

# Por qué la Arquitectura de los Sistemas de Seguridad No Importa

Roger Prew

Consultor de Seguridad

ABB

Howard Road, St. Neots, Reino Unido

## Resumen

¡“Más” puede ser “Menos” cuando se aplica a la Arquitectura de los Sistemas de Seguridad!

Cuando ABB introdujo sus primeros Sistemas de Seguridad en el Mar del Norte a finales de los años 70's, la arquitectura interna del sistema era de gran importancia. La forma en que los constructores de sistemas demostraban que su diseño podría alcanzar los niveles de integridad necesarios para las aplicaciones de seguridad era principalmente mediante la explicación de cómo la estructura interna proporcionaba redundancia. Al paso de los años, términos tales como votación 1oo2 y 2oo3, DMR, TMR y sistemas Quad han sido aceptados (si bien no totalmente comprendidos) en el mercado y aún aparecen en las especificaciones de requerimientos de clientes y en folletos de proveedores. Sin embargo, desde la llegada de los estándares IEC61508 e IEC61511, el término “Integridad de la Seguridad” (“Safety Integrity”) está totalmente definido y ha conducido a una nueva generación de sistemas donde los términos DMR, TMR y Quad no se aplican y son irrelevantes. Roger Prew, Consultor de Seguridad en ABB argumenta que la categorización de la nueva generación de sistemas por la arquitectura de su hardware ya no es relevante y debe evitarse.

## 1. ¿Qué Hace un Sistema de Seguridad?

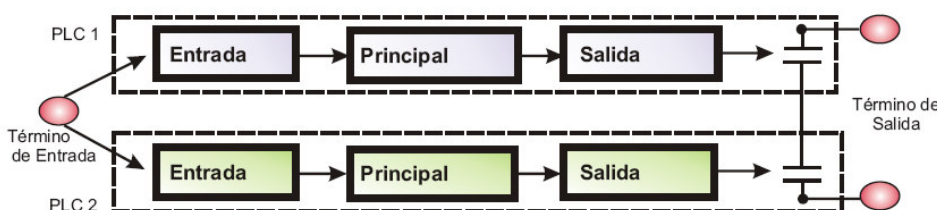
El propósito de un Sistema de Seguridad o de un SIS (Safety Instrumented System) es estar disponible en todo momento para llevar automáticamente un proceso peligroso a un estado seguro en el caso de una falla en algún lugar del proceso.

La mayoría de los Sistemas de Seguridad utilizados en las industrias de proceso son aplicaciones de baja demanda en donde el estado de seguridad del proceso está claramente definido y el sistema sólo es requerido para entrar en acción si surge una emergencia.

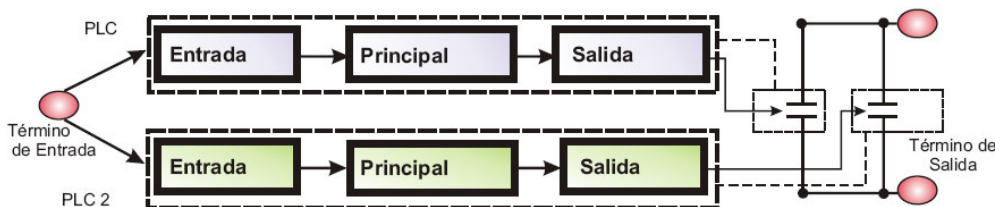
En consecuencia, las cualidades funcionales que necesita un sistema de seguridad son, primeramente, seguir estando disponibles para una acción de paro de emergencia (ESD) durante tanto tiempo como sea posible (Alta Disponibilidad MTBF), y en segundo lugar, ser capaz de responder ante fallas de sí mismo de una manera predeterminada y segura (Acción de Seguridad ante Falla). Los falsos disparos ocasionados por fallas del sistema de seguridad son tanto potencialmente peligrosos como extremadamente costosos para el operador.

¡En los primeros sistemas estas dos cualidades frecuentemente se hacían confusas! Si podía garantizarse el 100% de disponibilidad del sistema, entonces el modo de falla de los sistemas es irrelevante y no hay necesidad de diagnósticos internos o cualquier forma garantizada de acción a prueba de fallas.

