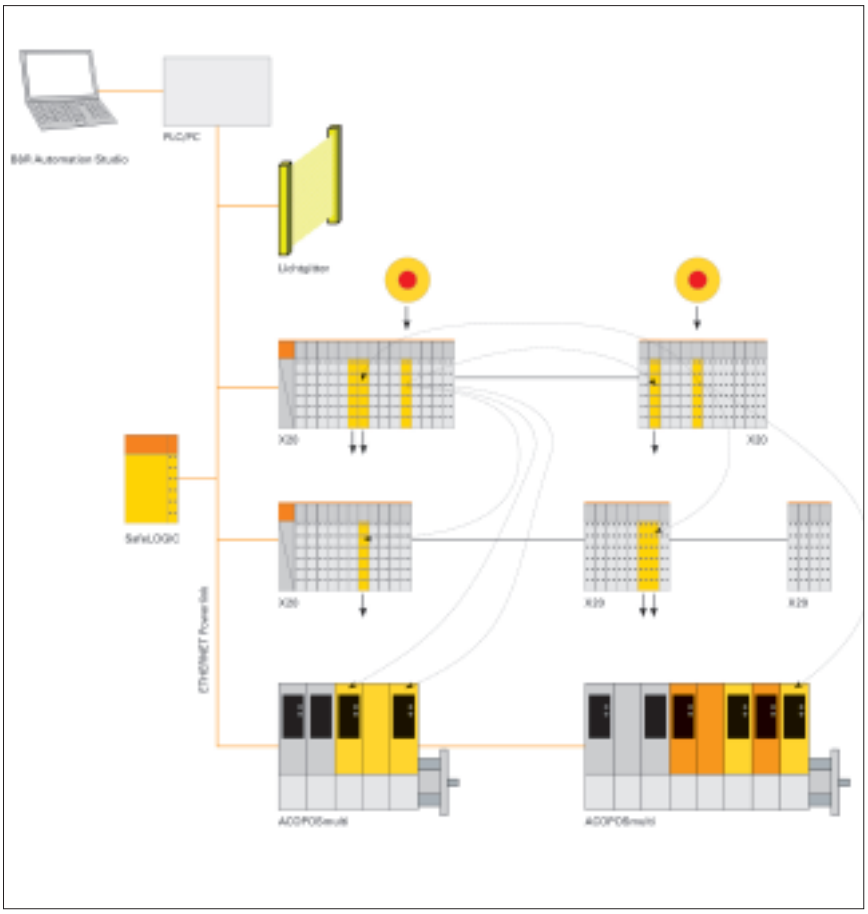
Ethernet Powerlink Safety (EPLsafety)

Una solución abierta para la seguridad funcional en tiempo real

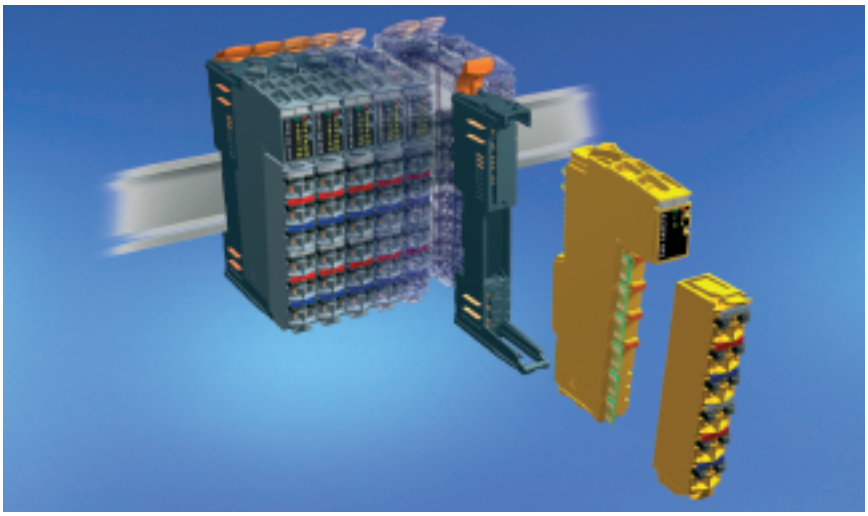
Las especificaciones para el protocolo de seguridad Ethernet Powerlink Safety (EPLsafety) fueron diseñadas por un grupo de trabajo independiente que pertenece al Grupo de Estandarización Ethernet Powerlink *(Ethernet Powerlink Standardization Group - EPSG)*. El desarrollo del protocolo se ha visto impulsado por los principales fabricantes de componentes de automatismos, así como por expertos en el campo de tecnología de seguridad.

