, y del entorno de la planta. Es

esencial que las operaciones que se realicen en las plantas sean seguras: en ellas se trabaja con grandes cantidades de material que puede ser tóxico, inflamable y/o explosivo, y las emisiones accidentales de estos materiales pueden acarrear graves problemas medio ambientales, pérdidas económicas y daños a las personas. Aunque la seguridad de la industria química es bastante más alta que lo que la prensa nos pueda hacer creer (Sanders, 2005), son muchas las vidas que se han perdido por culpa de los accidentes, algunos de ellos auténticas catástrofes (Flixborough,1974; Seveso, 1976; Bhopal, 1984), por lo que garantizar la seguridad es siempre importante.

En las plantas modernas se disponen varios niveles de protección para mantener una operación segura (fig 1.1). Cada una de las capas debe ser independiente de las demás. En primer lugar se trata de diseñar procesos intrínsecamente seguros. Por ejemplo, muchos incidentes son el resultado de fugas de materiales peligrosos, con lo cual, siempre y cuando sea posible se debe evitar el uso de estos. La siguiente capa de protección la constituye el sistema de control que regula la operación de la planta y suministra información al operador. Aunque es una capa de protección, su objetivo principal es otro. La capa de protección física está constituida por válvulas de seguridad, discos de ruptura y otros elementos similares. A este nivel nunca debería llegarse, ya que es muy difícil instalar elementos que siempre sean lo suficientemente grandes y que actúen lo suficientemente rápido en caso de emergencia. Una vez que el accidente se ha producido entrarían en juego los procedimientos de emergencia y evacuación de la planta y del entorno.

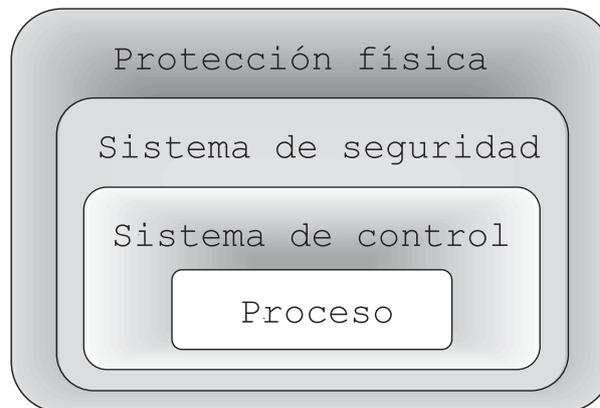


Figura 1.1: Capas de protección en plantas de proceso

La capa que realiza fundamentalmente la protección en las plantas es el sistema automático de seguridad (sistemas instrumentados de seguridad, SIS), que se sitúa entre el sistema de control y los elementos físicos de protección. Este sistema actúa de forma automática cuando se detecta una situación

anormal, intentando que el uso de los sistemas de protección física sea mínimo. Los sistemas automáticos de seguridad son fundamentalmente sistemas de control basados en lógica implementados sobre autómatas programables (PLC) redundantes y con alto nivel de integridad, específicos para esta aplicación. Entre los fabricantes de estos equipos se encuentran Allen-Bradley (Rockwell), Triconex (Invensys), Hima, Honeywell y Siemens.

En las plantas, estos autómatas implementan los enclavamientos o sistemas de fallo seguro (*Fail Safe System*). Definiciones y normas para su diseño se pueden encontrar en las publicaciones de IEC, ISA, NFPA y otras organizaciones. Es notable el cambio que ha supuesto la última generación normativa concretada en la IEC/UNE-EN 61511 *Seguridad funcional. Sistemas instrumentados de seguridad para el sector de las industrias de procesos* (UNE-EN 61511, 2006) (en el marco de la IEC/UNE-EN 61508) también adoptada como ANSI/ISA 84.00.01-2004 (sustituyendo a la precursora de 1996).

Las acciones (funciones instrumentadas de seguridad, SIF) principales de estos sistemas comprenden:

- **Paradas de emergencia:** La planta o parte, se para ante determinadas condiciones.
- **Permisivos:** Se comprueban ciertos requisitos antes de permitir una actuación.
- **Secuencias:** Se fuerza la operación en una determinada secuencia de acciones.

El sistema de seguridad opera de forma *estática*, es decir, recibe continuamente señales pero solo actúa si ocurre alguna situación anormal.