En la práctica, el objetivo de los diseñadores era obtener altas cifras de MTBF mediante la aplicación de arquitecturas redundantes tolerantes a fallas para compensar el hecho de que los diagnósticos internos eran limitados y podían ocurrir modos peligrosos de fallas (aunque con poca frecuencia). Por lo tanto, el sistema Triple o Cuádruple con tolerancia a fallas inherentes y consecuentemente alto MTBF podía alcanzar un alto PFD (Probability of Failure on Demand) con baja cobertura de diagnóstico. Muchos de estos sistemas usaban algoritmos de votación simple como 1oo2 (1 de 2) o 2oo3 (2 de 3) para identificar fallas y tomar las acciones pertinentes. Los sistemas de votación son una forma extremadamente elegante para identificar que ha fallado una u otra ruta de la señal, pero no proporcionan mucha información sobre la causa de la falla y qué acción debe tomarse. Sólo que la falla ha ocurrido en una de las rutas de la señal. A diferencia del diagnóstico activo en tiempo real, la votación solamente tiene lugar cuando ocurre una demanda en el sistema – ¡cuando puede ser demasiado tarde! Además, un sistema convencional dual redundante puede tanto proporcionar disponibilidad cuando la votación se configura a 1 de 2, o integridad cuando la votación se configura a 2 de 2. ¡Pero no ambas! Este es un hecho que con frecuencia no se comprende.



**Figura 1 Un sistema dual 1oo2 proporciona Alta Integridad, pero Baja Disponibilidad**



**Figura 2 Un sistema dual 2oo2 proporciona Alta Disponibilidad pero Baja Integridad**

## Por qué la Arquitectura de los Sistemas de Seguridad No Importa

Hasta la adopción de los estándares IEC61508 e IEC61511, las cifras de MTBF o PFD eran la principal medida para evaluar la calidad de un sistema de seguridad. Sin embargo, es una métrica relativamente burda para sistemas de automatización basados en software extremadamente sofisticado y no se ocupa de cuestiones tales como cobertura de diagnóstico, fallas sistemáticas, problemas de modo común y la calidad e integridad del software.

### 2. IEC61508 / IEC61511

Los autores de los estándares IEC reexaminaron los requisitos básicos que necesitan satisfacerse para alcanzar la integridad de la seguridad<sup>1</sup> y la reducción de riesgo y definieron cuatro criterios de medición principales que los sistemas deben alcanzar a fin de que el SIL (Safety Integrity Level ) se considere que cumple con los niveles definidos en los estándares y que ahora se esperan por la industria en general. Estos son:

- La integridad de la seguridad del hardware se refiere a la capacidad del hardware para minimizar los efectos de peligrosas fallas aleatorias del hardware, y se expresa como un valor de PFD (Probability of failure to danger ).
- Funcionamiento del sistema posterior a la detección de una condición de falla. Los sistemas de seguridad necesitan ser capaces de emprender acciones a prueba de falla, la cual es una habilidad del sistema para reaccionar de una forma segura y predeterminada (por ejemplo, un paro de planta) bajo todos y cada uno de los modos de falla. Generalmente esto se expresa como el SFF (Safe Failure Fraction) y se determina a partir de un análisis de la cobertura del diagnóstico que el diseño puede alcanzar (véase más adelante).
- El nuevo parámetro importante es el SFF (Safe Failure Fraction) el cual es una medida de la cobertura y la eficacia del diagnóstico en el sistema. A fin de acomodar diseños previos de sistema basados en altos niveles de redundancia y menores niveles de cobertura del diagnóstico, el estándar considera la arquitectura completa del sistema en la evaluación del SIL alcanzado. La máxima clasificación SIL está relacionada con el SFF (Safe Failure Fraction) y con el HFT (Hardware Fault Tolerante), de acuerdo con la Tabla 1 que se muestra más adelante.
- La integridad sistemática de seguridad se refiere a fallas que puedan surgir debido al proceso de desarrollo del sistema, diseño y puesta en marcha de funciones instrumentadas de seguridad, incluidos todos los aspectos de su gestión operativa y de mantenimiento de la seguridad en su ciclo de vida.

Las cifras PFD y SFF pueden ser evaluadas para una configuración específica del sistema a partir de los FMEA (Failure Modes and Effects Análisis) y los requisitos para satisfacer los 3 niveles SIL aceptables en las industrias de proceso que se muestran en la tabla siguiente.

