
# APROBACION DE PRODUCTOS CON IEC 61508 – DESVIANDOSE DEL CURSO

Angela E. Summers, P.E., PhD, President, SIS-TECH Solutions, LP

Publicado en Internet: "IEC 61508 Product Approvals – Veering Off Course," ControlGlobal.com, Julio 2008.
http://www.controlglobal.com/articles/2008/187.html

Mediante un examen detallado, pareciera que el proceso de aprobación de productos de IEC 61508 (1) se ha desviado de su curso, posiblemente dejando muchas aplicaciones de Sistemas Instrumentados de Seguridad (SIS) menos confiables de lo esperado o requerido.

Después de una cuidadosa revisión de una variedad significativa de manuales de seguridad de productos, pareciera que muchos instrumentos de campo están logrando niveles de integridad segura (SIL) más altos de los que pueden ser soportados por los datos de la industria de procesos. El apéndice F.1.3 de libro de CCPS "Guidelines for Safe and Reliable Instrumented Protective System" (2) establece que "una muestra de los datos para transmisores de presión de varios fabricantes reportan valores teóricos de tiempo promedio de fallas peligrosas ($MTTF^D$) que son de tres a diez veces mejores que los datos usados previamente por el dueño/operadora" – un argumento que algunos fabricantes (3) han validado abiertamente.

Desafortunadamente, cambios actualmente considerados por el comité de la IEC 61508 probablemente no mejorarán la situación. Parece que el comité tiene la intención de crear requerimientos adicionales, en vez de abordar serias debilidades estructurales. La única opción razonable es que los usuarios tomen el control de esta situación, rechazando la instalación de cualquier instrumento de campo en una aplicación de seguridad en donde no haya sido demostrada su integridad y confiabilidad requerida en un ambiente de operación similar (Ejemplo una aplicación de Control). Los usuarios deberían exigir que los fabricantes no realicen argumentos exagerados de desempeño, manipulando la fracción segura de falla (SFF), y trasladando la responsabilidad de la operación segura al operador de producción cuando los productos demuestren ser poco confiables. Adicionalmente, los usuarios deben exigir que los manuales de seguridad contengan procedimientos de prueba completos, que logren el cumplimiento con IEC 61511 (5) y los requerimientos de OSHA en gerencia de seguridad de procesos (PSM, 6).

Las siguientes secciones resaltan algunos de los aspectos asociados con los manuales de seguridad y sus argumentos de desempeño.

## Crédito Exagerado del Rendimiento

Antes de la publicación de la IEC 61508, muchos fabricantes proporcionaban datos de pruebas –en servicio- y pruebas de fallas aceleradas. Después de la aprobación de la IEC 61508, los fabricantes comenzaron a manifestar cumplimiento con la IEC 61508, basados en un análisis de laboratorio con condiciones aparentemente perfectas del ambiente operacional. La IEC 61508 permite a los fabricantes manifestar el cumplimiento del SIL basados en un análisis predictivo sin ninguna condición de que

posteriormente soporten esta declaración usando datos de campo, así que técnicamente los fabricantes no están haciendo nada malo. Sin embargo, el índice teórico de falla peligrosa, el índice de falla segura, y los valores de probabilidad de falla en demanda (PFD) declarados en los reportes del análisis son mucho mejores que los que pueden ser alcanzados en aplicaciones actuales de campo. La diferencia entre el análisis teórico y el desempeño en el mundo real es clara y notable.

Con raras excepciones, estos reportes de análisis no proporcionan suficiente información para aclarar completamente la disparidad entre las afirmaciones del fabricante y la experiencia del usuario – exactamente el punto realizado por Thomas y otros (4) al declarar “hace falta calidad y consistencia en los manuales de seguridad”. Los reportes de análisis no proporcionan una descripción de los límites del mismo, configuración e instalación asumida, o los modos de falla y lista de distribución de fallas. Por el contrario, los reportes proveen una tabla resumida de la distribución de la clase de falla. El problema que esto genera, es que mientras los modos de falla y efectos están relacionados al producto y pueden ser evaluados independientemente por el fabricante, la clasificación de la falla depende de la aplicación.

Hay muchas maneras en las que un dispositivo de campo puede ser instalado y configurado, haciendo que la clasificación de falla sea difícil para los fabricantes, especialmente para productos básicos. El fabricante no puede evaluar apropiadamente si una falla debería ser clasificada como segura o peligrosa, sin primero adquirir conocimiento de la aplicación deseada.