El estándar de red Ethernet es ahora una parte integral de la automatización de máquinas y procesos de fabricación. Las ventajas de utilizar componentes, protocolos y herramientas estandarizadas proporcionan, además de una mayor apertura, continuidad y transparencia de los datos. Por este motivo, el uso de Ethernet en automatización se está convirtiendo en un requisito previo para obtener aplicaciones sencillas de ejecutar, fiables y rentables. La capacidad de actuar en tiempo real desempeña un papel fundamental en este ámbito. Los tiempos de reacción y una precisión de microsegundos son aspectos cada vez más importantes, y no sólo en la fabricación de maquinaria. Sin embargo, para hacer frente a los requisitos del futuro, además del rendimiento, existen otros factores importantes a la hora de elegir un sistema Ethernet en tiempo real, como son la integración de la seguridad funcional y el modo en que se ha llevado a cabo dicha integración.



Ejemplo de configuración en una planta con infraestructura de seguridad Ethernet Powerlink.

Las especificaciones para el protocolo de seguridad Ethernet Powerlink Safety (EPLsafety) fueron diseñadas por un grupo de trabajo independiente que pertenece al Grupo de Estandarización *Ethernet Powerlink (Ethernet Powerlink Standardization Group - EPSG)*. El desarrollo del protocolo se ha visto impulsado por los principales fabricantes de componentes de automatismos, así como por expertos en el campo de tecnología de seguridad. El principal objetivo era desarrollar un sistema totalmente abierto con el más alto rendimiento, conseguir una absoluta



La familia de E/S de *B&R* X20 integra módulos "gris" y "amarillos" en redes Ethernet Powerlink.

independencia con respecto a los protocolos de transporte no seguros y posibilitar un intercambio de datos transparente entre áreas seguras y no seguras.

Soluciones actuales

Hoy en día, la mayoría de las soluciones de seguridad se basan en un sistema de cableado fiable con dispositivos centrales de parada de emergencia, lo que refleja el hecho de que los controladores especiales de seguridad todavía resultan, en general, excesivamente costosos para maquinaria y sistemas de tamaño medio, pues carecen de flexibilidad y aumentan la complejidad y el coste del sistema de cableado. Además, en este caso el diagnóstico de errores resulta complicado y limitado.

Una segunda solución depende únicamente de un controlador de seguridad. Una vez separadas del entorno no seguro, todas las señales se transmiten a un controlador seguro bien directamente o a través de sistemas especiales de bus. Aquí también será preciso contar con un cableado fiable y seguro. El uso de componentes de infraestructura seguros, como conectores de bus, originará costes adicionales.

Los sistemas de seguridad modernos funcionan con un bus de campo estándar que se ha convertido en seguro mediante medidas especiales aplicadas para la transmisión de datos. Con esta solución, es posible distribuir con facilidad componentes remotos de entrada/salida seguros a lo largo del sistema. La función de controlador seguro es controlada localmente por un PLC también seguro. Si se combina una CPU para controlar la programación segura y la no segura, la transmisión de datos entre el entorno amarillo (seguro) y el gris (no seguro) (ver figura en página anterior) resulta relativamente sencilla, pero la escalabilidad del rendimiento del controlador queda enormemente limitada. Por este motivo, existen sistemas que ejecutan las secuencias de seguridad de sus programas en una unidad de control segura independiente. A la hora de seleccionar el sistema de bus de campo y el protocolo de seguridad estándar, resulta importante tener en cuenta el tiempo de ejecución de los datos seguros, de modo que pueda respetarse el tiempo de respuesta segura de la totalidad del sistema (ver figura en página anterior).

