

Jorge Bourdette
Gerente de I&D

AWAO8

Automation
World
Argentina
2008

Seguridad y Disponibilidad en Calderas y Hornos

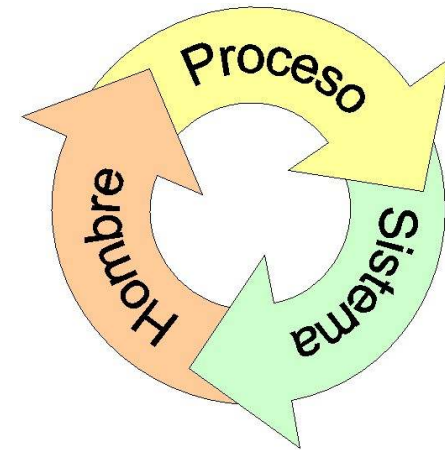


Agenda

- Normas de referencia
- Hornos
- Calderas
- Calderas de Recuperación
- IEC61508/61511
- Prescriptive vs. Performance-based
- Disponibilidad
- Usabilidad

Estándares más difundidos

- NFPA 86 (Standard for Ovens and Furnaces)
 - Hornos de procesos
- NFPA 85 (Boiler and Combustion Systems Hazards Code)
 - Calderas y generadores de vapor
- BLRBAC "Good practices" (Black Liquor Recovery Boiler Advisory Committee)
 - Calderas de recuperación de líquido negro
- IEC 61508
 - Seguridad funcional de E/E/PES (equipos)
- IEC61511
 - Seguridad funcional en industrias de procesos (instalaciones)



Abreviaturas comunes

- SIS Safety Instrumented System
- BMS Burner Management System
- MFT Master Fuel Trip
- WDT Watchdog Timer
- BCS Boiler Control System
- CCS Combustion Control System
- BLRB Black Liquor Recovery Boiler
- ESP Emergency Shutdown Procedure
- BLT Black Liquor Trip
- MTBF Mean Time Between Failures
- MTTF Mean Time To Repair
- PFD Probability of Failure on Demand
- SIL Safety Integrity Level
- HAZOP Hazard and Operability study
- H&RA Hazard and Risk Assessment
- LOPA Layer Of Protection Analysis
- ALARP As Low As Reasonably Practicable

NFP A86 (hornos)

- Recintos a presión atmosférica para calentamiento de materiales
 - Clase A: calentamiento de materiales combustibles
 - Clase B: calentamiento de materiales no combustibles
 - Clase C: atmósfera inflamable
 - Clase D: otros
- Sistemas de calentamiento:
 - Internos y Externos
 - Directo o indirecto
 - Fuel oil, gas, eléctrico, etc.
- Requerimientos generales (constructivos, interlocks, etc.)
- Uso de equipos aprobados

- Principios del SIS:
 - Separación de sistemas
 - PLCs:
 - Independencia de aplicaciones
 - Protección contra alteraciones
 - Seguro ante falla (energía, diagnóstico interno, watchdog externo, etc.)
 - Sin relés intermedios (exc. estricta necesidad, req. failsafe)
 - Pulsador manual directo
 - Prohibición de bypass
 - Intervención manual para restablecimiento
 - Mantenimiento, documentación, entrenamiento

Incluye secuencias

- Barrido de gases¹
- Encendido de piloto²
- Encendido de quemador
- Supervisión de llama (independiente³)
- Regulación
- Bloqueos de combustible (individual o general)
- Pruebas anuales:
 - *“All safety interlocks shall be tested for function...”, “The set point of temperature, pressure, or flow devices used as safety interlocks shall be verified...”, “Safety device testing shall be documented”, etc.*
 - *Se puede puentear un dispositivo durante la prueba*

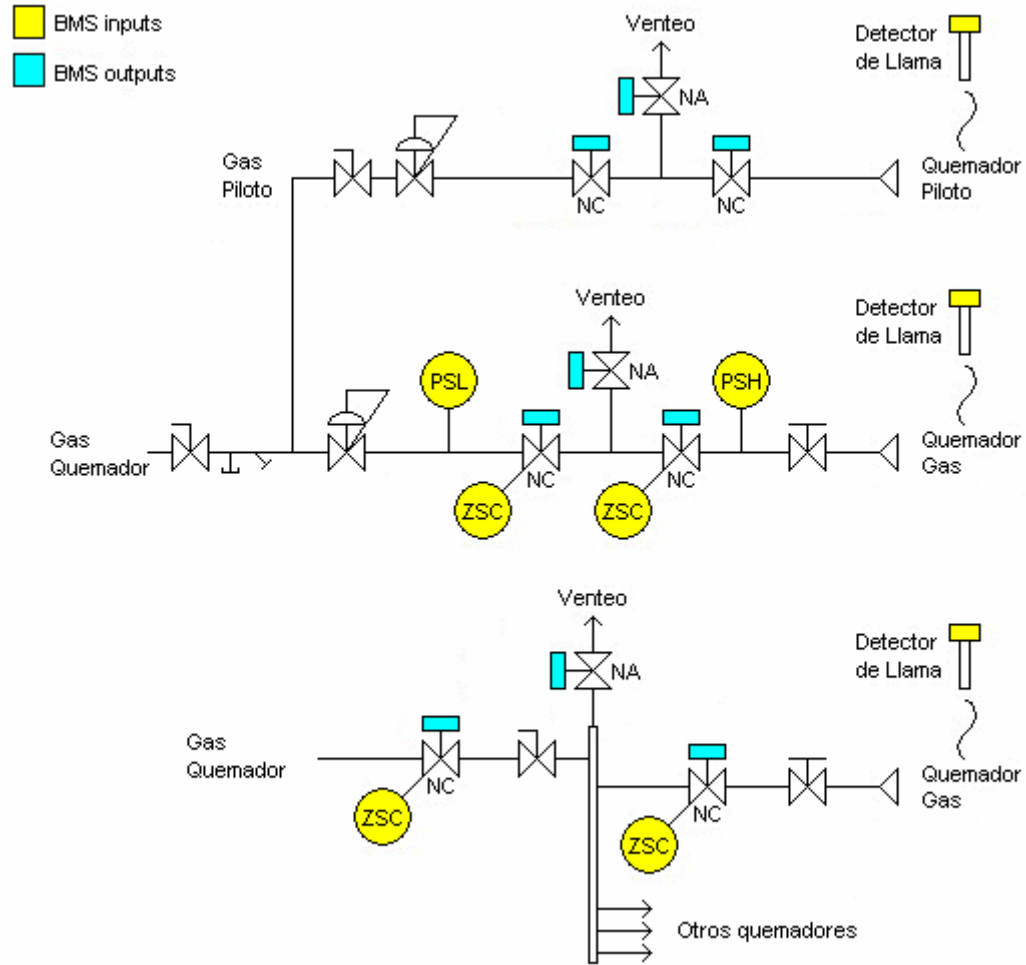
¹Excepto radiante a prueba de explosión (7.4.1.4)

