Tendencias en Sistemas de Seguridad de Calderas

Jorge Bourdette, ABB Argentina*

Normas aplicables a Calderas

Las tendencias actuales en la industria y el mercado de los Sistemas Instrumentados de Seguridad (SIS) muestran un interés creciente en considerar los estándares IEC 61508 y IEC 61511 (o su equivalente en USA, el ANSI/ISA S84.01) para el diseño, instalación, operación y mantenimiento de sistemas de seguridad de calderas (BMS).

Estos nuevos estándares (basados en conceptos como ciclo de vida de seguridad, riesgo tolerable y aceptable, y niveles de integridad de los sistemas) van ganando lugar entre las metodologías tradicionalmente usadas para diseñar sistemas de seguridad de calderas[1]: normas prescriptivas como la NFPA 85 y/o recomendaciones específicas para casos particulares, como las prácticas recomendadas por el BLRBAC[2] para calderas de recuperación de líquido negro. Se espera que en el futuro cercano normas como la NFPA 85 (o la NFPA 86 para seguridad de hornos) incluyan conceptos básicos de las IEC 61508/61511, o directamente refieran a ellas.

De hecho, la práctica recomendada del BLRBAC sobre instrumentación para sistemas de seguridad de calderas de recuperación incorpora definiciones de la ISA S84.01: la de BPCS (sistema de control de procesos básico) y la de SIS (sistema instrumentado de seguridad). Además, recomienda que el sistema de control y hardware asociado al paro de emergencia "haya pasado las pruebas de al menos una organización de estándares como UL, CSA, ULC, FM, NOC, etc. para uso en aplicaciones industriales"[3] y que "el uso de un SIS para BMS en una caldera de recuperación debe conformar a los requerimientos de comités de estándares apropiados como BLRBAC, FM, NFPA, UL, etc."[4].

Incluso hay estándares de certificación de equipos para uso en sistemas de seguridad de calderas, como el FM 7605, que requieren que los mismos sigan el estándar IEC 61508 cumpliendo un SIL especificado[5] (SIL, *safety integrity level*, es una forma de medir la integridad de un sistema que en principio se basa en la probabilidad de que el mismo falle en responder cuando tiene que actuar).

Por otra parte, los expertos reconocen que las normas como la NFPA por sí solas no garantizan la seguridad, ya que "se puede diseñar un SIS que cumpla todos los requerimientos de estándares prescriptivos como NFPA 85 o 86 y aún así NO satisfagan los requerimientos de un SIS"[6].

Según la ISA, un BMS típico incluirá varias funciones SIL 1 y seguramente una o más SIL 2[7], determinando el uso de más de un SIS o directamente de un resolvedor lógico[8] SIL 2 como

---

[1] ISA, 2004: "Industry update: Safety Instrumented Burner Management Systems (SI-BMS)".

[2] Black Liquor Recovery Boiler Advisory Committee

[3] BLRBAC, 2005: "Instrumentation checklist and classification guide for instruments and control systems used in the operation of black liquor recovery boilers".

[4] BLRBAC, *op cit*.

[5] FM, 1999: "Approval Standard for Programmable Logic Control (PLC) based Burner Management System"

[6] ISA, *op cit*.

[7] ISA, *op cit*.

mínimo, considerando entradas y salidas SIL 1 o 2 redundantes o no según la función a implementar. En realidad, debería notarse que el nivel SIL determinado para un SIS dependerá de los riesgos inherentes al proceso y equipos a controlar, otros sistemas de protección existentes, y en el fondo del nivel de riesgo que se considere tolerable[9].

Hoy, la mayoría de las calderas siguen la NFPA 85. Los datos que siguen reflejan nuestra experiencia en Argentina y Sudamérica, y a la vez son bastante representativos de lo que ocurre en la mayoría de los países[10].

En el caso de la industria de Pulpa y Papel, por ejemplo, al menos tres plantas tienen en cuenta para sus nuevos equipos el cumplimiento de las normas NFPA, FM y ISA, mientras que otra planta sigue usando la NFPA 85, pero ha decidido conformar un equipo de gestión de riesgo corporativo para determinar los pasos a seguir en casos futuros.