Redes seguras

¿De qué modo se convierte un sistema de bus en un sistema de bus para aplicaciones seguras? ¿Cuáles son las propiedades que lo distinguen de los sistemas de bus convencionales?

Los requisitos de seguridad se especifican en la norma IEC 61508-1, así como en las políticas de ensayos que maneja la HVBG (asociación que se ocupa de temas de seguridad en Austria y Alemania **www.hvbg.de**) para realizar pruebas y certificar "sistemas de bus para transmitir mensajes seguros". Para poder utilizarse en aplicaciones seguras, un sistema de bus debe estar preparado para cualquier error que pueda producirse durante la transmisión de datos e incluir mecanismos que puedan controlar el error y evitar que se produzcan situaciones potencialmente peligrosas. La probabilidad de que existan errores no descubiertos que podrían originar situaciones peligrosas no podrá superar los límites especificados en la norma. Para aplicaciones de fabricación de maquinaria en las que se aplique habitualmente el nivel de seguridad IEC 61508 SIL 3, este límite no podrá superar los 10^{-9} errores por hora. En otras palabras, sólo podrá producirse una situación de peligro debida a un error en el bus una vez cada 115,500 años, más o menos.

Para satisfacer estos exigentes requisitos, los sistemas de bus seguros cuentan con varios mecanismos diferentes para evitar que se produzcan los siguientes errores potenciales durante la transmisión de datos:

- Datos redundantes
- Pérdida de datos
- Datos introducidos
- Secuencias incorrectas de datos
- Corrupción de datos
- Excesivos retrasos en las transmisiones

Asimismo, una red debe ser capaz de soportar la totalidad del ciclo vital de la aplicación, a la vez que proporciona los servicios necesarios para un funcionamiento sin errores, intercambio de dispositivos, diagnósticos, configuraciones, etc.

Ethernet Powerlink Safety (EPLsafety)

Para que la tecnología de seguridad pueda integrarse en sistemas que utilizan varios sistemas de

ETHERNET POWERLINK safety technology

bus, es importante que el protocolo de seguridad no se desarrolle exclusivamente para una determinada red o sistema de bus. Para poder controlar esto, todas las medidas necesarias para evitar errores deberán estar totalmente aplicadas en la capa del protocolo de seguridad. Puede que no sea posible emplear propiedades o características especiales del protocolo de transporte subyacente para evitar posibles errores. La especificación de EPLsafety se tomó este asunto muy en serio desde un primer momento. Por este motivo, EPLsafety es totalmente independiente del protocolo de transporte y puede utilizarse para redes no basadas en Ethernet con un ancho de banda menor, como un bus CAN.

Para controlar la gestión de datos, EPLsafety utiliza un diccionario de objetos cuya estructura y formato utiliza los mecanismos presentes en el diccionario de objetos del CANopen. Esta propiedad es especialmente apreciada por los usuarios con experiencia en este bus.

Los servos de *B&R* ACOPOSMulti pueden trabajar en modalidad segura en una red Ethernet Powerlink.

Todo en un único bus

Los antiguos sistemas de bus de seguridad se aislaban y se estructuraban para intercambiar exclusivamente datos seguros. Estos sistemas de bus cuentan con un mayor número de adeptos, ya que esta arquitectura utiliza un ancho de banda reservado exclusivamente para los datos seguros. Estos paquetes de datos de máxima seguridad no podrán en ningún caso ser detenidos por otros paquetes de datos. En principio, esta argumentación es generalmente correcta y comprensible, pero pierde su validez cuando entran en juego sistemas Ethernet en tiempo real como Ethernet Powerlink. Este sistema reserva la cantidad exacta de ancho de banda de red necesario para cada estación. Asimismo, Ethernet Powerlink dispone de las siguientes características:

- Sincronización estricta, determinística
- Ciclos muy cortos de 200 µs o inferiores
- Baja fluctuación de red inferior a 1 µs
- Tiempos de respuesta seguros en "casos graves"

La especificación EPLsafety presta una especial atención al uso del protocolo en máquinas modulares. Existen servicios especiales para estos tipos de aplicaciones para permitir la puesta en marcha y los intercambios de hardware durante el funcionamiento en los sistemas en los que la seguridad resulta fundamental.