Por ejemplo, en una operación típica de modo de demanda donde una válvula operada por solenoide controla el suministro neumático al actuador de la válvula, la falla de la bobina en la solenoide es segura en una aplicación donde se des-energizar para el disparo y es peligrosa en una aplicación en donde se energizar para el disparo. Todas las fallas de una válvula operada por solenoide probablemente sean peligrosas en aplicaciones de modo continuo.

Los usuarios deberían ser proveídos con los modos de falla y resultados de los efectos, no solo con un resumen de la clasificación de falla. Dotado de esta información, el usuario puede así clasificar las fallas de acuerdo con la aplicación deseada y calcular un PFD e índice de disparos inesperados para una aplicación específica.

La mayoría de los reportes no definen claramente el límite del análisis o describen que es lo que se incluye o excluye del análisis. Por una variedad de razones, muchas fallas -en servicio- están excluidas de los reportes de análisis del producto. Algunas fallas se consideran que ocurren debido al desgaste del producto y son excluidas del análisis de vida útil. Los impactos del ambiente operacional, tales como taponamiento, corrosión, e interferencia eléctrica, son considerados problemas de aplicación y de responsabilidad del usuario para analizar y estimar. La visión restringida del producto y su ambiente es una fuente significativa de disparidad entre el análisis teórico y el rendimiento en el mundo real, pero este no es el único problema.

Un excesivo crédito al diagnostico es dado rutinariamente a dispositivos de campo electrónicos programables. Créditos en exceso de hasta un 90% son muy comunes aun con límites restringidos y suposiciones del ambiente operacional. Un alto crédito al diagnostico se traduce directamente a un alto limite de SIL y un bajo PFD reportado. Esto tiene sentido cuando el diagnostico acreditado actualmente da paso a operaciones más seguras y su funcionamiento es periódicamente probado - la misma regla es aplicada a cualquier dispositivo de seguridad. Los diagnósticos se deben poder verificar y auditar.

Desafortunadamente, muchos diagnósticos suministrados por los fabricantes no poseen la capacidad de prueba para el cumplimiento con la IEC 61511 cláusulas 11.3 - Requerimientos del comportamiento del sistema cuando se detecta una falla – y 16.3.1.1 - Pruebas funcionales periódicas la deberán ser conducidas usando un procedimiento escrito para descubrir fallas no detectadas, las cuales previenen que los SIS operen de acuerdo con la especificación de los requerimientos de seguridad. Adicionalmente, los reportes de análisis no incluyen información de la integridad del producto, para los casos en los cuales el diagnóstico no está configurado de acuerdo con el manual de seguridad o si este falla durante la operación.

El manual de seguridad debería describir claramente el límite del análisis y las suposiciones con respecto a la instalación, comisionamiento, configuración, diagnóstico, mantenimiento, y pruebas que soportan el SIL reportado. Sin esta información, es muy difícil para los usuarios cumplir con IEC 61511 Cláusula 5.2.5.3 –Procedimientos deben ser implementados para evaluar el rendimiento de los sistemas instrumentados de seguridad contra sus requerimientos de seguridad – el cual requiere una comparación entre las suposiciones de confiabilidad del equipo con el rendimiento operacional de campo. Los modos de falla y sus efectos identificados deben ser incluidos en la guía de mantenimiento de problemas técnicos para que las fallas generadas durante la operación sean rastreadas usando los mismos modos, permitiendo a los usuarios comparar periódicamente los resultados actuales de operación contra los argumentos del fabricante.

## Manipulación de la fracción de falla segura

El comité de la IEC 61508 incluyo la fracción de falla segura (SFF) y los requerimientos de tolerancia de falla del hardware asociado como una manera de evitar que los fabricantes afirmen tener altos SIL para dispositivos no redundantes, simplemente basándose en los cálculos de PFD. Las tablas de SFF fueron creadas con la intención de asegurar la tolerancia a falla (por medio de la redundancia requerida) en un ambiente de datos teóricos optimista. Sin embargo, debido a que la SFF es calculada a partir de los mismos datos potencialmente “errónea”, la SFF es susceptible al mismo error.

En la práctica, no hay correlación entre la SFF y la seguridad del producto. Lo inverso ha sido demostrado en el proceso de aprobación del producto, donde ha llegado a ser mas fácil certificar para SIL-3 un dispositivo con un total de fallas alta y nivel de diagnostico elevado, que lo que es certificar un dispositivo con un índice total de fallas bajo pero sin diagnostico.