1.2. Sistemas de control en situaciones anormales

El esquema descrito ha venido garantizando la seguridad de las plantas durante muchos años y está basado en principios racionales contrastados por la experiencia. No obstante, resulta insatisfactorio, a nuestro entender por varios motivos, entre ellos:

- El sistema de control y monitorización es normalmente el primero en detectar las situaciones anormales y, junto al operador, el primero que

intenta resolverlas o mitigarlas. Pero el sistema de control está diseñado para el entorno de las condiciones nominales y puede ser de poca utilidad si nos alejamos de ellas, obligando a la intervención radical del sistema de seguridad, lo que supone con frecuencia paradas parciales o totales.

Existe un margen entre estos dos sistemas que no está contemplado en el diseño de los sistemas automáticos de la planta probablemente por su dificultad. Si bien esto era razonable en el pasado, la capacidad tecnológica del presente permite abordar el problema.

- Una vez que se ha producido el fallo o el accidente, hasta alcanzar la condición segura se está en una situación de riesgo, incertidumbre y tensión en la que no sobra ninguna ayuda. De nuevo, el sistema de control, que sigue recogiendo información de los instrumentos que han sobrevivido, no ha sido diseñado para explotarla en estas circunstancias, creando incluso confusión con el disparo incesante de alarmas.
- Aunque cueste creerlo, el diseño de la parte funcional de los sistemas automáticos de planta es relativamente primitivo. Unido a la disponibilidad de equipos y software cada vez más potentes nos encontramos con la peligrosa combinación de sistemas complejos creados de manera no sistemática. Una de las consecuencias es la situación no infrecuente de tener que desconectar el sistema de seguridad durante la puesta en marcha, porque las funciones de seguridad no permiten el arranque. Otra es la larga tradición de la «gestión de alarmas»: racionalización de la infinidad de alarmas planteadas, prácticamente una necesidad en la actualidad.

Es en estos puntos, fundamentalmente el primero y el segundo, donde se quiere trabajar en esta propuesta de proyecto de investigación.

Propuesta

2.1. Identificación del área de trabajo

En relación con la lista de áreas de interés para REPSOL-YPF que aparece en el primer apartado de la convocatoria, esta propuesta se encuadra fundamentalmente en la octava: *Sistemas avanzados de control de procesos químicos y de refino*.

2.2. Objetivos

El objetivo del proyecto es el desarrollo de nuevas técnicas y arquitecturas para sistemas de control de plantas químicas que en situaciones de emergencia mantengan la continuidad operativa o al menos mitiguen los daños de forma automática o colaborando con los operadores.

2.3. Estado de la técnica

En 1992 Honeywell y cuatro grandes petroleras (Amoco, Chevron, Exxon y Shell) establecieron un grupo de trabajo para mejorar los sistemas de alarmas en sistemas de control distribuido (DCS). Posteriormente, en 1994 se formalizó la constitución del *Abnormal Situation Management (ASM) Joint R&D Consortium* (Abnormal Situation Management Consortium, 1992) con la incorporación de otras cuatro grandes empresas (BP, Mobil, NOVA y Texaco). Este consorcio, que continúa activo, ha sido el agente principal en el estudio y desarrollo de la intervención de los sistemas de control en emergencias. Los resultados publica-

dos de los primeros años parecen ser fundamentalmente los del *Laboratory por Intelligent Process Systems (LIPS)* de la universidad de Purdue, dirigido por el profesor V. Venkatasubramanian. Se desarrolló una aplicación de diagnóstico (DKit) con arquitectura de pizarra (*blackboard*) integrando diversas técnicas de inteligencia artificial, sobre la que se implementó AEGIS (Nimmo, 1999) (*Abnormal Event Guidance and Information System*). De estos trabajos se han obtenido posteriormente varias patentes (Emigholz et al., 2008).

En la actualidad, el interés del consorcio parece centrarse en:

- Formación de operadores y entrenamiento por medio de simulación.
- Gestión de alarmas.
- Detección precoz de fallos.
- Mejora de la interfaz de usuario y el diseño de las salas de control.
- Análisis del factor humano en las situaciones de emergencia.
- Gestión de procedimientos de operación.

