SISTEMAS DE SEGURIDAD
IEC61508

JOSE CARLOS RUIZ
SIEMSA CONTROL Y SISTEMAS, S.A.

En gran número de procesos industriales el hecho de transformar o manipular las materias primas, o incluso los equipos-herramientas empleados, pueden aportar un cierto peligro. El punto de vista de la sociedad ante dichos peligros ha cambiado considerablemente a lo largo del presente siglo y en mayor medida durante las dos últimas décadas, de ser considerado como una situación normal, en la cual el hecho de que existiesen accidentes era admitido, a ser totalmente repudiado y perseguido.
En la mente de muchos de nosotros persisten accidentes por todos conocidos, desde el más espectacular de Chernovil, ¿Cuántas vidas, enfermedades y daños ha provocado?; Hasta aquellos recientes en los cuales el impacto ha sido "únicamente" medioambiental como las minas de Aznalcollar o los producidos por derrames de petróleo (petroleros, oleoductos, etc.); sin olvidarnos de cientos de accidentes que han provocado desde un número limitado de heridos hasta cientos de muertos (Bhopal, India >2500 muertos).
Las nuevas tendencias exigen de nosotros garantizar un menor impacto en el entorno eliminando o mitigando aquellos peligros que lleve asociada nuestra actividad productiva, por lo que optamos por tomar determinadas medidas y protecciones que garanticen una mayor seguridad.
En el presente articulo se presentan diferentes standards internacionales aplicables, y se repasa en detalle la normativa IEC61508, todavía en fase de aprobación.

1. INTRODUCCION

¿Qué es un sistema de seguridad?. Si atendemos a la definición del Health and Safety Executive (HSE) "Es un Sistema diseñado para responder a las condiciones de proceso que pueden ser por si mismas peligrosas o, si no se tomasen medidas, podrían llevar eventualmente a aumentar el peligro, y que genera la salida adecuada para mitigar las consecuencias peligrosas o prevenir el peligro."
Tradicionalmente, las seguridades de los procesos productivos, y de muchas máquinas – herramientas, recaían en relés especiales cableados y conectados utilizando la técnica de "Fallo Seguro" ó utilizando circuitos electrónicos de estado sólido; en ambos casos las probabilidades de fallo eran bien conocidas y garantizaban una seguridad adecuada a las necesidades, a éste hecho debemos añadir que las necesidades de rentabilidad/producción eran inferiores lo que suponía trabajar con márgenes de seguridad superiores. Adicionalmente estos sistemas eran auténticas cajas negras mínimamente manipulables lo que garantizaba su integridad.
Con la aparición de los Sistemas Programables, estos han ido cogiendo mayor fuerza debido a su versatilidad, programabilidad, y algo muy importante, en todos los aspectos, son fácilmente manipulables; lo que ha llevado al uso inadecuado de dichos equipos en seguridad, llegándose a emplear en algunos casos los mismos Sistemas de Control como Sistemas de Seguridad.
Existen una serie de normativas internacionales que regulan el uso de equipos electricos-electrónicos en aplicaciones de seguridad, quizá las más conocidas y reconocidas son:

- DIN V VDE 0801 – Principios para Ordenadores en Aplicaciones relacionadas con Seguridad.
- DIN 19250 – Requisitos aplicables a los Sistemas de Seguridad para cumplir con la DIN V VDE 0801

Otras son más específicas, como:

- EN 50156 – Equipos eléctricos en Hornos
- EN 60204 – Seguridades de equipamientos eléctricos de maquinas.

o la más reciente ISA SP-84 – Aplicación de Sistemas de Seguridad en procesos industriales.
Recientemente se está impulsando la creación de una normativa aplicable internacionalmente y que sirva como punto de partida a aquella más específicas de la aplicación o la tecnología.