Fracción de falla segura SFF	Tolerancia a fallas del Hardware (véase nota)		
	0	1	2
< 60%	No permitido	SIL 1	SIL 2
60% - < 90%	SIL 1	SIL 2	SIL 3
90% - < 99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

Nota 2: Una tolerancia a fallas del hardware de N significa que N + 1 fallas no detectadas podría causar una pérdida de la función de seguridad

*Tabla 1 Integridad de la seguridad del hardware: restricciones arquitectónicas sobre subsistemas electrónicos complejos / programables relacionados con la seguridad (fuente: IEC61508-2 Tabla 3)*

## Por qué la Arquitectura de los Sistemas de Seguridad No Importa

La Integridad Sistemática (Systematic Integrity) es una evaluación cualitativa realizada por el organismo certificador que considera cómo los diseñadores de sistemas han interpretado y puesto en marcha las medidas para reducir las fallas sistemáticas durante la fase de diseño y dentro de la funcionalidad del sistema.

El estándar no intenta específicamente evaluar el tema de fallas de Modo Común, dejando esto a ser tratado en la Integridad de Seguridad Sistemática (Systematic Safety Integrity). Sin embargo, “Modo Común” es un problema con los sistemas que usan rutas redundantes idénticas para alcanzar un SIL más alto con un SFF más bajo; pero abundaremos en eso más adelante.

<sup>1</sup> Integridad de la seguridad es la probabilidad de que un sistema relacionado con la seguridad realice satisfactoriamente las funciones requeridas bajo todas las condiciones establecidas dentro de un periodo de tiempo establecido [1].

### 3. ¿Qué significa todo esto en la práctica?

El controlador SIL3 800xA HI (High Integrity) de ABB es una evolución del controlador SIL2 existente que ha sido exitosamente comercializado durante los últimos 3 años. El controlador SIL3 certificado tiene la misma estructura física que la versión SIL2 pero con un firmware y software mejorados. De igual forma que con la unidad SIL2, es un ejemplo de un sistema de seguridad diseñado desde su concepción específicamente para satisfacer los requisitos detallados del estándar IEC61508.

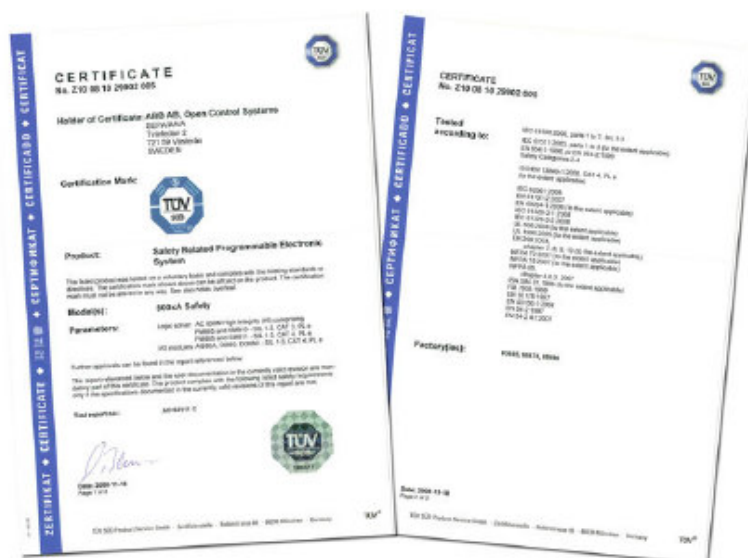


Figura 3 Certificado de Alta Integridad del 800xA

El controlador 800xA High Integrity puede ser configurado en diversas arquitecturas simples o redundantes, pero todas las combinaciones posibles de procesadores y E/S satisfacen exactamente los mismos criterios de integridad de la seguridad y todos satisfacen los requisitos de SIL3. La forma en que esto se logra en el diseño del producto se explicará más adelante, pero esto significa que los requisitos de disponibilidad (MTBF) pueden estar completamente separados de los requisitos de integridad de la seguridad definidos dentro del estándar. Duplicando el controlador de seguridad y/o los módulos de E/S aumenta la disponibilidad de esa parte del sistema dependiendo de las necesidades de la aplicación, pero en todos los caso la métrica de la integridad de seguridad continúa siendo la misma.