En Refinería y Petroquímica, tradicionalmente se ha usado la NFPA 85 para calderas y estándares corporativos o la NFPA 86 para hornos; además (y aunque las normas no lo exigen), típicamente se han usado controladores redundantes para las calderas y triple redundantes para hornos. Ahora, sin embargo, y acorde con la difusión de los nuevos estándares, las grandes compañías están adoptando criterios de la IEC 61511 aunque todavía hay mucha confusión en cuanto a la forma de aplicarla. Por ejemplo, no siempre se realiza un análisis de riesgo para determinar los niveles de integridad, y pocos han implantado un sistema de gestión de seguridad de acuerdo a la IEC; más bien, muchas veces se sigue especificando hardware en base a la tradición y no a un ciclo de vida de seguridad.

A pesar de que la industria en general no se aparta mucho de la media, los profesionales en seguridad funcional de Argentina se destacan. Argentina fue el primer país en adoptar un doble enfoque (determinístico y probabilístico) para la medición de riesgo en la industria nuclear[11], el primero en realizar un congreso internacional sobre SIS en el marco de las IEC 61508/61511[12], y casi el 6% de los ingenieros certificados en seguridad funcional[13] son argentinos. En la industria nuclear, además, se ha adoptado un novedoso concepto de balance de riesgo (además de considerar el riesgo total del proceso, se dispone que ningún riesgo particular supere el 10% del total).

---

[8] *Resolvedor lógico* es la terminología usada por la IEC para el aparato eléctrico, electrónico o programable electrónico que tiene a su cargo la lógica de seguridad; incluye entre otros a PLCs y controladores electrónicos.

[9] Los niveles de riesgo aceptable y tolerable deberían consensuarse entre quien provoca el riesgo, la comunidad expuesta al mismo, y la autoridad de regulación. Puede establecerse por sector: por ejemplo, un estudio de la OHSA considera aceptable 10^{-6} muertes por año, igual que la industria nuclear. En refinación, la estadística actual según API es de $2.4x10^{-5}$ muertes por año.

[10] Las diferencias suelen estar en el nivel de cumplimiento de las normativas legales, existiendo mayor preocupación en países desarrollados donde hay leyes más estrictas y beneficios claros sobre todo en costo de seguros.

[11] Kirk Clark, *Tolerable and Acceptable Risk: Establishing Quantitative Targets for the Hydrocarbon /Petrochemical / Chemical (HPC) Industry*

[12] SISIS 2003

[13] Personas certificadas a junio de 2006 como *Functional Safety Engineer* en el campo de los SIS de acuerdo al *TÜV Functional Safety Program* del *TÜV Rheinland Group*. Es interesante notar la distribución de los certificados: Australia 25%, USA 12%, Holanda 9.7%, Singapur 8.5%, Venezuela 6.7%, Alemania y Argentina 5.9%, Hungría 4.1%, China y Emiratos Arabes 3.5%. Los demás países están por debajo del 2%, incluyendo varios países europeos y latinoamericanos.

Requerimientos de la IEC61511

Después de esta breve introducción, nos centraremos en los requerimientos de la norma IEC 61511 para la implementación de SIS en la industria de procesos, incluyendo por lo dicho los sistemas de seguridad de calderas (e incluso el ESP en calderas de recuperación)[14].

La implementación de este estándar requiere no sólo contar con equipos adecuados, sino también con un sistema de gestión de seguridad con mecanismos de evaluación y auditoría que permitan sostenerla en el tiempo. Estos sistemas de gestión son muy similares a los de calidad ISO 9000, de manera que empresas certificadas podrían extenderlos fácilmente para adaptarlos al marco de la IEC 61511. Pensar que un sistema es seguro de acuerdo a los conceptos de la IEC 61511 sin tal sistema de gestión en funcionamiento es un error, y una evasión de las responsabilidades que competen a la industria por su propia actividad.

El término SIL ha ganado popularidad en la industria, pero la visión que existe en general es incompleta. Por ejemplo, dos errores típicos que se cometen: suponer que basta un equipo certificado para aplicaciones SIL X para estar protegido[15], o asignar un SIL X a todos los sistemas de seguridad sin ningún tipo de análisis[16]. Determinar el nivel SIL requerido para cada función de seguridad no es trivial: un SIL demasiado alto será caro, mientras que si es insuficiente no ofrecerá el nivel de protección necesario.