2. PRINCIPIOS BASICOS

La normativa IEC 61508 está dividida en los siguientes apartados:
Aptdo.1 – Requisitos Generales (Normativa)
Aptdo. 2 – Requisitos para Sistemas E/E/PE (Normativa)
Aptdo. 3 – Requisitos de Software (Normativa)

Aptdo. 4 – Definiciones y Abreviaciones de Términos.
Aptdo. 5 – Sugerencias sobre la Aplicación del Aptdo. 1.
Aptdo. 6 – Sugerencias sobre la Aplicación del Aptdo. 2.
Aptdo. 7 – Bibliografía de Técnicas y Medidas.

Los sectores de aplicación de la IEC61508 son:
- Industria de Proceso (Sistemas de Parada de Emergéncia, Sist. de Detección de Fuego y Gas, Control de Hornos y Quemadores)
- Industria de Manufactura (Robots, Maquinaria)
- Transporte (Señalización en Ferrocarriles, Ascensores)
- Medicina

Las siguientes definiciones y puntos son de clave importancia para seguir la IEC 61508:

- Definición de Riesgo y Reducción del Riesgo:
  El riesgo existente en una actividad viene directamente relacionado con la extensión de los daños y la frecuencia con la que ocurre el evento, por lo que podemos establecer una ecuación del tipo:
  R = E * F
  donde:
  - E – extensión de los daños
  - F – frecuencia del evento

  Se pretende conocer con exactitud el Riesgo, para desde este punto de partida determinar las medidas de reducción del riesgo que lo permitan ser tolerable, para ello se utilizarán aquellos medios/métodos que permitan reducir el riesgo, actuando sobre la extensión y/o sobre la frecuencia.

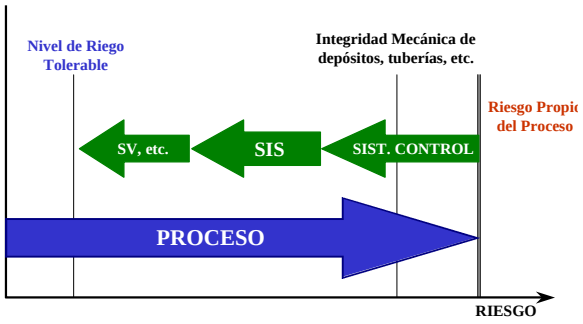

Figura 1 – Riesgo - Reducción del Riesgo

La evaluación del riesgo se puede realizar de dos formas, cualitativa y cuantitativa; en la primera se formará un grupo de expertos que tras análisis detallados utilizando HAZOPS, tablas tipo SI-Evento, árbol de fallos consecuencias determinará las frecuencias y la extensión; en el método cuantitativo se utilizarán tablas estadísticas para determinar la probabilidad y el impacto.
Una vez conocido el Riesgo podremos dictaminar en que medida deberemos reducirlo hasta hacerlo tolerable, o lo que es lo mismo, la frecuencia es tan baja y/o el daño tan reducido que podemos permitirnos actuar con el requisito actual.

- Integridad de la Seguridad, que se define:
  "La Probabilidad de que un Sistema relacionado con Seguridad realice adecuadamente la totalidad de las Funciones de Seguridad requeridas bajo todas las *circunstancias establecidas* y durante *el Período de Tiempo Especificado*.
  La Integridad de la Seguridad viene determinada por la Integridad del Hardware y la Integridad del Software; en el primer caso la IEC61508 establece los fallos del hardware (incluyendo las de modo común del hardware) indicando el objetivo a cumplir en función del SIL "*Safety Integrity Level*"

Safety Integrity Level	**MODO DEMANDA DE OPERACION PFDavg (1)**	**MODO DE DEMANDA DE OPERACION CONTINUA – ELEVADA (2)**
4	$>= 10^{-5} – 10^{-4}$	$>= 10^{-9} - 10^{-8}$
3	$>= 10^{-4} – 10^{-3}$	$>=10^{-8} – 10^{-7}$
2	$>= 10^{-3} – 10^{-2}$	$>=10^{-7} – 10^{-6}$
1	$>= 10^{-2} – 10^{-1}$	$>=10^{-6} – 10^{-5}$

(1) – PFDavg – Probabilidad de fallar la función para la que se ha diseñado bajo demanda. Este factor se ve profundamente afectado por los diagnósticos pudiendo cambiar su valor por 10 e incluso por 100 con lo caul el requisito puede cambiar de SIL 1 a SIL 2 por ejemplo.