²Sin reencendido excepto calor y llama

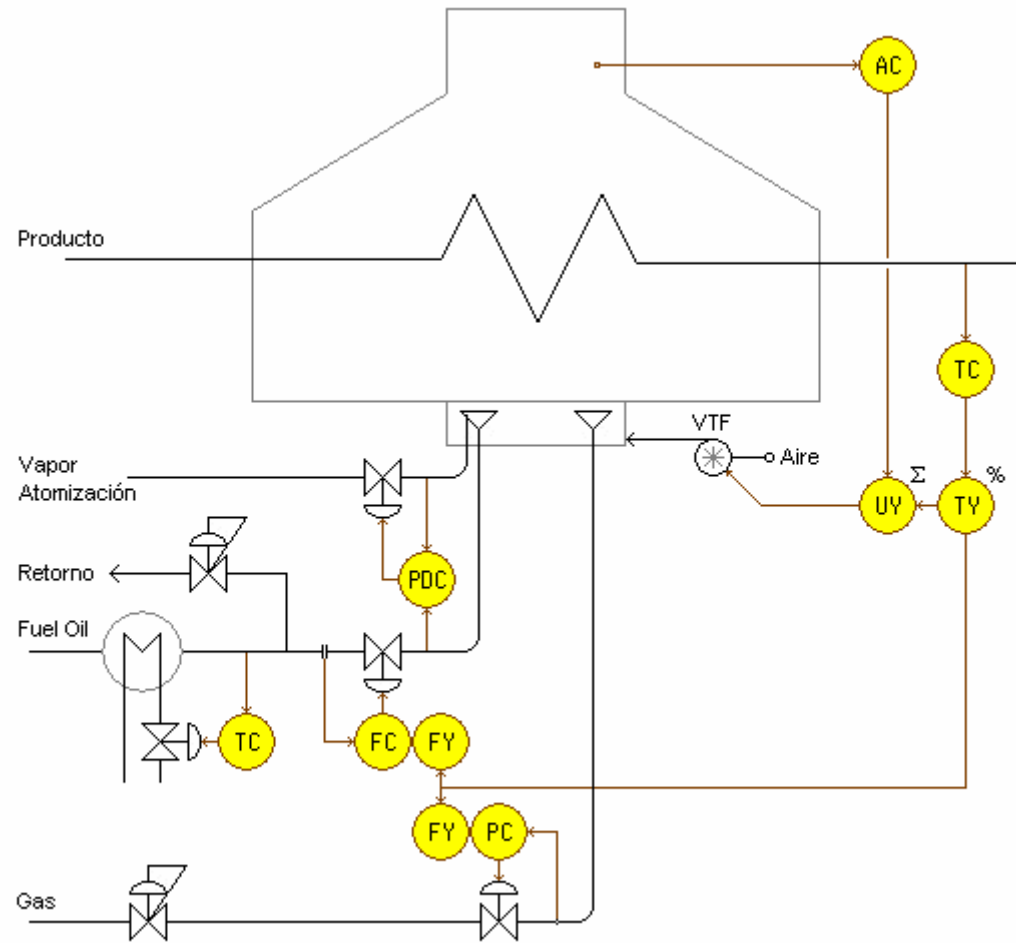
³Excepto piloto interrumpido



Esquemas típicos



Control regulatorio



NFPA 85 (calderas)

- Recomendaciones para prevenir explosión o implosión de calderas
 - Tipos: Acuotubular, Humotubular, HRSG...
 - Uno o más quemadores
 - Uno o más combustibles: Gas, Fuel, polvos...
 - Operación automática, supervisada o manual (no recomendada)
- Requisitos mínimos de seguridad y control
 - Referencia, no para diseño
 - Incluye piloto, quemadores y control de combustión
 - NO incluye otros sistemas auxiliares

- Sistemas:
 - BMS: sistema de seguridad, basado en concepto MFT
 - BCS: sistema de control, incluye CCS (control de combustión)
- Filosofía:
 - Separación de los sistemas (*excepto en ciertos casos*)
 - La falla de un componente del sistema no debe impedir que se produzca un paro en condiciones riesgosas
 - Prohibición de bypass
 - Mantenimiento, documentación, entrenamiento

Funciones del BMS

- Asegurar condiciones operativas seguras
- Apagar rápidamente en condiciones inseguras
 - MFT (Corte Maestro de Combustible)
 - Disparo si hay posibilidad de combustible sin quemar
 - Registrar causa de disparo
 - Switch manual remoto
- Asegurar barrido luego de disparo
 - También en condiciones iniciales “inseguras”

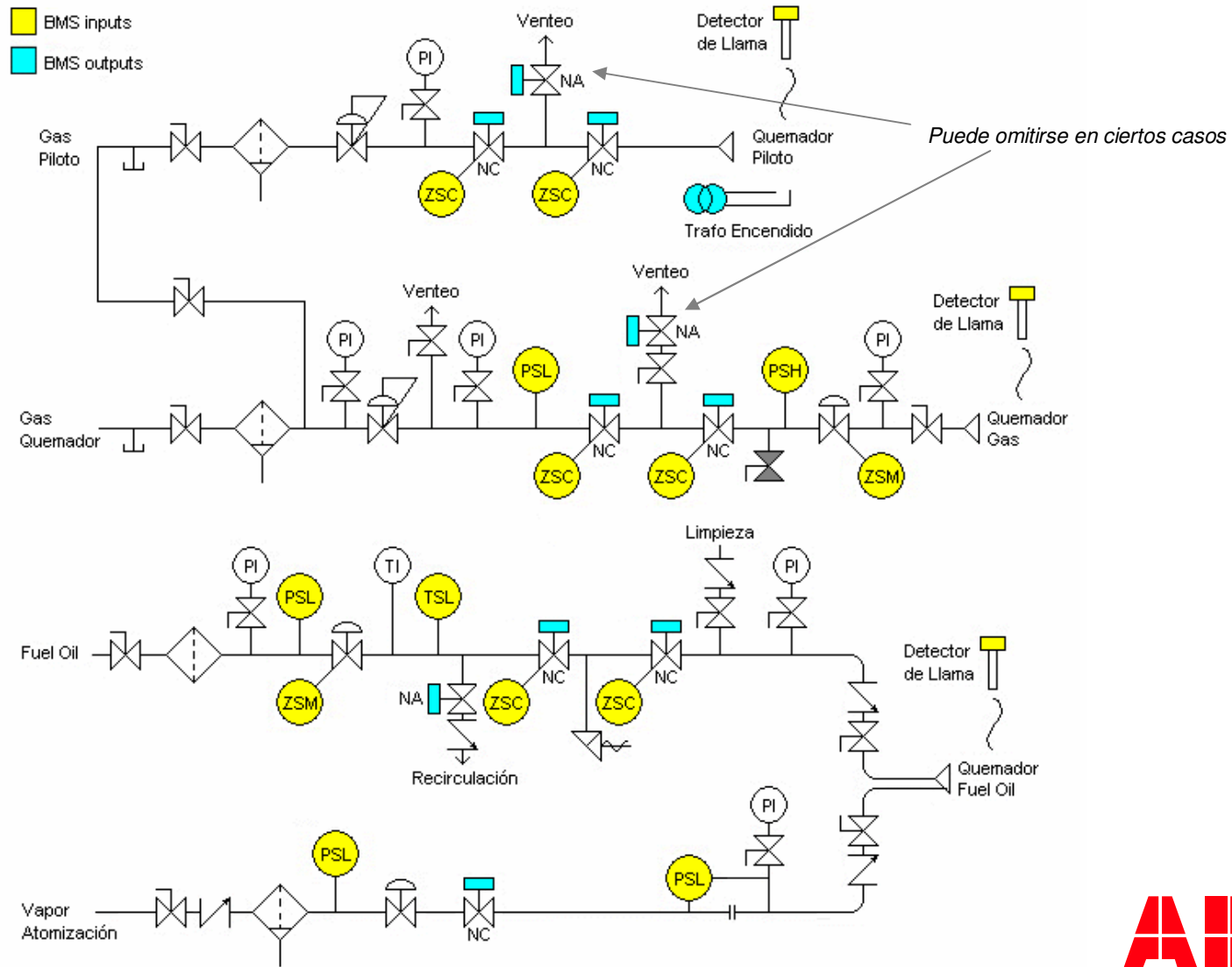
Requisitos

- Hardware confiable
 - Seguro ante falla
 - Tolerancia al ruido
 - Autodiagnósticos, feedback, mantenimiento y prueba en línea
 - Watchdog externo + Relé MFT, con pulsador directo
 - *“one of the possible means to implement monitoring of the logic system for failure”*
 - Señales de disparo sólo cableadas
- Software confiable
 - Información para el operador (segundo nivel de protección)
 - Tendencias y Alarmas
 - Restricción de acceso para modificaciones
- *“Operation, set points, and adjustments shall be verified by testing at specified intervals, and the results shall be documented.”*