## Por qué la Arquitectura de los Sistemas de Seguridad No Importa

Si damos un vistazo al controlador SIL3 simple se orienta a los cuatro requisitos básicos del estándar de una forma muy directa:

- El PFD es una medida de la probabilidad de que el sistema falle de una manera peligrosa (no detectada). Los controladores 800xA SIL2 y SIL3 tienen esencialmente el mismo hardware. La electrónica básica está diseñada para los niveles más altos de confiabilidad. Utiliza integración de gran escala, componentes probados en campo y producción y métodos de prueba de clase mundial. Con base en cifras empíricas el PFD calculado para elementos de sistemas básicos se muestra en la tabla de abajo. Estas se encuentran justo en la parte superior de la banda de requisitos para los sistemas SIL3. Si analizamos las fallas reales del hardware a partir de los resultados (hay unos 3200 módulos en campo, muchos durante 2 años), esta cifra podría aumentar aún más. ¡Esta cifra se logra por el diseño fundamental más que por la duplicación y la votación! (el PFH de la Tabla siguiente es la probabilidad de falla peligrosa por hora).

Variante	Incluye	SFF %	$\lambda_{du}$	SIL2/SIL3	SIL2/SIL3
				PFD	PFH
<u>PM865 UP Sencillo</u> Módulo procesador Placa terminal Módulo de supervisión Placa terminal	1 x PM865 1 x TP830 1 x SM810/SM811 1 x TP855	99.55%	5.74E-09	SIL2 1.21E-5 SIL3 8.04E-6	SIL2 1.72E-10 SIL3 1.15E-10
<u>PM865 UP Redundante</u> Módulo procesador Placa terminal Unidad de interconexión CEX-Bus Placa terminal Módulo de supervisión Placa terminal	2 x PM865 2 x TP830 2 x BC810 2 x TP857 2 x SM810/SM811 2 x TP855	99.55 %	5.74E-09	SIL2 1.21E-5 SIL3 8.04E-6	SIL2 1.72E-10 SIL3 1.15E-10
<u>E/S</u> Módulo de entrada digital Unidad terminal de módulo (MTU)	1ch DI880 TU842/843	99.98 %	1.36E-10	9.52E-6	1.36E-10

*La Tabla 2 muestra los SFF, PFD y PFH para los componentes de 800xA HI*

- La Integridad de Seguridad Sistemática (Systematic Safety Integrity) del 800xA HI se logra principalmente por un programa exhaustivo de diseño, desarrollo y prueba por parte del diseñador del sistema con todos los procesos e hitos de diseño realizados dentro de un riguroso sistema FSMS (Functional Safety Management System) con certificación TÜV y con cada etapa del proceso de desarrollo de hardware y software escrutado y aprobado por un organismo independiente de certificación como TÜV. Uno puede argumentar que no importa qué tan buenos son los procesos, las fallas de diseño o sistemáticas no pueden ser eliminadas al 100%. Aquí es donde la “Diversidad Embebida” (“Embedded Diversity”) del 800xA HI (la cual se presenta más adelante en el texto) aparece y proporciona una verificación activa continua para las fallas operativas del software.
- La cifra SFF y el concepto de HFT son los parámetros interesantes y es aquí que 800xA HI desafía el análisis basado en la arquitectura convencional.
- El diseño fundamental asegura que todas las fallas detectadas se reportan y ya sea que deja al controlador operando en un modo degradado (pero aún seguro) o inicia una acción segura (paro).

#### 4. Un SFF alto indica un Diseño de Alta Integridad

El SFF (Safe Failure Fraction) de un subsistema se calcula como:

$$SFF = (\sum \lambda_s + \sum \lambda_{DD}) / (\sum \lambda_s + \sum \lambda_D)$$

Donde

$\sum \lambda_s$  es la probabilidad total de fallas seguras;

$\sum \lambda_D$  es la probabilidad total de fallas peligrosas; y

$\sum \lambda_{DD}$  es la probabilidad total de fallas peligrosas detectadas por las pruebas de diagnóstico.

Los tres tipos de falla están claramente definidos en el estándar de la manera siguiente:

- Falla Segura
  - El subsistema falló de manera segura si lleva a cabo la función de seguridad sin una demanda del proceso.
- Falla Peligrosa
  - El subsistema falló y se puso en peligro si no puede llevar a cabo su función de seguridad en demanda
- Falla Detectada
  - Una falla es detectada si el diagnóstico integrado revela la falla, para el 800xA High Integrity las fallas son reveladas en un tiempo entre 50mS y 1S.