El estándar IEC61511 lista una serie de cláusulas que se deben satisfacer:

- Requerimientos generales:
  - Gestión de la seguridad funcional
  - Requerimientos del ciclo de vida de seguridad
  - Verificación
  - Información y documentación
- Requerimientos técnicos:
  - Conceptualización, definición de alcance y análisis de riesgo
  - Asignacion de los requerimientos a funciones de seguridad
  - Especificación de los requerimientos de seguridad
  - Diseño e ingeniería del SIS
  - Diseño del software de aplicación
  - FAT
  - Instalación y puesta en servicio
  - Validación
  - Operación y mantenimiento
  - Modificaciones

---

[14] Por otra parte, hay que tener en cuenta que si la autoridad gobernante ha establecido requerimientos aplicables, éstos tienen precedencia sobre la IEC 61511.

[15] Los equipos se certifican *para ser usados* en aplicaciones SIL X: el concepto de SIL se aplica a todo el lazo y no a un solo elemento. Un sensor o actuador puede invalidar el SIL de todo el lazo, aún con el mejor resolvedor lógico del mercado.

[16] Definir, por ejemplo, SIL 3 para todo un proceso, no es conveniente: el análisis de riesgo hay que hacerlo de todos modos para determinar cuáles son las funciones de seguridad a implementar; sin análisis no se puede saber si es necesario agregar más capas de protección porque un SIL 3 pueda ser insuficiente; y el costo de implementar SIL 3 para todos los lazos suele ser muy alto.

- Retiro de servicio (decommissioning)

Lo que sigue es un resumen de algunos puntos importantes a tener en cuenta; para el estudio completo de los requerimientos remitimos a la letra de la norma.

Gestión de la Seguridad

La IEC 61511 requiere que la organización instale un Sistema de Gestión de Seguridad Funcional (FSMS, *Functional Safety Management System*[17]) que asegure que cuando se usen SIS éstos mantengan el proceso en un estado seguro. La organización debe definir una política y una estrategia de seguridad, comunicarla a su gente, y determinar la forma de evaluar su cumplimiento.

Esto implica identificar las personas, departamentos u otras unidades responsables de llevar a cabo y revisar las fases del ciclo de vida de seguridad, informarlas de sus responsabilidades, y asegurar su competencia. La organización debe definir los roles y responsabilidades de cada integrante del equipo, y a quién reporta.

La gestión de la seguridad incluye la evaluación y control de riesgos, planificación de las actividades, e implementación, seguimiento, evaluación y revisión de los sistemas de seguridad. Esto requerirá la conformación de un equipo que tenga la competencia técnica, de aplicación y de operaciones necesarias para la instalación, y que incluya como mínimo un miembro competente independiente (interno o externo) no involucrado en el equipo de diseño para asegurar la objetividad[18].

El equipo debe asegurar que se realice al menos una evaluación de seguridad funcional antes de la puesta en servicio, confirmando que se hizo un análisis de riesgo, se aplicaron las recomendaciones resultantes, se cumplen las especificaciones de requerimientos de seguridad, se validaron los sistemas y se entrenó al personal.

También deben definirse procedimientos de auditoría del sistema (incluyendo frecuencia, *independencia* de los auditores y registro), y procedimientos para modificaciones y cambios.

Uno de los dos conceptos más importantes de la IEC 61511[19] es el de ciclo de vida de seguridad: las actividades involucradas en la implementación de funciones instrumentadas de seguridad (SIF) que comienzan con la fase de conceptualización y terminan cuando las SIF ya no se usan. La norma requiere que las actividades se organicen en un ciclo de vida y que se definan las fases y requerimientos del mismo. Cada fase debe tener sus objetivos, entradas, salidas y actividades de verificación.

Las fases típicas mencionadas por la norma son:

1. Análisis de peligros y riesgos
2. Asignación de las funciones de seguridad a capas de protección
3. Especificación de requerimientos del SIS
4. Evaluación de la seguridad funcional del SIS
5. Diseño e ingeniería del SIS
6. Instalación, puesta en servicio y validación del SIS
7. Operación y mantenimiento del SIS

---

[17] Usamos *seguridad funcional* para diferenciar de la seguridad personal. La seguridad funcional es la que depende del correcto funcionamiento de los SIS y otros sistemas de protección.

[18] IEC 61511-2, 5.2.6.1.2.

[19] El otro es el de Safety Integrity Level (SIL)

8. Modificaciones al SIS
9. Retiro de servicio del SIS

Existe además una fase en paralelo a todas las otras que es la de verificación para asegurar que cada fase provea los resultados requeridos.

Todas estas actividades deben ser planificadas y documentadas desde el principio, como así también las personas que participarán en cada fase y verificación. No menos importante es documentar qué debe verificarse y cómo manejar las no conformidades.