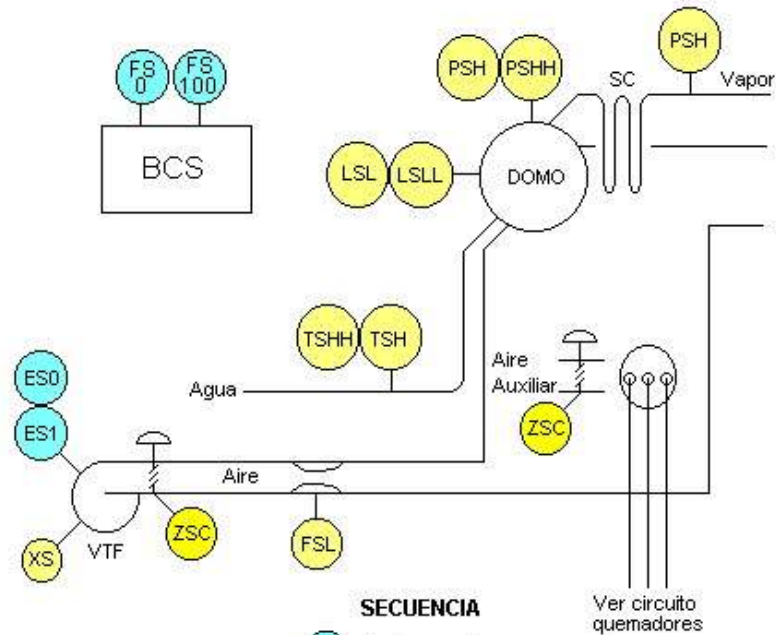
Incluye secuencias

- Permisos arranque
- Barrido de gases
- Habilitación encendido (reset MFT)
- Encendido piloto
- Aire mínimo
- Encendido quemador
- Supervisión de llama
- Regulación
- Bloqueos de combustible (individual o general)

Esquema típico (BMS)



Esquema típico (BMS)



- Entradas BMS
- Salidas BMS

SECUENCIA

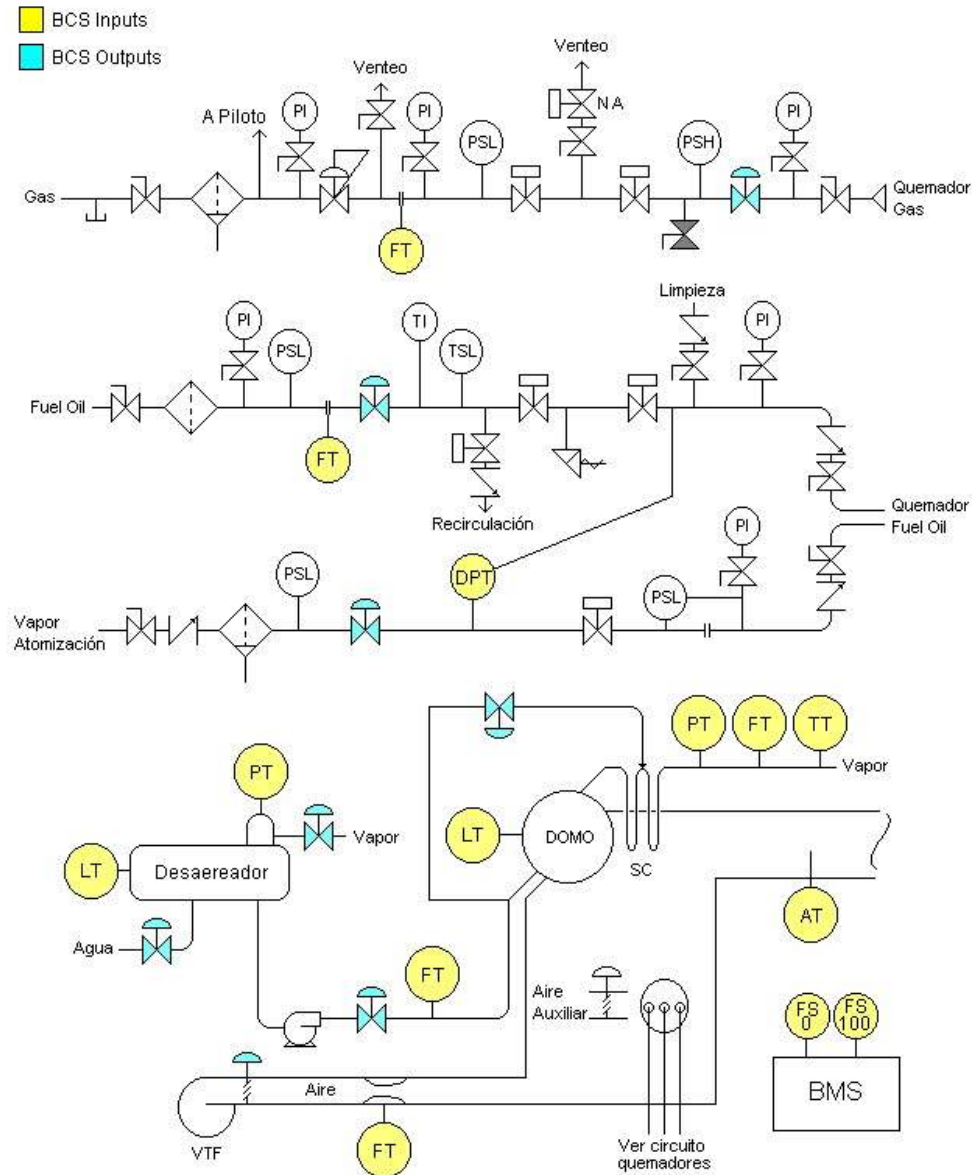
- XL Listo para barrer
- XL Barriendo
- XL Fin barrido
- XL Piloto Encendido
- XL Falla Piloto
- XL Gas Encendido
- XL Falla Quemador Gas
- XL Fuel Oil Encendido
- XL Falla Quemador Fuel Oil

- PB Paro Emergencia
- PB Paro Emergencia
- PB Arranque
- PB Encender Piloto
- PB Apagar Piloto
- PB Encender Quemador
- PB Apagar Quemador
- HS Selector GAS/FUEL
- PB Reconocimiento