Si se realiza una revisión de varios manuales de seguridad, es obvio que la manipulación de la SFF es bastante común. Muchos reportes de análisis, descartando directamente la intención original de la SFF, han incluido clasificaciones de falla que ni siquiera son reconocidas en la IEC 61508 o IEC 61511. Contrario a lo que estos reportes frecuentemente establecen, las fallas “sin efecto”, “residual”, “sin importancia”, y ‘anuncio no detectado’ no son discutidas en la IEC 61508 y no son incluidas en ninguna definición de falla.

En algunos reportes de análisis, clases de fallas, tales como “sin efecto”, “sin importancia”, y “residual” están siendo definidas ligeramente como una falla que no es ni segura ni peligrosa. La IEC 61508 define una falla como el cese ó finalización de la habilidad de una unidad funcional para realizar una función requerida. Definiciones similares pueden encontrarse en la IEC 61511 y el libro CCPS, “Guidelines for Safe and Reliable Instrumented Protective Systems”. Si el dispositivo no ha fallado hacia un estado determinado – seguro o peligroso - aun esta funcionando. No ha finalizado su habilidad para funcionar

como es especificado. Sin embargo, el análisis ha tomado estas “no-fallas” como seguras en los cálculos de la SFF, por lo tanto, artificialmente se están exagerando los valores calculados de la SFF.

La IEC 61508 solo reconoce dos tipos de fallas, segura y peligrosa, así que debe ser que los analistas creen que cualquier falla degradada, no segura o no peligrosa puede ser catalogada como una falla segura. Irónicamente, aunque estas “no-fallas” por lo general están incluidas en el cálculo de la SFF, los reportes de análisis recomiendan no incluirlas en ningún cálculo de índice de disparo inesperado.

Algunos reportes están definiendo “anuncio no detectado” como la falla del circuito de diagnostico de manera tal que no anunciara la ocurrencia de una falla en el futuro. La simple verdad es que, si el usuario no es notificado de la falla del diagnostico, el usuario no puede estar en cumplimiento con la IEC 61511 Cláusula 11.3, la cual cubre los requerimientos para el uso de pruebas de diagnostico, pruebas funcionales u otros medios para detectar fallas peligrosas. Las Fallas peligrosas del diagnostico no deberían ser clasificadas como seguras, pero una vez más, los analistas están reportando consistentemente fallas de “anuncio no detectado” como seguras e increíblemente citan la IEC 61508 como la base de su argumento.

Cuando los analistas clasifican estas “nuevas” clases de fallas como seguras, el producto logra una más alta SFF sin ningún beneficio significativo de seguridad. Frecuentemente, se asume que los productos con componentes mecánicos tienen un porcentaje substancial de fallas de “sin-efecto”, logrando así valores de SFF mayores que 60% o 90% de los valores requeridos para reducir los requerimientos de tolerancia a falla del hardware de acuerdo con la IEC 61508 Tablas 5 y 6. Una SFF más alta frecuentemente conlleva a reportar límites de SIL 2 ó SIL 3 sin ningún requerimiento de redundancia.

Por ejemplo, una fabricante de válvula de globo actuada por diafragma ha reportado índices de falla “sin efecto” de 9.356e-03 por año en un producto con solo 8.226e-03 por año de fallas reales seguras y peligrosas. Se incluyen una cantidad mayor de “no fallas” que de fallas reales. La SFF calculada sin la falla de “sin efecto” es 59.2%, el cual esta por debajo del argumento de SIL 2 para un componente de clase A. Incluyendo la falla de “sin efecto”, la SFF incrementa a un 80.9%, suficiente para lograr un SIL 2.

Todo esto nos dice, que estas “nuevas” clases de fallas parecen haber sido creadas desde la aprobación de la IEC 61508 únicamente con el propósito de exagerar la SFF; así que, estas “nuevas” clases de fallas son construcciones teóricas insostenibles - esto es lo mismo a la teoría del flogisto aplicada a la ingeniería de seguridad. Los usuarios deberían rechazar los argumentos de tolerancia de falla de hardware basados en estas clases de fallas y deberían exigir que los fabricantes soporten sus argumentos siguiendo principios de ingeniería aceptados y confiables.