Las fallas también pueden ser reveladas de tres formas:

- A través de la operación normal – (que usualmente resulta en un disparo falso)
- A través de exámenes periódicos de prueba – (podrían ser tan infrecuentes como cada 8 años para el 800xA HI)
- A través del diagnóstico integrado

El diseño único del sistema de diagnóstico del 800xA HI utiliza un alto grado de diagnóstico activo convencional (pruebas integradas) más verificación activa de discrepancias entre las dos distintas rutas de ejecución, dando al controlador simple un SFF de cerca de 100% (99.8% es la cifra citada). También, en virtud de la distinta estructura, el producto SIL3 tiene un HFT de 1 para el controlador simple y las E/S simples. A partir de la tabla anterior se puede ver que el 800xA HI satisface eficazmente los requisitos de PFD y SFF para SIL4, a pesar de estar sólo certificado para cumplir con SIL3. La razón de que esto se haya logrado es porque el controlador SIL2 está clasificado como que tiene un AFT de 0, pero aún así cumple con los requerimientos SIL3 para PFD. Sin embargo, el controlador SIL3, debido a su distinta tecnología embebida tiene un HFT de 1 lo cual mejora su integridad sistemática así como también proporciona un nivel de tolerancia de fallas.

¡Con frecuencia se argumenta que aumentando el SFF simplemente mueve los modos de falla peligrosa no detectada a la categoría de detectada, lo cual a su vez significa un incremento en los contratiempos falsos!

## Por qué la Arquitectura de los Sistemas de Seguridad No Importa

Por confianza en nuestro sistema de seguridad, ¡la única cosa que no queremos son modos de falla peligrosa no detectada! Éstos aumentan el potencial de fallas no detectadas a largo plazo e incluso en un sistema convencional dual o triple, una falla peligrosa no detectada, en el mejor de los casos degrada el sistema al hacer una ruta inoperable en demanda, y en el peor de los casos si la falla es común, podría dejar a todo el sistema en estado peligroso. Esto es especialmente cierto para TMR donde una simple falla no descubierta produce 2 de los 3 algoritmos de votación, de los que depende la integridad, ¡incapaz de trabajar!

El 800xA HI logra eficazmente el 100% de la cobertura de diagnóstico ya que no hay modos conocidos de falla peligrosa, y por lo tanto puede alcanzar el cumplimiento SIL3 sin recurrir a la carta del HFT. HFT se incluyó en el estándar, principalmente para posibilitar que los sistemas heredados, que dependían fuertemente de sistemas de redundancia o votación, satisficieran el nivel de requisitos SIL. Sin embargo, la definición de HFT en el estándar es muy específica y se aplica solamente en fallas no detectadas. Definitivamente no es una indicación de que el producto continuará funcionando después de que una falla se haya detectado, lo cual es lo que la mayoría de los usuarios esperan de un sistema tolerante de fallas.

¿Y qué hay acerca de los disparos falsos? Si un sistema de seguridad tiene una cobertura de 100% pero es propenso a la falla de componentes o de software, ¡entonces producirá un nivel inaceptable de disparos falsos!

Además de la alta cifra de PFD más el alto SFF, el controlador y E/S simples de 800xA HI tiene un nivel inherentemente alto de confiabilidad debido a los altos niveles de integración y la electrónica de baja intensidad y disipación. Esto da al controlador simple un MTBF que se acerca a los 20 años. (¡Está en la misma región que la última generación del sistema TMR!)

La estructura diversa embebida del controlador simple mejora además las estadísticas MTBF (tiempo medio entre fallas) permitiendo que el controlador SIL3 continúe funcionando de una manera degradada (pero certificada) durante un periodo limitado después de que se haya detectado una falla en el canal de E/S.

Sin embargo, si la disponibilidad del sistema es de enorme importancia, lo cual es el caso en muchas aplicaciones de petróleo, gas y petroquímica, el 800xA HI puede ser configurado de diversos modos duales redundantes, como se dijo anteriormente. Lo importante es que el sistema simple y los sistemas duales redundantes tienen exactamente el mismo PFD, exactamente el mismo SFF y ambos tienen un HFT de 1. Tienen exactamente la misma integridad de seguridad: lo único que cambia es el MTBF (disponibilidad) el cual puede aumentar en más de 400 años sobre un sistema simple similar.