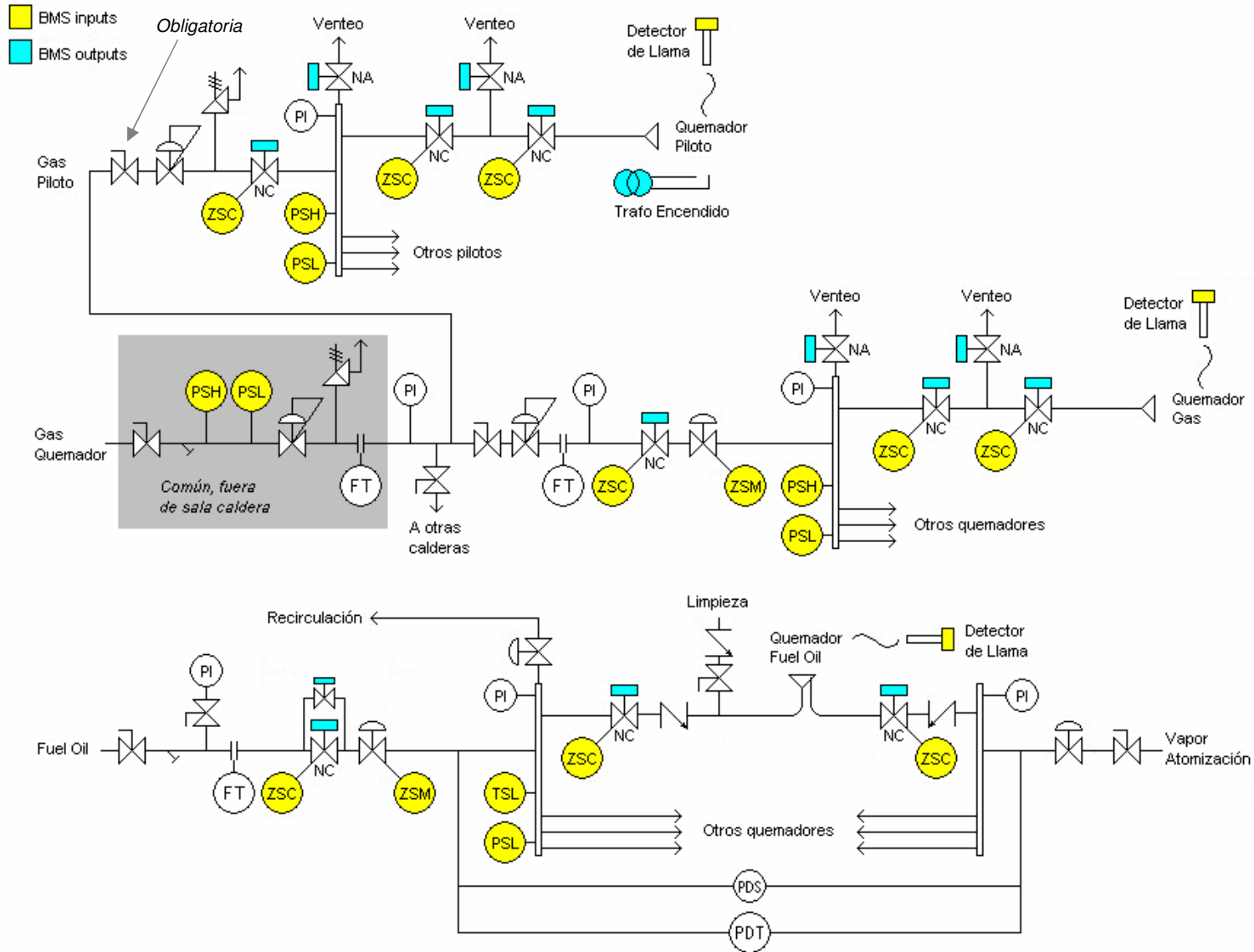
ALARMAS

- XA Paro General
- XA Paro por VTF F/S
- XA Paro por falta aire
- XA Paro por nivel domo
- XA Paro por presión vapor
- XA Paro por temperatura agua
- XA Paro emergencia (puls)
- XA Paro por falla combustible
- XA Paro por falta llama
- XA Bocina

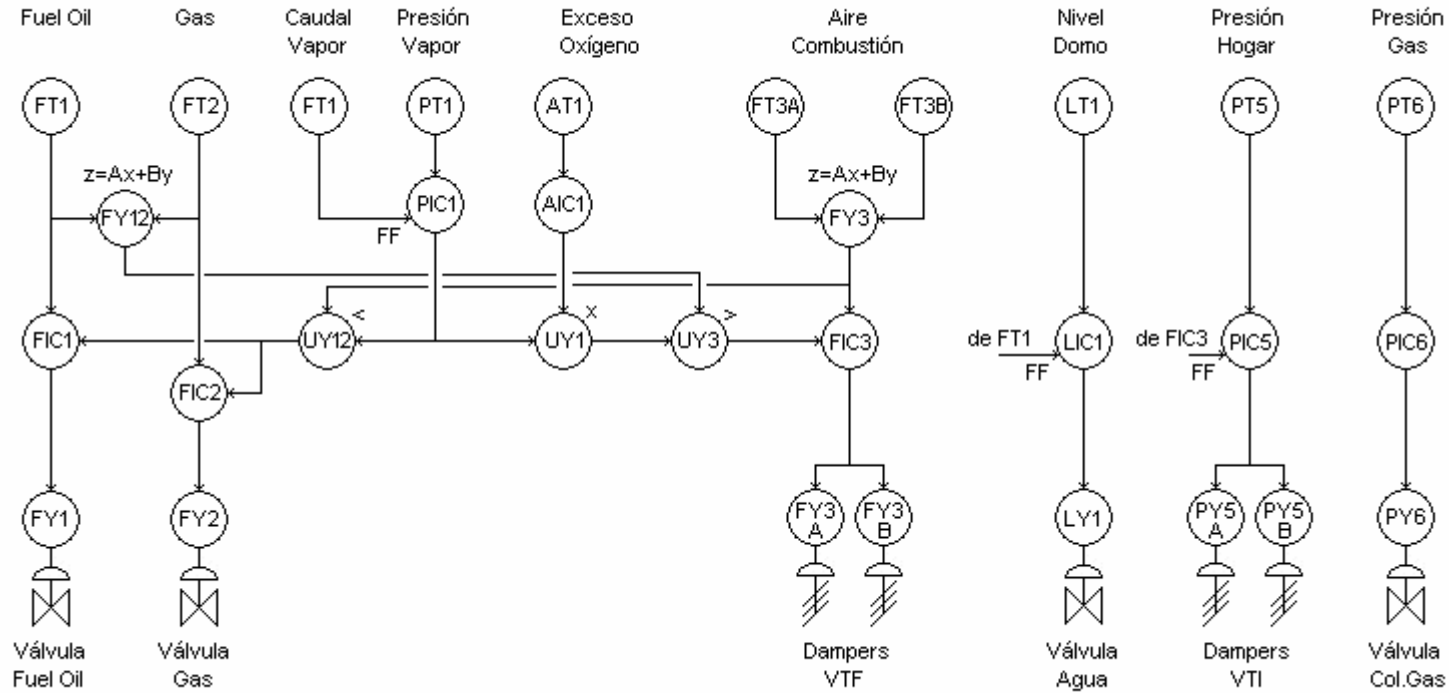
Esquema típico (BCS)