La orientación a los operadores de gran parte de los esfuerzos se corresponde con el dato de ser los errores humanos los responsables de más del 40 % de los incidentes. La detección precoz de fallos es otro de los temas importantes si bien en este campo existe ya una ingente producción de artículos desde diferentes planteamientos (Frank, Ding, & Marcu, 2000; Venkatasubramanian, Rengaswamy, Yin, & Kavuri, 2003c, 2003b, 2003a).

Varios de los puntos anteriores están recogidos en la herramienta GEM de la empresa 4DM Technologies (4DM Technologies, 2008). Básicamente se trata de recoger en tiempo real toda la información relevante en una situación anormal y presentarla de una manera integrada. Además se muestran al operador los procedimientos establecidos en cada caso y una predicción de la evolución ayudándose de simuladores, datos meteorológicos, etc, todo ello con una interfaz gráfica que puede señalar rutas de escape, mostrar planos o la posición de los operadores en campo ubicados mediante GPS. Desarrollado por un grupo de ex-pilotos israelíes, además de en la planta de fertilizantes de ICL, se dice que se utiliza en el aeropuerto de Tel Aviv.

La propuesta que se describe en este documento se llevaría cabo dentro del grupo de investigación del *Autonomous Systems Laboratory (ASLab)* de la UPM al que pertenece el tutor. Este grupo participa en la recién presentada propuesta de proyecto integrado (FP7) *Integrated System for Air transport Protection*

(ISAP) dentro de un consorcio de 38 miembros entre los que se encuentran SAGEM, EADS, Saab o Thales. Uno de los objetivos es desarrollar sistemas (automáticos) de supervivencia que mantengan operativo y ayuden al piloto a controlar el avión en caso de haber sido dañado por un ataque terrorista. La forma de conseguirlo se basa en la reconfiguración automática de los sistemas de vuelo por medio de la redundancia física y la reconfiguración funcional de acuerdo a los datos y equipos disponibles. También se trata aquí de la necesidad de procesar la información para que sea útil en una situación compleja como lo es una emergencia.

De todos los factores citados que influyen en una situación anormal en una planta y su gestión es en la última línea del proyecto ISAP en la que se quiere trabajar: una vez que se ha producido el incidente, que puede hacer un sistema automático de control para resolver, ayudar a resolver o mitigar el problema con los elementos que han sobrevivido.

2.4. Metodología

Además de la necesaria recopilación y análisis de información existente se plantean dos vías para encontrar soluciones realistas que se puedan contrastar sin riesgo:

1. Recabar de una planta de REPSOL-YPF datos sobre una unidad de pequeña escala, así como casos de emergencia o situaciones anormales que se puedan dar en la misma.
2. Construir un banco de pruebas simulado para esa unidad y el sistema de control propuesto para evaluar su funcionamiento, presentando posteriormente a la planta el resultado para sus comentarios.

La planta con la que se ha contactado ha sido la refinería de A Coruña que nos ha comunicado su aceptación e interés en el proyecto.

2.5. Plan de trabajo

El trabajo se organiza en torno a tres paquetes de los que se detalla tentativamente a continuación sus objetivos, plazos, tareas, entregas (documentos *D* o programas *P*) e hitos.

2.5.1. Aplicación a una unidad de REPSOL-YPF

Aplicación a una unidad de REPSOL-YPF	
<i>Comienzo</i>	Mes 0
<i>Final</i>	Mes 12
<i>Dedicación</i>	1 mes
<i>Objetivos</i>	<p>Se trata de definir un caso de uso al que aplicar las soluciones propuestas. La colaboración con una planta de REPSOL-YPF se ordenaría en torno a dos reuniones:</p> <ol style="list-style-type: none"> 1. Recopilación de información de una unidad de la planta elegida por REPSOL-YPF de cara a poder construir un modelo de simulación de la unidad y su control, así como casos de situaciones anormales en esa unidad en las que probar las técnicas resultantes del proyecto. Por las características del proyecto debería ser una unidad relativamente sencilla. Además, por medio de un cuestionario y eventualmente entrevistas, se solicitará a los técnicos de REPSOL-YPF su opinión sobre funcionalidades deseables del sistema de control en una situación de emergencia. 2. Presentación de los resultados y evaluación conjunta de los mismos.
<i>Tareas</i>	<p><i>T1.1 Caracterización de la unidad</i> <i>T1.2 Caracterización de casos de emergencia</i> <i>T1.3 Cuestionario</i> <i>T1.4 Evaluación de resultados</i></p>
<i>Entregas</i>	<p><i>E1.1 Caso de aplicación (D)</i> <i>E1.2 Informes de reuniones con técnicos de REPSOL-YPF (D)</i></p>
<i>Hitos</i>	<p><i>H1.1 Definición del caso de aplicación</i> <i>H1.2 Presentación de resultados y juicio crítico</i></p>