(2) Probabilidad de un fallo peligropso por hora.
La Integridad Sistemática es de dificil evaluación y puede venir dictaminada por fallos de hardware, software, operación, etc.; la IEC 61508 proporciona una serie de consejos que permitan disminuir dichos fallos, las técnicas vienen dictaminadas por el SIL.

- El Ciclo de vida de la Seguridad

Tal y como se representa en la Figura 2 se define el "Ciclo de Vida", en el que se especifican todos los pasos a seguirse desde el inicio y desarrollo conceptual del proyecto hasta la finalización de la vida de la instalación y su retirada. En el caso en concreto, para los sistemas de Seguridad

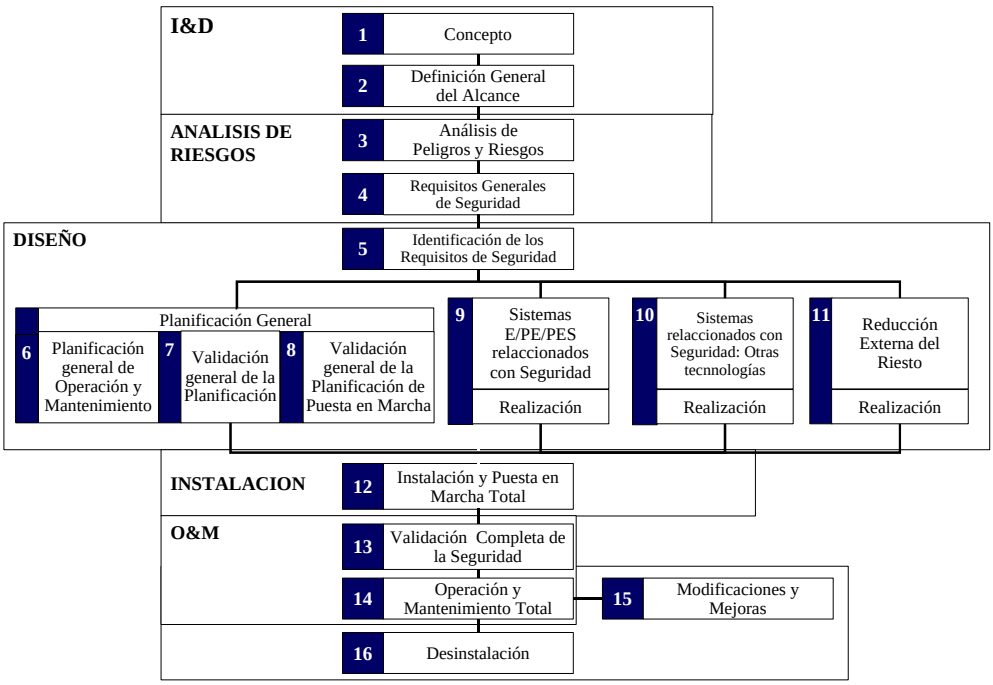

Figura 2 – Riesgo - Reducción del Riesgo

Programables (Punto 9), deberemos estudiar en detalle dos conceptos de máxima importancia ya indicados anteriormente, el Ciclo de Vida de la Integridad del Hardware y el Ciclo de Vida de la Integridad del Software.

Otro punto importante dentro de la normativa, es el indicado en el punto 14 de la Figura 2 "Operación y Mantenimiento", en el que se detallan los pasos a seguir ante un fallo de operación o durante las actividades rutinarias de mantenimiento incluyendo aquellos pasos relativos a la gestión.

En el Apartado 1 también se detalla el nivel de independencia y el grado de formación del equipo de asesores que dictamine y evalúe el Nivel de Seguridad, indicando para cada SIL la recomendación de trabajar con personas, equipos y organizaciones independientes.