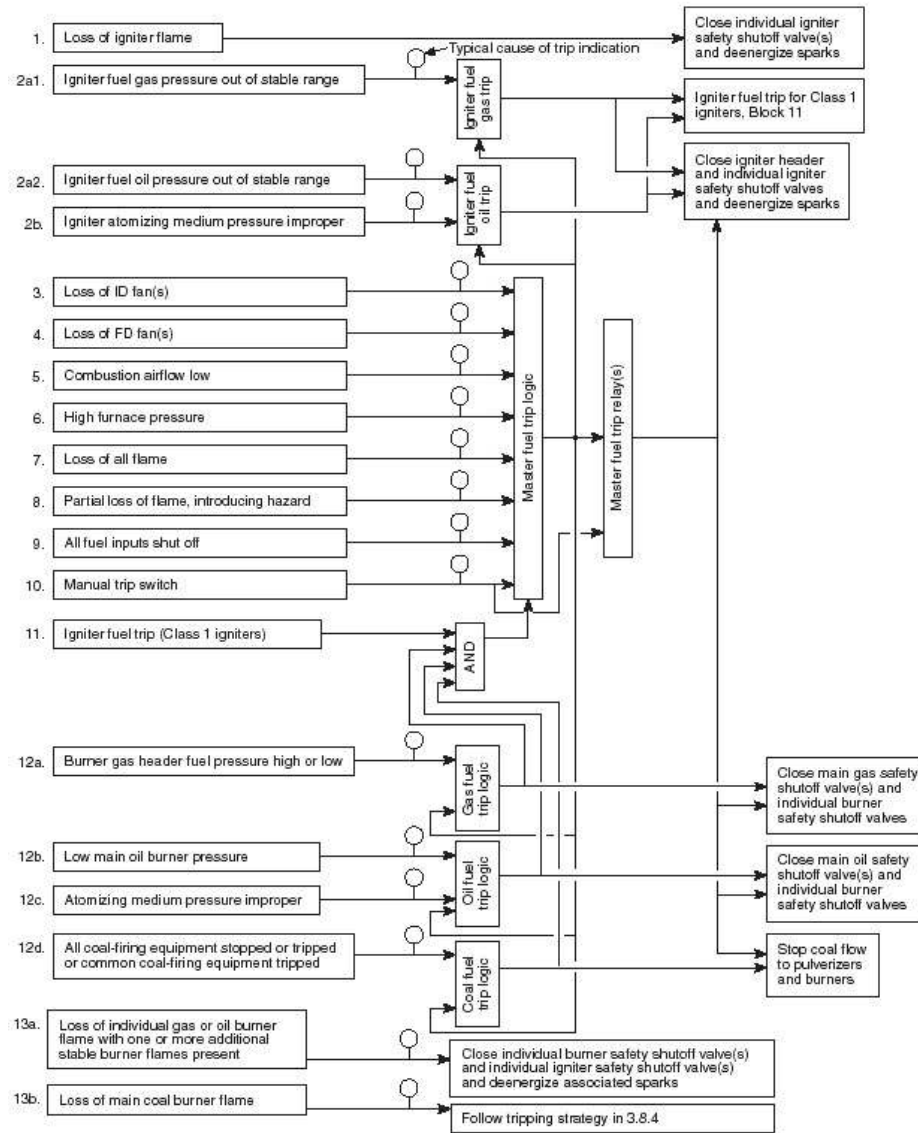
Múltiples quemadores



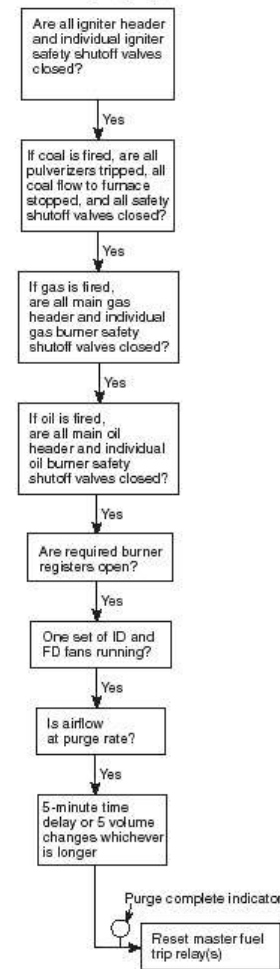
Control regulatorio



MFT típico

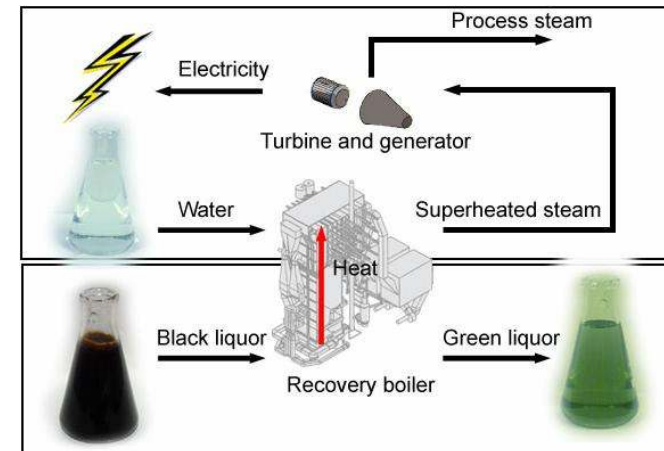


Furnace purge system



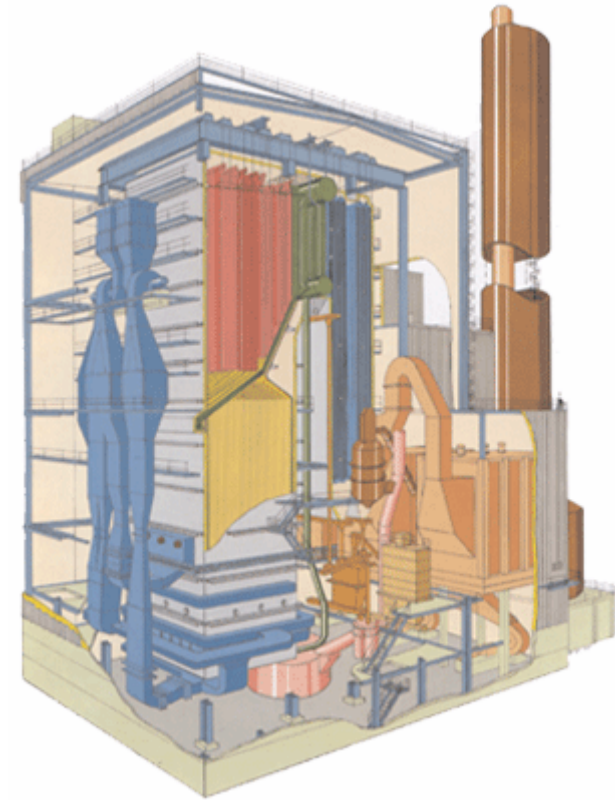
Calderas de Recuperación

- Caldera acuotubular usada en plantas de pulpa y papel
 - Quemado de líquido negro resultante de la producción de pulpa
 - Propósitos: recuperación química, eficiencia energética, reducir contaminación
- En general queman gas, fuel oil y líquido negro
 - Gas & Fuel para arranque y carga alta



Calderas de Recuperación

- Riesgos principales
 - Explosiones de combustible sin quemar
 - Ingreso de agua al hogar puede provocar explosiones por reacción química con el lecho fluido (smelt)
 - Explosión de gases de pirólisis si la combustión del líquido negro no es completa (ej. partículas combustibles en el precipitador)