2.5.2. Sistemas de control en situaciones de emergencia

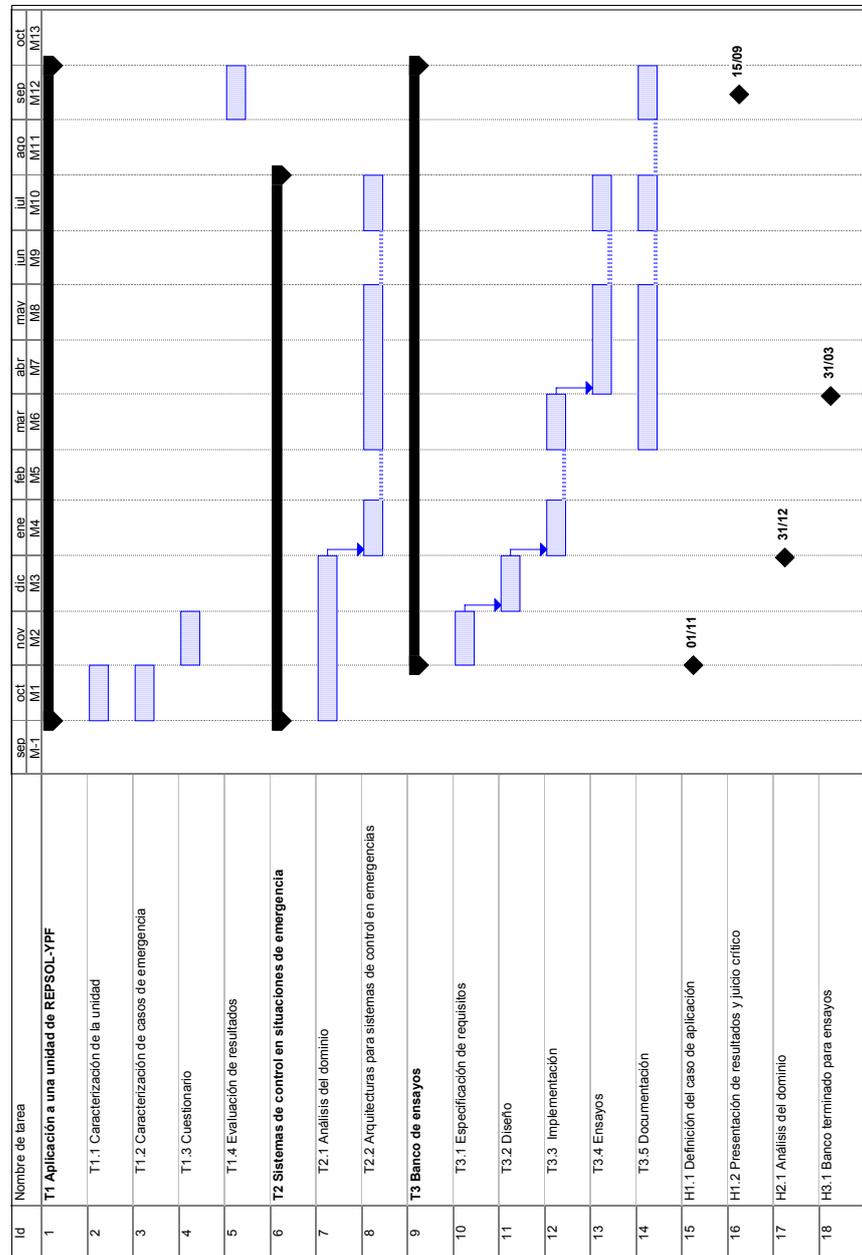
Análisis del dominio	
<i>Comienzo</i>	Mes 0
<i>Final</i>	Mes 10
<i>Dedicación</i>	4 meses
<i>Objetivos</i>	<p>El objetivo es el análisis científico del problema objeto de este proyecto. Se trata de analizar los sistemas existentes y propuestos identificando potenciales esquemas de trabajo así como herramientas teóricas para su diseño y validación.</p> <p>Estas tareas se solapan con el desarrollo del banco de pruebas, que debe ser lo suficientemente flexible como para acomodar las arquitecturas resultantes en una etapa posterior a su diseño.</p>
<i>Tareas</i>	<i>T2.1 Análisis del dominio</i> <i>T2.2 Arquitecturas para sistemas de control en emergencias</i>
<i>Entregas</i>	<i>E2.1 Análisis del dominio (D)</i> <i>E2.2 Sistemas de control en situaciones de emergencia (D)</i>
<i>Hitos</i>	<i>H2.1 Análisis del dominio</i>