Análisis de Riesgo

El punto de partida para definir los requerimientos de un SIS (e incluso si es necesario o no) es el análisis de riesgo, que se usa para determinar los peligros y eventos peligrosos del proceso y equipos, la secuencia de eventos que pueden causar un accidente, los riesgos asociados, los requerimientos de reducción de riesgo, las funciones de seguridad necesarias para dicha reducción y si alguna de ellas requiere un SIS.

El análisis de riesgo se hace sobre el proceso y equipos asociados, incluyendo al sistema de control (BPCS). Existen diversas metodologías aplicables (Risk Matrix, Risk Graph, FTA, ETA, HAZOP, etcétera); la selección de una de ellas dependerá de la etapa del proceso y del costo involucrado. En la práctica se suele utilizar más de una para contrastar resultados; por ejemplo, se parte de una metodología sencilla y rápida como Risk Graph y luego se aplica un HAZOP en una etapa posterior.

Es responsabilidad del usuario final[20] definir el riesgo asociado con su operación (riesgo inherente del proceso), y la organización debe definir el criterio de riesgo aceptable. Cuando de acuerdo al resultado del análisis un riesgo es superior al aceptable, se definirán las funciones de seguridad necesarias y se asignarán a distintas capas de protección (análisis LOPA). En caso de que sea necesario, se utilizará un SIS para implementar una o más SIF.

Para definir el riesgo aceptable debe considerarse la percepción y visión de aquellos expuestos al peligro, incluyendo también leyes y regulaciones existentes, discusiones con las partes, estándares industriales aplicables, y asesoramiento de expertos. Un modelo utilizable en esta etapa es el ALARP[21] (as low as reasonably practicable), que define como “tolerable” a aquél riesgo que ha sido reducido al punto que el beneficio de reducirlo más es superado por el costo de hacerlo. Usar ALARP implica definir niveles de riesgo inaceptable, tolerable y aceptable[22] en una matriz que se construye en base a factores sociales, políticos y económicos y que dependerá de la filosofía de seguridad adoptada.

Selección del SIS

El SIL requerido será resultado directo del factor de reducción de riesgo (RRF) necesario para llevar el riesgo a un valor tolerable tan bajo como sea razonable. Un factor de reducción alto puede conseguirse con un solo equipo, o usando dos o más equipos independientes que provea cada uno parte de la reducción del riesgo. Esto es válido tanto para los sensores, como para los actuadores, como para el resolvedor lógico[23].

---

[20] ISA, *op cit*.

[21] IEC 61511-3, Annex A

[22] Si un riesgo es *aceptable* no requiere agregar medidas de reducción.

[23] El requisito de independencia es crítico. Es necesario eliminar todos los factores comunes para poder acumular la reducción de riesgo que provee cada equipo.

Los equipos utilizados para implementar el SIS deben ser aprobados conforme a la IEC 61508, o “probados en uso” (este término se refiere al uso de equipos existentes con *amplia experiencia documentada en aplicaciones muy similares*[24] que demuestre que el equipo es apropiado para el nivel de seguridad requerido por la aplicación).

Recordamos una vez más que el análisis de riesgo puede determinar la necesidad de una o más SIF, que se asignarán a uno o más SIS. Si es posible por la cantidad de funciones y señales involucradas, lo más común es utilizar un único SIS que cumpla con los requerimientos conjuntos. En otros casos será conveniente utilizar distintos SIS que pueden tener niveles de integridad (SIL) diferente.

Si el sistema de control (BPCS) se considera una capa de protección, no se le debe asignar un RRF mayor o igual a 10 (de otro modo sería un SIS, y como tal debería estar certificado o probado en uso). También debe considerarse que ciertas fallas del BPCS podrían actuar como eventos iniciadores (por ejemplo, la falla de una salida que pone en condición insegura al proceso).

Normalmente el BPCS y el SIS serán independientes, pero debe analizarse esta independencia y tener en cuenta fallas de modo común (por ejemplo si comparten la alimentación, o si están ubicados en el mismo lugar cuando se analiza un incendio).

La acción del operador considerado como capa de protección debe ser analizada cuidadosamente; típicamente, el RRF no será mayor que 10[25]. En este caso, la alarma que “dispara” la acción del operador debe ser también independiente del SIS, y el sensor que la activa no debe usarse para control (ya que en una falla en el mismo implicaría que no actúen dos capas: el BPCS y el operador). La utilización de sensores con diagnósticos y alarmas permite también que el operador actúe para reponer tan pronto como sea posible el sensor fallado, mejorando la integridad del sistema.