En el Apartado 2 se especifican los requisitos (hardware) para cada nivel SIL, mencionando las técnicas y medidas aplicables; se incluyen 3 tablas indicando para cada SIL, en función de la configuración elegida, los diagnósticos y el tiempo entre pruebas (con sistema parado), el tiempo medio estimado para tener un fallo; estas tablas están divididas para Sistemas E/E/PE, sensores y elementos finales.

Este apartado se encuentra actualmente en discusión y está pendiente de aprobación final, a diferencia de los apartados 1,3,4 y 5 que se mantendrán tal cual hasta la revisión final; uno de los puntos de discusión son los requisitos y los modelos de fallo para los diferentes modelos hardware así como en los diferentes datos de cálculo aplicables, en muchos conceptos la IEC 61508 sigue los datos y procedimientos establecidos en la prEN 50156-1, siendo esta más restrictiva en algunos conceptos que la IEC 61508 dado que exige que la totalidad del equipo sea seguro ante la ocurrencia de un primer fallo, mientras que esta ultima tolera un punto de fallo único, indicando explícitamente que en tal caso se puede llegar a tener un "Fallo Peligroso"; lo que supone que equipos con canal único no pueden ser empleados en aplicaciones clasificadas como SIL3, y aquellos que utilizan técnicas de redundancia 1oo2 ó 1oo2D deberán parar la instalación ante un fallo de sus componentes.

3. CONCLUSION

La IEC61508, todavía sujeta a aprobación definitiva, establece unos métodos completos para el análisis y determinación de requisitos de seguridad, en un principio diseñada para ser aplicables con Sistemas Electrónicos Programables, siendo algunos de los puntos extensibles a Sistemas Eléctricos y Electrónicos, todavía en discusión.

Tal y como se ha referenciado anteriormente su ámbito de aplicación no se limita a la industria de procesos, se encuentra en preparación la normativa IEC61511 dedicada en exclusiva a la Industria de

Control de Procesos conteniendo 7 apartados similares a los indicados para la IEC 61508 en la cual se basa. USA ha pedido a la IED que mientras se termina la elaboración y aprobación de la normativa IEC 61511 se utilice la ISA S84.01, petición que ha sido contestada favorablemente.

Tanto en la IEC61508 como en la IEC 61511 se establecen los requisitos para Sistemas Electrónicos Programables empleados en Seguridad, dándose a entender que dichos equipos deben cumplir una serie de requisitos pero nunca limitando su campo de aplicación a un conjunto determinado. Sin embargo la ISA S84.01 establece claramente la recomendación de diferenciar los equipos en función de su utilización, segregando equipos de control, equipos de seguridad, etc. (ver figura 3). Si bien este concepto se puede extraer de la IEC como una medida empleada para reducir los riesgos de modo común de la aplicación.

Por último cabe mencionar que en el uso de sistemas de seguridad, no existe incompatibilidad entre seguridad y disponibilidad, ya que se indican técnicas para obtener unos MTBFs elevados, pero que siempre debe predominar el desarrollo basado en la seguridad, y que como tal todas las partes involucradas en el "Ciclo de Vida Total" aporten sinergias comunes que permitan incrementar la seguridad de la instalación, incluyendo su desmontaje.

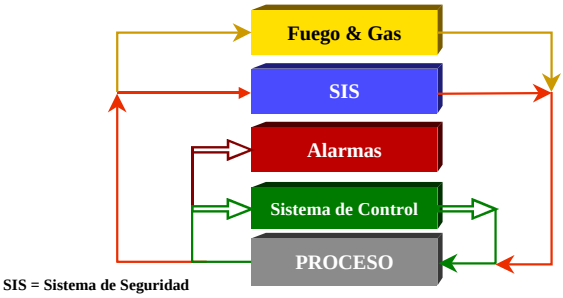

Figura 3 – Capas de Protección

BIBLIOGRAFIA

- Draft IEC 61508
- "Design Critical Control or Emergency Shut Down Systems for Safety AND Reliability" - Robert S. Adamski; Triconex
- "Use of Quantitative Risk Assessment to increase Reliability of Turbomachinery Shutdown Systems" – Angela Summers; Premier Consulting Services