Confiabilidad, integridad de seguridad y redundancia son términos que se ha confundido mucho en generaciones anteriores de sistemas, ahora están mucho mejor definidos y separando la confiabilidad de la integridad de la seguridad y la tolerancia a fallas del HFT, se debería hacer mucho más fácil las comparaciones del desempeño del sistema de seguridad bajo los nuevos estándares.

Aparte, es irónico que un sistema triple que dice tener altos niveles de cobertura de diagnóstico no gane nada en forma de integridad de la arquitectura triple. La votación 2oo3 no mejora la integridad de la seguridad y debido a que los canales son todos de la misma tecnología, no mejora la evaluación sistemática ni los problemas de modo común, y debido a las leyes de disminución de resultados, no mejora necesariamente la disponibilidad sobre una arquitectura dual redundante similar.

## 5. Votación y diagnóstico

La votación es el método más común usado para detectar discrepancias en los resultados de procesamiento de canales redundantes en sistemas de canales múltiples. La tabla 1 anterior que está tomada directamente de los estándares indica que los resultados de la votación pueden ser considerados un mecanismo para incrementar la cobertura de diagnóstico. Sin embargo, los autores de los estándares IEC61508 reconocieron que hay debilidades inherentes con los sistemas de votación cuando se intenta alcanzar altos niveles de integridad. Si el mecanismo de votación se vuelve indisponible debido a una falla no descubierta que se desarrolla en un canal, la integridad del sistema se pone en peligro, y lo que es peor ¡nadie lo sabe! Si una falla es detectada a partir de la votación, el sistema entra en un modo degradado y puede ver reducidas sus capacidades de integridad de seguridad. Aún más importante si la falla no es detectada, el estado degradado no es descubierto necesariamente hasta que se realiza una demanda en el sistema – cuando puede ser demasiado tarde.

También, los sistemas de votación simple con frecuencia sufren a partir de puntos sencillos de falla potencial en el sistema de votación mismo.

La disponibilidad solamente puede ser aumentada eficazmente si el sistema redundante puede continuar operando en el SIL especificado tanto en un estado totalmente redundante como en uno degradado. Como se dijo antes, el 800xA HI tiene exactamente la misma integridad de seguridad tanto en configuraciones simples como duales redundantes.

El estándar considera los siguientes tres tipos de falla del sistema:

- Fallas aleatorias del hardware
- Fallas sistemáticas – de diseño, de puesta en marcha u operativas
- Fallas de modo común

La probabilidad de fallas aleatorias del hardware que se presenten puede ser evaluada a partir de los datos de confiabilidad de componentes proporcionados por el fabricante y es probable que solamente afecte a un canal sencillo en un momento en un sistema redundante de canales múltiples. Sin embargo, las fallas sistemáticas y de modo común podrían afectar a todos los canales de un sistema de votación de canales múltiples exactamente de la misma forma. ¡Esto podría dar como resultado una falla completa del sistema!

Consecuentemente, los sistemas de votación con canales idénticos deben ser evitados si los efectos de los problemas sistemáticos y de modo común van a ser reducidos. Desde luego, la mayoría de los sistemas duales, triples y cuádruples dependen de la votación entre canales idénticos.

## 6 ¡Mejor diversidad que cantidad!

Los distintos sistemas de votación han estado presentes durante un largo tiempo. Los sistemas de seguridad usados para la energía nuclear utilizan la votación entre diferentes sistemas que utilizan con frecuencia diferentes tecnologías (relevadores, neumática, electrónica, etc.), proporcionados por diferentes compañías e instalados y puestos en servicio por diferentes equipos de trabajo. La probabilidad de fallas sistemáticas o de modo común que afectan a la integridad de todo el sistema se reduce por lo tanto de manera importante.