Cuando los sistemas no son totalmente independientes, los RRF no pueden acumularse. En esos casos existen técnicas analíticas para determinar el factor de reducción total. En caso de compartir el mismo hardware para BPCS y SIS se requiere que las aplicaciones estén efectivamente separadas y libres de interferencia[26], y el BPCS no puede ser considerado una capa de protección[27].

Consideraciones para calderas y hornos existentes

En vista de lo anterior y considerando como objetivo final disponer de un sistema acorde con el estándar IEC 61511 con el propósito de garantizar la seguridad funcional, se sugiere cumplir los siguientes pasos:

Si no existe un Sistema de Gestión de Seguridad:

1. Definir un Responsable de Gestión de Seguridad de Procesos.
2. Implementar el Sistema de Gestión de Seguridad

---

[24] Entre otras cosas requiere un límite de confianza mínimo del 70%, con datos de fallas registrados efectivamente en aplicaciones iguales o muy similares y con las mismas condiciones ambientales, configuración, funciones realizadas, interfaces y factores humanos…

[25] Ver IEC 61511-1 y IEC 61511-2, 9.4.

[26] Existen equipos certificados con dichas características: cada aplicación corre en un entorno protegido independiente, aún cuando comparta el mismo hardware. Ver IEC 61511-1 y IEC 61511-2, 11.2.4 y 11.2.9.

[27] Inevitablemente, al ser el hardware común, existen fallas que afectan ambas aplicaciones (ej. alimentación). Lo más sencillo es descartar el BPCS como capa de protección.

a. Definir Misión y Alcance
b. Asignar recursos (Equipo de Seguridad - integrantes con participación full- y part-time)
c. Especificar responsabilidades (análisis de riesgo, implementación de sistemas de prevención, protección y mitigación, capacitación del personal, gestión de mejora continua, auditorías periódicas, etc.)
d. Definir, aprobar y comunicar la Política de Seguridad (incluye estándares a aplicar)
e. Definir los procesos y procedimientos a utilizar (ciclo de vida, metodologías de análisis, etc.)
f. Programar la aplicación de las políticas de seguridad en la planta existente, incluyendo responsabilidades, tiempos y presupuestos.

Para cada caldera u horno en cuestión, en el marco del ciclo de vida de seguridad y documentando todo el proceso:

1. Si reglamentaciones vigentes disponen el seguimiento de otras normas (como las NFPA), analizar las diferencias entre los requerimientos y la instalación actual;
2. En el caso de encontrar requerimientos legales incumplidos, diseñar la solución en forma preliminar;
3. Realizar un análisis preliminar de riesgo (PHA) para determinar las SIF necesarias y estimar el SIL requerido por cada una en el marco de IEC 61511;
4. Analizar si las SIF necesarias ya existen en el sistema instalado (o en las soluciones consideradas en el paso 2), y si son acordes al SIL requerido;
5. Diseñar las modificaciones necesarias al proceso y/o equipos que permitan cumplir los requerimientos del paso 4;
6. Realizar un análisis de riesgo (ej. HAZOP o LOPA) para complementar el análisis anterior y determinar si son necesarias acciones adicionales;
7. Asignar plazos y responsables para las acciones determinadas,
8. Escribir los procedimientos operativos y de mantenimiento que permitan asegurar que el sistema cumple en todo momento con su función,
9. Verificar el cumplimiento de las acciones,
10. Validar el sistema de acuerdo a los requerimientos,
11. Entrenar al personal.

Por supuesto esta es sólo una sugerencia de los pasos a seguir, debiendo adecuarse a cada caso. Lo importante a tener en cuenta es que la base de todo es el sistema de gestión de seguridad funcional: un sistema funcionando adecuadamente, con auditorías periódicas independientes, procedimientos en uso y registros al día, que aplique un modelo de ciclo de vida para los sistemas de seguridad para asegurar que no existan riesgos inaceptables en ningún momento.

---

[*] Jorge Bourdette es Gerente de Investigación y Desarrollo en ABB Argentina y se especializa en control avanzado, sistemas de seguridad e integración de sistemas. Ha implementado sistemas de seguridad de procesos desde 1986, y cuenta con una certificación de TÜV Functional Safety Engineer en el campo de los SIS de acuerdo al TÜV Functional Safety Program.