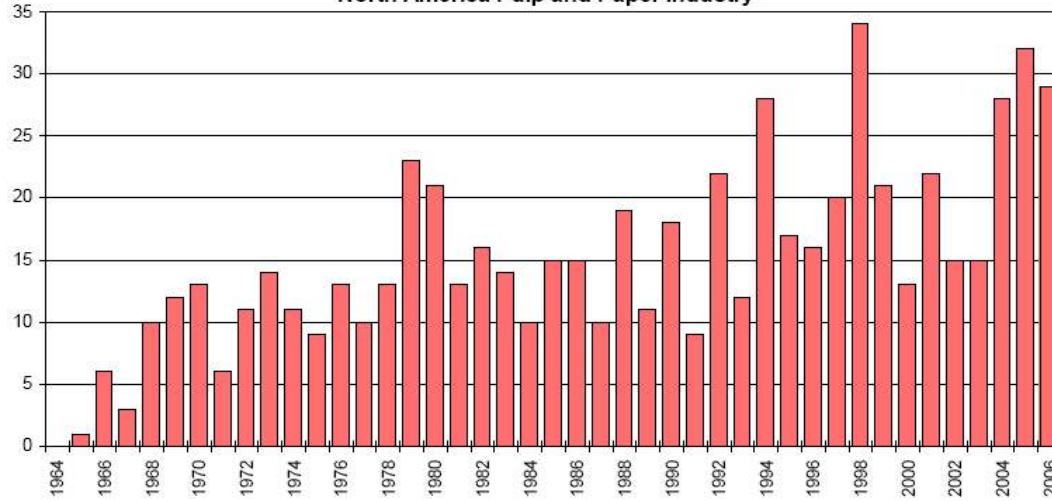
Detalle de causas de explosión

- Comunes a otras calderas (acumulación de gases combustibles)
- Por ingreso de agua
 - *Rotura de partes bajo presión*
 - Condiciones inseguras (bajos sólidos o mala atomización)
 - Ingreso de BL en hogar fuera de servicio
 - Ingreso de agua por sistema de BL
 - Ingreso de agua desde el exterior
- Explosión de gases de pirólisis
 - Ingreso de BL sin combustión suficiente y estable
 - Encendido de combustible auxiliar con sólidos sin purgar

Estadísticas (BLRBAC 2006; sobre 181 calderas operando en USA)

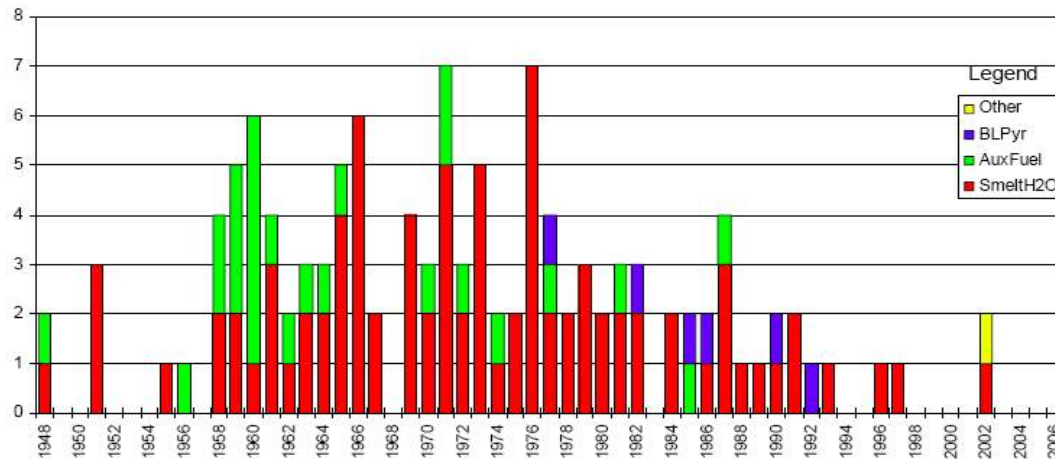
KRAFT RECOVERY BOILER CRITICAL INCIDENTS

North America Pulp and Paper Industry

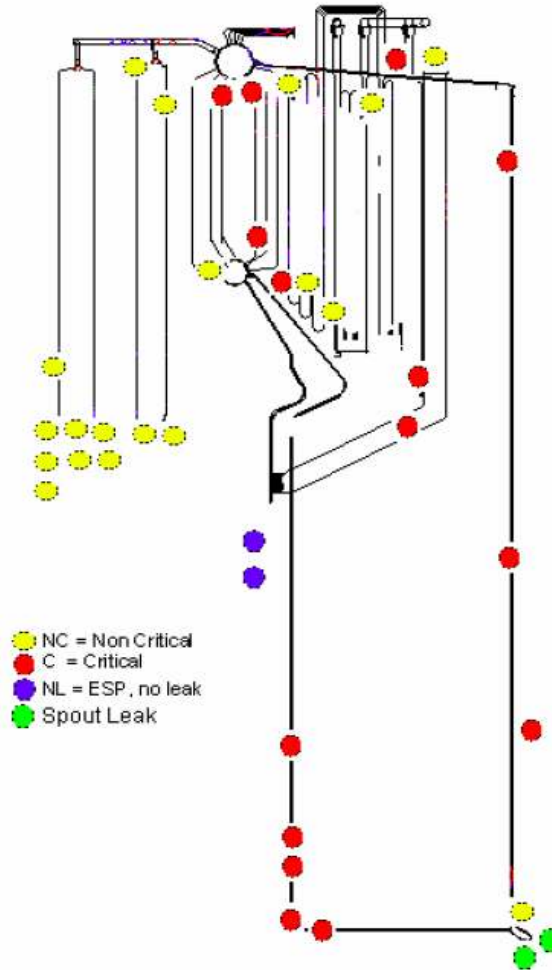


KRAFT RECOVERY BOILER EXPLOSIONS

North America Pulp and Paper Industry



Fall 2006 Incident Locations



Calderas de recuperación

- Puntos clave:
 - “Se recomienda la **inspección** anual de partes bajo presión para localizar pérdidas [...] y tomar medidas proactivas para prevenir el ingreso de agua. Durante la misma se recomienda **probar** todos los sistemas de seguridad [...], y también la verificación periódica de que los **operadores** [...] saben reconocer distintas situaciones riesgosas, tomar acciones correctivas apropiadas, determinar si está ingresando agua al hogar y actuar el sistema ESP.”

David Parrish, FMR Corp., in National Board of Boiler and Pressure Vessel Inspectors Bulletin, Winter 1998



- Principios del SIS:
 - La falla de un componente del sistema no debe impedir que se produzca un paro en condiciones riesgosas
 - Supervisión con relé externo (paro manual)
 - Separación de los sistemas
 - Protección contra alteraciones
 - Prohibición de bypass
 - Mantenimiento, documentación, entrenamiento

- Emergency Shutdown Procedure
 - *“An immediate emergency shutdown must be performed whenever water in any amount is known or suspected to be entering the furnace and cannot be stopped immediately.” (BLRBAC)*
- Sistema dedicado para:
 - Activar alarma
 - Cortar combustibles
 - Cortar fuentes de agua y vapor
 - Cortar aire primario, minimizar resto
 - Drenar caldera y economizador a 8 pies
 - Reducir presión

Sistema ESP

- Sensores
 - Refractómetro (redundante + diagnósticos) para monitoreo de sólidos
 - Fuga de agua – Pero el ESP siempre lo inicia el operador
- Actuadores
 - Válvulas para drenar caldera, desviar LN y cerrar agua y vapor
 - Detener bombas de LN
 - Corte de combustible y ajuste de aire con BMS
 - Válvulas de bloqueo manuales en lugar remoto
- Sistema lógico
 - PLC u otro resolvedor lógico (hardware, o hardware + software)
 - Lógica muy simple

Procedimientos post-ESP

- Si no hubo explosión
- Pasos:
 - Verificar ESP correcto y completo
 - Procedimientos operativos
 - Control de acceso
 - Aislación del proceso
 - Documentación
 - Investigar causa
 - Tiempo de espera
 - Habilitar ingreso (mínimo)
 - Evaluar condición
 - Reacondicionar
 - Probar