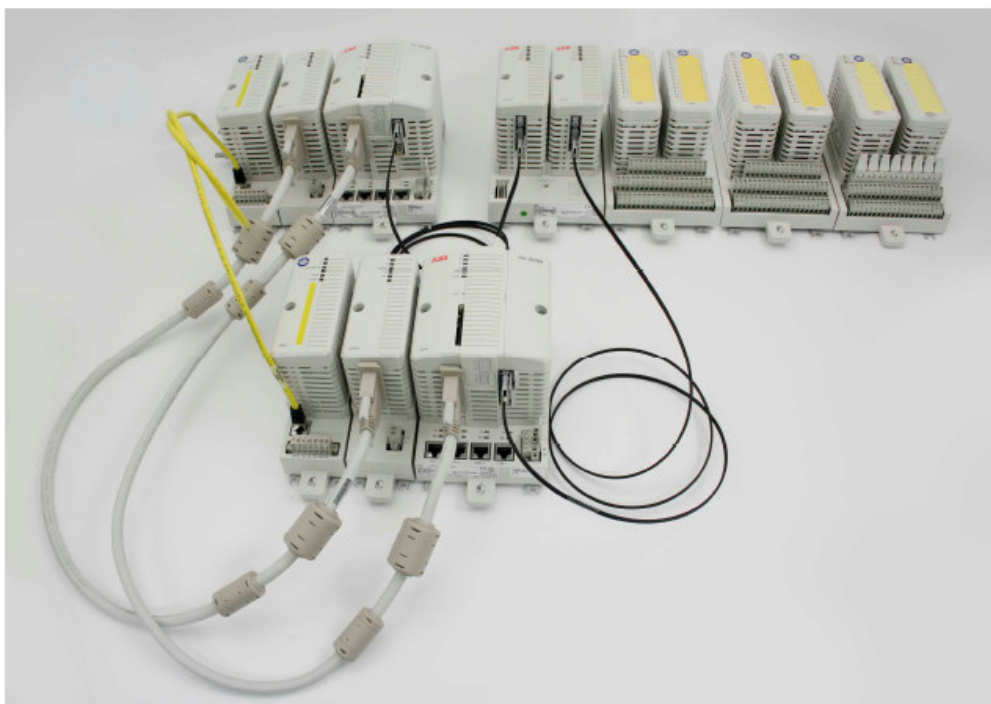
Las unidades de controlador simple y E/S de 800xA HI han incluido diversas rutas de procesamiento paralelo donde la verificación activa de discrepancia entre las rutas complementa el diagnóstico activo incluido. La diversidad del hardware incrustado en el hardware del controlador se logra por el uso de tarjetas diferentes del procesador para el controlador (PM865) y el módulo de supervisión (SM811). La diversidad en el software se logra por el uso de diferentes interpretaciones, compiladores, líneas de codificación y distintas mejoras programáticas del sistema operativo entre el controlador y el módulo de supervisión. Como una medida extra contra los problemas sistemáticos y de modo común, el controlador y el módulo de supervisión fueron desarrollados y probados por diferentes equipos de trabajo que operan en dos países distintos por personas con distintos antecedentes y experiencias. Los módulos de E/S también usan dos rutas de señal con distintas tecnologías incrustadas, una que utiliza tecnología FPGA y la otra que usa MCPU.

El 800xA HI no se ajusta a la arquitectura convencional 1oo2D y no puede describirse en tales términos. Si se considera necesario darle una etiqueta arquitectónica, la arquitectura de seguridad debería ser descrita como: -¡sí, adivinaron! **“Tecnología Diversa, Embebida”** (“Embedded, Diverse Technology”). Esta tecnología distinta se emplea en un formato **Dual** cuando se pone en funcionamiento en una configuración sencilla y un formato **Quad** cuando se pone en funcionamiento en una configuración redundante.



*Figura 4 El 800xA Alta Integridad en formato Dual con E/S sencillas*

## Por qué la Arquitectura de los Sistemas de Seguridad No Importa



*Figura 5 El 800xA Alta Integridad en formato Quad con E/S's redundantes*

Debido al diseño de los sistemas y a la forma en que se manejó el proceso de desarrollo, y debido al uso de tecnología de firewall que separa y protege diferentes aplicaciones que corren en un controlador sencillo, el 800xA HI es capaz de correr tanto aplicaciones SIL3 certificadas como de control de proceso básico en el mismo controlador ya sea en modo simple o dual redundante. Obviamente se debe hacer una consideración para el acceso, actualizaciones y modificación, que tienden a ser requisitos para aplicaciones de control y son un problema para los sistemas certificados de seguridad, pero la flexibilidad agregada que se logra, especialmente para pequeños programas de automatización, es extremadamente valiosa.

### **7. Votación Activa o Principal – Modo de Espera**

Una vez que se han separado los requisitos para integridad de los de disponibilidad, es mucho más fácil medir la eficacia de los diversos diseños.