2.5.3. Banco de ensayos

Banco de ensayos	
<i>Comienzo</i>	Mes 2
<i>Final</i>	Mes 12
<i>Dedicación</i>	4 meses
<i>Objetivos</i>	En este paquete se desarrollará el software específico para simular el funcionamiento de la unidad elegida y los esquemas de sistemas de control propuestos en casos de emergencia.
<i>Tareas</i>	T3.1 Especificación de requisitos T3.2 Diseño T3.3 Implementación T3.4 Ensayos T3.5 Documentación
<i>Entregas</i>	E3.1 Especificación de requisitos (D) E3.2 Diseño (D) E3.3 Implementación (D+P) E3.4 Ensayos (D) E3.5 Documentación (D)
<i>Hitos</i>	H3.1 Banco terminado para ensayos

2.5.4. Programación

El diagrama de Gantt muestra la distribución temporal de tareas y las dependencias entre ellas.



2.6. Firma y aval del tutor

La presente propuesta de proyecto de investigación para la convocatoria de becas de Iniciación a la I+D+i de la Cátedra Repsol ETSII-UPM de 2008 es presentada por D.^a Laura Lanchas Fuentes y avalada por el profesor del departamento de Ingeniería Química de la ETSII-UPM D. Santos Galán Casado.

Madrid, 2 de junio de 2008

Laura Lanchas Fuentes

Santos Galán Casado (tutor)

Bibliografía

- 4DM Technologies. (2008). Available from <http://www.4dm-tech.com/>
- Abnormal Situation Management Consortium. (1992). Available from <http://www.asmconsortium.com>
- Emigholz et al. (2008). *System and method for abnormal event detection in the operation of continuous industrial processes*. US Patent. (ExxonMobil)
- Frank, P. M., Ding, S. X., & Marcu, T. (2000). Model-based fault diagnosis in technical processes. *Transactions of the Institution of Measurement and Control*, 22(1), 57–101.
- Nimmo, I. (1999). Future of supervisory systems in process industries: Lessons for discrete manufacturing. *Annual Reviews in Control*, 23, 45–52.
- Sanders, R. E. (2005). *Chemical process safety. learning from case histories* (3rd ed.). Burlington: Elsevier Butterworth-Heinemann.
- UNE-EN 61511. (2006). *Seguridad funcional. Sistemas instrumentados de seguridad para el sector de las industrias de procesos*. Madrid: AENOR.
- Venkatasubramanian, V., Rengaswamy, R., Yin, K., & Kavuri, S. N. (2003a). A review of process fault detection and diagnosis. Part III: Process history based methods. *Computers & Chemical Engineering*, 27, 327–346.
- Venkatasubramanian, V., Rengaswamy, R., Yin, K., & Kavuri, S. N. (2003b). A review of process fault detection and diagnosis. Part II: Qualitative models and search strategies. *Computers & Chemical Engineering*, 27, 313–326.
- Venkatasubramanian, V., Rengaswamy, R., Yin, K., & Kavuri, S. N. (2003c). A review of process fault detection and diagnosis. Part I: Quantitative model-based methods. *Computers & Chemical Engineering*, 27, 293–311.

Title: Sistemas de control de plantas químicas en situaciones de emergencia
Subtitle: Propuesta de proyecto de Investigación para la convocatoria de becas de Iniciación a la I+D+i de la Cátedra Repsol ETSII-UPM
Author: Laura Lanchas Fuentes
Santos Galán Casado (tutor)

Date: 2 de junio de 2008
Reference: R-2008-B01 v 1.0 Edición

URL:

© 2008 ASLab

Autonomous Systems Laboratory

UNIVERSIDAD POLITÉCNICA DE MADRID
C/JOSÉ GUTIÉRREZ ABASCAL, 2
MADRID 28006 (SPAIN)