Interlocks

- Combustibles auxiliares como NFPA 85
 - Concepto MFT válido
 - Barrido con aire >30%, por debajo de ingreso líquido negro, más de 5 min o hasta O₂ en exceso
- Disparos adicionales
 - ESP (emergency shutdown procedure)
 - BLT (black liquor trip)
 - Alta temperatura salida evaporador/precipitador
- Interlocks de líquido negro
 - Bloqueos de limpieza de lanza
 - Control de temperatura y presión de líquido negro
 - Bloqueo de colector y apertura de desvío automáticos
 - Protección contra explosión de gases de pirólisis

Instrumentación y control

- Consideraciones sobre:
 - Modos de falla (fail-safe)
 - Alimentación, tierras, medio ambiente
 - Redundancia
 - CPU
 - Lazos críticos: nivel de agua, tiro inducido, combustible(s), aire
 - Comunicaciones
 - Interfaz Hombre-Máquina
 - “jumper policy”
 - Mantenimiento preventivo
- Recomendaciones sobre instrumentación

Resumen

- La falla de un componente del sistema no debe impedir que se produzca un paro en condiciones riesgosas
- Sistemas independientes
- Condición segura ante falla
- Prohibición de modificaciones o bypass
- Sistema de paro manual independiente
- Mantenimiento
- Documentación
- Entrenamiento

SIS basados en riesgo

- Seguridad: excención de riesgo inaceptable
- Riesgo dado por:
 - Probabilidad de ocurrencia de un evento riesgoso, y
 - Gravedad de las consecuencias
- Sistemas de seguridad
 - Se definen en base a análisis de riesgo
- Fallas de los sistemas de seguridad
 - Probabilidad de falla ante demanda (falla riesgosa)
 - $PFD = 1 - A_S$
 - Probabilidad de actuar sin causa (falla segura)
 - "Nuisance trips"

- Aplicación general
- Conceptos básicos
 - Seguridad Funcional (E/E/PE)
 - Parte de la seguridad general que depende de que un sistema o equipo opere correctamente ante cambios en sus entradas
 - Function Requirements + Integrity Requirements
 - Ciclo de vida de seguridad
 - H&RA → Requerimientos → Diseño → Construcción → Instalación → Pruebas → Validación → Operación → Mantenimiento → Desguace
- Condiciones base para certificar equipos

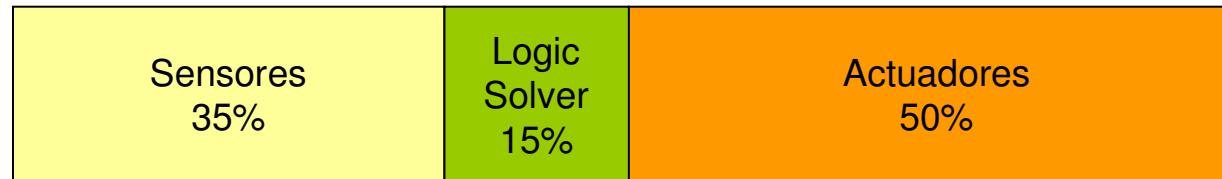
IEC 61511

- Para Industrias de Procesos
- Conceptos de Riesgo Tolerable & ALARP
 - ¿Qué riesgo es “aceptable”? (probabilidad x consecuencias)
- Base para determinar SIL (Safety Integrity Level)
 - Métodos: safety matrix, risk graph, LOPA, etc.

SIL	PFD	Safety Availability	Risk Reduction
4	0.0001 – 0.00001	0.99990 – 0.99999	10000 – 100000
3	0.001 – 0.0001	0.99900 – 0.99990	1000 – 10000
2	0.01 – 0.001	0.99000 – 0.99900	100 – 1000
1	0.1 – 0.01	0.90000 – 0.99000	10 – 100

¿Cómo fallan los sistemas?

■ SIS



■ Factor humano

- Más de la mitad de los accidentes se deben al factor humano
 - Entrenamiento, procedimientos, mantenimiento, puentes

■ Dos conceptos clave

- Ciclo de vida de seguridad
- Sistema de gestión de seguridad

Pros y contras

- Estándares prescriptivos
 - Beneficios
 - Fácil de aplicar (seguir las reglas)
 - Bajo costo de aplicación (no requieren HRA etc.)
 - Certeza de cumplimiento (cumple o no cumple)
 - Las decisiones del usuario son limitadas
 - Sin compromiso sobre niveles de riesgo tolerable
 - Problemas
 - Falta de flexibilidad para nuevas tecnologías e innovaciones
 - Puede haber problemas de seguridad no considerados en el estándar
 - En general no consideran la variable tiempo
 - Las decisiones del usuario son limitadas
 - No da directivas claras sobre integridad del SIS

Pros y contras

- Estándares basados en riesgo (performance)
 - Beneficios
 - Flexibilidad (muchos sistemas posibles para un problema dado)
 - Cobertura minuciosa de riesgos (métodos de análisis de riesgo)
 - Mantenimiento y pruebas considerados en los cálculos
 - Provee un objetivo de validación
 - Requiere justificación de decisiones basada en información objetiva
 - Problemas
 - Más tiempo y dificultad para implementar (HRA, FSMS, tests, etc.)
 - Demostrar el nivel de seguridad alcanzado puede ser caro
 - Requiere justificación de decisiones basada en información objetiva
 - Requiere decisión del usuario sobre tolerancia a riesgo (!)

Grandfather clause (ISA S84.00.01)

- *“For existing SIS designed and constructed in accordance with codes, standards, or practices prior to the issue of this standard (e.g., ANSI/ISA-84.01-1996), the owner/operator shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner”*
- Implica:
 - Hay que hacer análisis de riesgo
 - Verificar que los sistemas existentes tienen en cuenta el nivel de riesgo definido
 - Documentar conclusiones y decisiones
 - Revisar y actualizar el sistema (si es necesario)

Qué dicen los expertos...?

- *“Industry update: Safety Instrumented Burner Management Systems” (M.Scott, paper presented at ISA 2004)*
 - “Burner Management Systems [...] are all defined SIS if they contain sensors, a logic solver and a final control element according to ANSI/ISA 84.01.”
 - “FM Approval Standard 7605 requires that PLC based BMS must comply with IEC 61508.”
 - “A BMS can be designed that meets all requirements of the prescriptive standards such as NFPA 85 or 86 and yet will NOT satisfy the requirements of a SIS.”
- *“Is a BMS a SIS?” (M.Scott, ISA webinar, 2007)*
 - “A BMS is a SIS if the risk analysis determines that additional risk reduction is required and a SIL 1 or greater is assigned to a BMS SIF”

Qué dicen los expertos...?

- *“Independency Consideration for BMS and BCS” (D.Lee, paper presented at ISA 2006)*
 - “Physical separation of logic solvers does not ensure a safe logic design.”
 - *“Product listing or labeling does not ensure a safe system design.”*
 - “Designer’s responsibility to consider all possible failure modes and effect that each failure have on the integrity of the logic system, the safety of the unit being protected and the safety of the plant personnel”

Qué dicen los expertos...?

- *“Independency Consideration for BMS and BCS” (ISA Power Industry Division feedback on ISA dTR84.00.05 – Oct’06 draft)*
 - “The focus of the technical report is on boilers and other heaters that are part of a larger process plant and not on typical central station power plant boilers”
 - “It is not clear that there is a problem with BMS safety on power plants that is not adequately addressed by the existing NFPA code.”
 - “The cost of performing the recommended analysis on a large power plant boiler would be substantial and may not lead to any improvement in overall system safety.”