## La tendencia a cambiar la responsabilidad de la operación segura al operador

Muchos reportes argumentan niveles SIL asumiendo que las fallas detectadas están configuradas para alertar en vez de forzar la falla del producto a su estado seguro especificado. Esta suposición permite a los fabricantes reportar un bajo índice inesperado de disparos y un índice bajo de falla peligrosa no detectada, aun cuando el producto es inherentemente poco confiable. Bajo los requisitos de la IEC 61508, un producto con un alto índice total de fallas puede lograr un alto nivel de SIL siempre y cuando su falla es detectada y anunciada. La SFF no es penalizada por la opción de alarmar en vez de alcanzar el estado seguro. Por lo tanto, entre más fallas sean detectadas, más alto se vuelve la SFF, sin importar el numero

de veces, o la cantidad total de tiempo, que el dispositivo este en el estado de falla, dejando la responsabilidad de la protección del proceso en manos del operador.

La detección de falla simplemente informa al usuario que el dispositivo no es capaz de operar como lo es requerido; el mismo no logra o mantiene la seguridad del proceso. Continuar con la operación del proceso con un SIS degradado o deshabilitado es una decisión seria, que requirieren medidas de compensación planificadas que aseguren una operación segura y proporcionen una reducción de riesgo equivalente. Muchos sistemas instrumentados de seguridad (SISs) están instalados porque el operador no tiene suficiente tiempo, no esta continuamente presente, o no es capaz de lograr una reacción de protección consistente y confiable en el tiempo requerido. Si el análisis de peligro y riesgo ya ha acreditado el reconocimiento apropiado de una alarma por parte del Operador, la contribución del operador a la gerencia del peligro del proceso ya ha sido considerada. El que un operador reconozca una alarma de diagnostico, no reduce el riesgo o hace al operador sea mas fuerte, mas rápido, o mas inteligente. Solo el usuario, por medio de una consideración cuidadosa de muchos factores específicos de la aplicación, incluyendo el peligro del proceso, tiempo seguro del proceso, atención del operador, acciones requeridas para el estado seguro, y la carga de trabajo del operador, podrá determinar si el operador es capaz de proveer reducción de riesgo equivalente mientras la falla detectada es corregida.

Los fabricantes que recomiendan que las fallas sean alarmas en vez de tomar una acción apropiada de seguridad, están posiblemente aceptando una responsabilidad significativa. Ellos simplemente no tienen suficiente información acerca de la operación deseada o el riesgo del proceso para realizar estas recomendaciones. Desafortunadamente, casi todos los reportes de análisis revisados asumen que el operador esta listo para intervenir y sustituir al sistema básico de control de proceso (BPCS) y/o SIS inmediatamente después de recibir una alarma de diagnostico y que ellos están disponibles para monitorear los equipos de proceso hasta que el dispositivo fallado vuelva a estar en servicio. Tales suposiciones son irreales y fabricantes deberían aconsejar mucho mejor y proporcionar los análisis detallados de los modos de falla y efectos, para que así los usuarios entiendan lo que es necesario para una operación segura, puedan calcular el PFD de una aplicación específica y el índice de disparo inesperado.

## Falta de un Procedimiento de Prueba completo

El usuario debe validar y demostrar periódicamente que el equipo opera de acuerdo con la especificación de requerimientos de seguridad. Esta demostración incluye diagnósticos, alarmas, operaciones manuales, y funcionalidad de seguridad como lo es requerido por la IEC 61511 cláusula 11.3, 16.2.2, y 16.3. Desafortunadamente, pocos de los procedimientos de prueba revisados satisfacen los requerimientos de OSHA PSM de una prueba testificada de la habilidad del equipo para operar como es requerido.

La mayoría de los manuales de seguridad proveen un alcance limitado de las pruebas con coberturas estimadas de las mismas. La operación del producto no se comprueba completamente con estas pruebas parciales. Dado que los modos de falla y distribuciones no son proporcionados, no es posible determinar si la cobertura de la prueba declarada es razonablemente conservadora, o cuales fallas están cubiertas por la prueba sugerida y cuales no. Como se discutió anteriormente, los procedimientos de prueba no contemplan la prueba del diagnóstico del producto. Muchos dispositivos han logrado declarar altos limites de SIL a través grandes factores de cobertura de diagnostico; incluso, medios y procedimientos para probar los diagnósticos no son proporcionados o discutidos en la mayoría de los manuales de seguridad revisados.