Los componentes electrónicos de silicio son inherentemente muy confiables una vez que ha pasado la etapa de mortalidad infantil. La selección de los componentes y la producción realizada en pruebas garantizan que el 800xA HI, aun en modo simple, alcanza los niveles más altos de confiabilidad. Las evaluaciones empíricas (usadas en la formulación del SIL alcanzado) caen justo en lo alto de la banda SIL3 y los resultados de campo basados en más de 600 sistemas de seguridad entregados con más de 50,000 E/S en el campo en operación completa, indican que las cifras reales alcanzadas son un orden de magnitud mejor que éstos.

Con estos niveles de confiabilidad logrados con el producto en configuración simple, uno podría preguntarse por qué una oferta de dual redundante es necesaria en absoluto. Sin embargo, hay muchos procesos altamente cruciales o no preparados, donde el costo de tan sólo un contratiempo falso en un periodo de 20 años es infinitamente más costoso que la adición de un sistema redundante.

## Por qué la Arquitectura de los Sistemas de Seguridad No Importa

La estructura física del 800xA HI es única en cuanto a la posibilidad de que las E/S y controladores sean ofrecidos en modo redundante independientemente uno de otro, aumentando así la disponibilidad de las E/S y/o el controlador independientemente. Esto significa que para los procesos cruciales, que pueden mantenerse con la pérdida total de (digamos) un canal de E/S (dos fallas), solamente uno de los procesadores necesita duplicación. En la mayoría de los procesos sólo una pequeña proporción de las E/S es tan crucial que requiere una disponibilidad de 100%, consecuentemente pueden ser configurados sistemas E/S mixtos redundantes y no redundantes con un correspondiente ahorro de dinero.

La redundancia del 800xA HI se logra usando un enfoque de “hot-standby”, por ejemplo la configuración Quad. Un controlador realiza las funciones lógicas y de control mientras que el otro corre en paralelo manteniendo su operación en paso. Si ocurre una falla en el controlador principal, el controlador de respaldo toma el control de una manera sin sobresaltos dentro de un sólo ciclo de escaneo y la falla se reporta. Inversamente, si ocurre una falla en el esclavo, ésta es detectada y reportada. El SIL y el tiempo de reparación; la integridad total del sistema no se degrada en forma alguna debido a la falla en un lado del sistema. La estructura de conmutación “hot-standby” retiene todas las ventajas de correr sistemas de votación paralelos sin el potencial punto único de falla que un sistema de votación puede tener.

El aumento en disponibilidad que se obtiene entre el 99.995% de una aplicación sencilla, es decir, configuración dual, y el 99.995% del equivalente dual redundante, es decir configuración quad, puede no ser estadísticamente muy importante, pero si su proceso es probable que le coste millones de dólares en ingresos perdidos por tiempo de paro no programado, ¡es un pequeño precio a pagar para tener tranquilidad!

### 8. Olvídense de la Arquitectura – Vea el Conjunto de Datos Certificados

Ya no es importante si el sistema es dual, triple, quad, 1oo2, 2oo3 o 2oo4. De hecho, a menos que conozcamos exactamente para qué está diseñada la arquitectura, estos términos pueden ser por lo menos confusos, y en la última generación de sistemas las definiciones de “integridad” y “disponibilidad” eran definitivamente confusas. Los datos importantes que definen la integridad y disponibilidad de su sistema de seguridad estarán contenidos en el reporte de logros SIL que debe esperar de su integrador certificado de sistemas. Este reporte le dará la siguiente información:

- PFD calculada para la configuración de su sistema respaldada por datos y cálculos certificados de confiabilidad.
- La cifra de SFF (Safe Failure Fraction) para su sistema. Otra vez respaldada por datos y cálculos certificados de cobertura de diagnóstico.
- Certificados que confirmen la integridad sistemática del sistema básico que cubran el desarrollo de todos los subsistemas y elementos de seguridad relacionados. Véase el anexo para el 800xA HI.
- Certificados que cubran el FSMS (Functional Safety Management System) usado por el integrador del sistema en el que se confirma la competencia del equipo de proyectos y los procesos usados.
- Un reporte detallado del logro SIL que incluya los resultados del FSA (Functional Safety Assessment) llevado a cabo durante el proyecto y los reportes de auditoría realizados por el equipo.

Si cuenta con todos estos puntos, los cuales están a su disponibilidad en ABB, ¡entonces y sólo entonces estará satisfecho!