Qué dicen los expertos...?

- *“Independency Consideration for BMS and BCS” (ISA Power Industry Division feedback on ISA dTR84.00.05 – Oct’06 draft)*
 - “Declaring that a BMS is a SIS, or even just hinting that it might be, would greatly increase costs for large boiler operators (without providing a commensurate reduction in losses) [...] This document needs to clearly state at the very beginning that applying ISA 84 to a BMS may not be warranted unless the application is unusual or losses have occurred at a particular site even when strict compliance with existing industry codes and applications standards was performed”

Qué dicen los expertos...?

- *NFPA 8502 committee response to the Process Industry strategy to safety*
 - “Burner Management System is not a “safety system” as defined by the process industry”.
 - “It is not necessary for this standard (NFPA 8502) to reference or require the use of other standards which is the prerogative of the authority having jurisdiction”.

Qué dicen los expertos...?

■ Resumen:

- La industria de procesos en general considera que un BMS es un SIS como define S84
- La industria de generación en general no considera que la S84 aplique a los BMS
 - *“An increase in the number of incidents would make S84 more widely accepted”*
 - *“Otherwise, applying S84 would make the cost much bigger”*

■ Nota:

- OSHA no considera que S84 sea el único método para cumplir con PSM (CFR 1910.119), pero sí considera a S84 como “buenas prácticas de ingeniería”

Medidas de seguridad (Argentina)

- Estándares no obligatorios
 - Requerimientos legales simples, calderas de recuperación no consideradas específicamente, prueba diaria, etc.
 - DN 351/79, Tít.I, Art.5: incorporación de recomendaciones técnicas dictadas o a dictarse por organismos estatales o privados, nacionales o extranjeros una vez aprobadas por el Ministerio de Trabajo
- Práctica común en la industria:
 - Cumplir NFPA 85 (obligatorio en US)
 - Calderas de recuperación: seguir prácticas BLRBAC
- Tendencia (industria de procesos):
 - Hacer HRA, definir niveles SIL, pedir certificación IEC 61508 a proveedores
 - Pero – en muchos casos – no se instala FSMS

Aplicación: NFPA+BLRBAC vs. HAZOP

- Auditoría de seguridad durante revamping de caldera de recuperación
- Análisis múltiple:
 - NFPA 85 checklist
 - BLRBAC guidelines checklist
 - HAZOP (con clasificación de riesgos)
- Oportunidad de evaluar riesgos y beneficios usando estándares prescriptivos y basados en performance

Notes on NFPA 85 and BLRBAC guidelines

- Some requirements in BLRBAC (flame detection, forced draft fan operation under trip) are different from NFPA
 - BLRBAC approach was used for that specific boiler in such cases
- NFPA Appendix A is not mandatory but instrumentation examples are usually followed.
- NFPA requires “independent logic¹, independent input/output systems, and independent power supplies and shall be a functionally and physically separate device from other logic systems”, and one BMS per boiler.
- ESP system (BLRBAC) should be a “dedicated, stand-alone system”
 - Clarification October 2006: “physically and functionally independent” with outputs to BMS (MFT relay) and DCS (to position air dampers)

¹NFPA 85-2007 addition: “independent logic solving hardware”



Notes on NFPA 85 and BLRBAC guidelines

- NFPA/BLRBAC do not address system integrity
 - BLRBAC refers to ISA-S84.01 when defining SIS in the “Instrumentation Checklist and Classification Guide...”, mentions ESP as a SIS and considers that a SIS can be used as BMS
 - NFPA: the logic system designer shall evaluate failure modes of components and lists minimum failures that shall be addressed
 - NFPA lists logic system design requirements including monitoring and fuel trip in case of failure
- NFPA/BLRBAC do not require a functional safety management system in place
 - Documentation, maintenance, inspection, testing and proper training are described and required
- **ASSESSMENT IS VALID FOR THIS BOILER ONLY**

Aplicación: NFPA+BLRBAC vs. HAZOP

- Conclusiones del estudio:
 - NFPA/BLRBAC no establece niveles de integridad ni requiere cálculos de riesgo
 - Algunos casos (ej. fugas de combustible en el exterior) mencionados en NFPA o BLRBAC (“special hazards ... have to be addressed”), pero no hubieran sido detectados sin el HAZOP
 - Importancia de detección de llama y refractómetro evidente en el HAZOP
 - En unos pocos casos el HAZOP detectó riesgos que requerían mayor protección que la especificada por NFPA/BLRBAC
 - Detección de CO en gases, alta presión/temperatura en sobrecalentadores...
 - El HRA no implicó un costo extra alto, pero implementar un FSMS puede serlo – aunque no si se tiene ISO9000 o similar

Conclusiones

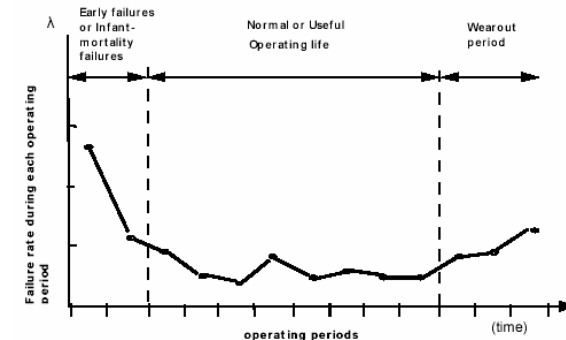
- No se puede saber la diferencia hasta hacer un análisis de riesgo
 - Muchas plantas construidas en base a normas prescriptivas han tenido accidentes
 - El riesgo no se puede evitar, pero se puede reducir
- El modelo de ciclo de vida y el sistema de gestión de seguridad funcional juegan un rol clave en la implementación de ISA S84/IEC 61511 que debe tenerse en cuenta

Disponibilidad

- Prioridad en la seguridad **y** la disponibilidad
- El diseño del sistema de seguridad y la selección de los elementos que lo forman son fundamentales para sostener ambos principios

Definiciones

- Confiabilidad
 - Probabilidad de que un elemento funcione durante un intervalo de tiempo específico y en condiciones operativas dadas
 - Varía en el tiempo
- Tiempo medio entre fallas (MTBF)
 - $R(t) = e^{-t/\mu} = e^{-t\lambda}$
 - $\mu = 1/\lambda = \mathbf{MTBF}$, permite comparar equipos
- Tiempo medio de reparación (MTTR)
 - Duración media de todas las actividades de reparación durante un período de tiempo dado.
 - Considerar tiempo de detección y MLDT (tiempo medio espera logística)



Disponibilidad

- Probabilidad de que un equipo cumpla la función para que fue diseñado en condiciones preestablecidas.
- $A = \text{MTBF} / (\text{MTBF} + \text{MTTR})$
- Mejoras de disponibilidad
 - MTBF↑
 - MTTR ↓
 - Redundancia
 - Diagnósticos
 - Tiempo sin redundancia
 - Reparación en línea

Arquitectura	Iniciación (FS)	Demanda (FR)
1oo1	0.0200	0.0100
1oo2	0.0400	0.0001
2oo2	0.0004	0.0200
2oo3	0.0024	0.0006



Usabilidad

- Seguridad ✓
- Disponibilidad ✓
- Usabilidad
 - Importancia del factor humano
 - Interfaz con el sistema de seguridad
 - Diagnósticos
 - Estado del sistema – Alarmas
 - Acciones
 - La interfaz en sí debe cumplir requisitos de funcionalidad y disponibilidad



Power and productivity
for a better world™