Los manuales de seguridad deberían proveer procedimientos de prueba que demuestren la operación del equipo, incluyendo diagnostico, funciones de alarma y disparo. Las pruebas parciales y los diagnósticos son herramientas que permiten la validación mas frecuente de un subconjunto de modos de falla, pero el uso de pruebas parciales no elimina la necesidad de una prueba funcional completa. Fundamentalmente, todas las capas de protección deben ser capaces de soportar una auditoría, por lo tanto pruebas periódicas son necesarias para asegurar que los errores sistemáticos no han degradado el rendimiento del equipo. Pruebas incompletas no pueden ser aceptadas cuando estas están basadas únicamente en técnicas probabilísticas. Cualquier falla que no es cubierta por una prueba es una condición latente que puede manifestarse en cualquier momento durante la vida útil del equipo. Ningún usuario debería aprobar un dispositivo para una aplicación de seguridad que no pueda ser completamente probada, con la finalidad de asegurar la operación apropiada de acuerdo con la especificación de requerimientos de seguridad.

## Camino a seguir

Los procesos operan en una manera segura cuando el equipo instalado cumple con los requerimientos de operabilidad, confiabilidad y capacidad de mantenimiento del dueño. La seguridad no es sostenible cuando se usan equipos poco confiables. Equipos de baja confiabilidad incrementan el costo de mantenimiento, reducen la confianza de los operadores en el equipo y de aquellos que los especifican, y aumentan el riesgo general debido a la desestabilización del proceso, parada y arranques. Los usuarios deben determinar que tan bien funciona el dispositivo en la aplicación deseada. Información del uso previo del dispositivo es esencial para asegurar una instalación, comisionamiento, prueba y mantenimiento adecuado en la industria de procesos.

La raíz del problema del manual de seguridad esta en el entendimiento inadecuado por parte de los fabricantes de lo que en realidad necesitan los usuarios. Los manuales revisados no contienen suficiente información para asegurar cumplimiento con IEC 61511 o los requerimientos de OSHA PSM. Para proporcionar un mejor soporte a los usuarios, los fabricantes deben hacer análisis razonables y conservadores de sus productos y proporcionar una mejor documentación de las premisas. Los usuarios requieren más que una tabla de números para verificar que las premisas hechas en el análisis corresponden con la aplicación del dispositivo. Los fabricantes son responsables de proporcionar la “información fundamental para aquello por lo cual tienen control, permitiendo así a los usuarios hacer su trabajo de manera efectiva y consiste (4)”. Por el contrario, la mayoría de los dispositivos hacen argumentos exagerados que son basados en evidencias débiles y en muchos casos sospechosas.

Desafortunadamente, parece que muchos de estos problemas no serán contemplados por una próxima emisión de la IEC 61508. Miembros del comité están siendo impulsados a considerar seriamente cambios a la IEC 61508 que dirijan a los fabricantes en una dirección que da paso a productos seguros y confiables. Los fabricantes deberían ser forzados a suministrar los análisis de modos de falla y efectos con distribuciones de falla, para que los usuarios puedan rastrear las fallas de acuerdo a los modos definidos. Ellos también deberían ser forzados a reportar los datos “en-servicios”, asegurando que las afirmaciones del producto puedan ser soportadas por el desempeño en campo. Los fabricantes no deberían asumir que es seguro alarmar una falla en vez de forzar el producto a su condición de estado seguro. Ellos deberían reportar los modos de falla que pueden ser detectados y permitir a los usuarios determinar si es apropiado alertar o disparar basado en el análisis de peligro y riesgo de los equipos de proceso. Finalmente, los fabricantes deberían proveer procedimientos de prueba que evalúen completamente toda la funcionalidad

requerida del producto, para que los usuarios logren y permanezcan en cumplimiento con la IEC 61511 y OSHA PSM.

## Referencias

IEC 61508, *Functional Safety of Electrical /Electronic/Programmable Electronic Safety Related Systems,* Parts 1-7, Geneva, Switzerland (1999-2001).

*Guidelines for Safe and Reliable Instrumented Protective Systems*, American Institute of Chemical Engineers, NY, (2007).

http://www.emersonprocess.com/rosemount/solution/faq61508.html

Thomas, Harold, David Deibert, David C. Arner, and David Weir, Air Products & Chemicals, Inc., *"Safety Instrumented System Manuals-A Need to Balance Reliability and Safety,"* Process Safety Progress, Vol 27, No 1 (March 2008)

IEC 61511, Functional Safety: *Safety Instrumented Systems for the Process Industry Sector*, Geneva, Switzerland (2003).

OSHA, "Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents, 29 CFR Part 1910." Federal Register 57, 36, Washington, DC (1992).