Tiempos de respuesta

Los tiempos de respuesta para los componentes con cableado discreto son siempre más cortos que los que están en red con sistemas de bus. Si un conmutador de parada de emergencia cuenta con un cableado discreto con relé de seguridad, la señal de desconexión se transmite de forma prácticamente instantánea, lo que permite que no resulte prioritario desde el punto de vista de seguridad. Cuando se utiliza una red, es preciso tener en cuenta los tiempos de ejecución en el bus tanto de la señal como del procesamiento.

Longitud de los datos de referencia por trama [bytes]	Probabilidad restante de error
1	$5{,}234\ 10^{20}$
8	$7{,}061\ 10^{20}$
249	$2{,}021\ 10^{19}$

Como ya se ha mencionado anteriormente, la norma IEC 61508 SIL 31) permite un máximo de 10^{-9} errores no detectados por hora. De una forma similar al principio del circuito cerrado con cableado discreto, un conmutador de parada de emergencia deberá transmitir datos sobre el bus de seguridad de forma constante hacia el respectivo relé de seguridad. Si se detiene la recepción de datos, el relé de seguridad reconoce un error y pasa automáticamente a un modo seguro. El intervalo entre dos paquetes de datos enviados desde el dispositivo de parada de emergencia se denomina *tiempo de refresco.* Si el tiempo de refresco es de 200 µs, sólo en una hora se llegan a intercambiar 18.000.000 mensajes de seguridad. Para alcanzar el límite de 10^{-9} errores no reconocidos por hora especificados en la norma, únicamente podrá darse un caso de datos corruptos no reconocidos en cada $1{,}8*10^{16}$ mensajes. Esto hace referencia a la probabilidad restante de error del protocolo, que en este caso deberá ser mejor que $1/(1{,}8*10^{16}) = 5{,}55*10^{-17}$. La probabilidad restante de error de un protocolo es el valor que determina el tiempo de refresco mínimo permitido en el sistema de bus de seguridad, y afecta de forma sustancial al tiempo de respuesta en casos graves de la aplicación.

Para hacer frente a esto, el forma-

to de datos de EPLsafety se ha dividido en dos subtramas. Se logra la seguridad de cada subtrama utilizando una suma de comprobación independiente (CRC), que se calcula de forma diferente. Este mecanismo permite a EPLsafety alcanzar los siguientes valores para la probabilidad restante de error.

Como muestran los datos de la tabla inferior, EPLsafety ni siquiera se aproxima a superar los límites establecidos por la norma IEC 61508. Por primera vez, es posible alcanzar tiempos de refresco de 100 µs o inferiores con un protocolo de seguridad.

Las configuraciones de Ethernet Powerlink disponibles en el mercado funcionan con tiempos de ciclo de aproximadamente 200 µs. Los dispositivos de prueba ya funcionan con tiempos de ciclo de 100 µs. La probabilidad restante de error extremadamente baja de EPLsafety ya está disponible para estos tiempos de ciclo tan reducidos, permitiendo su uso en redes Gigabit Ethernet en el futuro.

Como se ha mencionado anteriormente, un relé de seguridad pasa a un estado seguro si cesa la entrada de datos de máxima seguridad. Para evitar que la pérdida de un simple paquete provoque la caída del sistema, el tiempo de respuesta de este relé está configurado para que supere en más del doble el tiempo de refresco. Un tiempo de refresco de 200 µs origina un tiempo de respuesta en casos graves de alrededor de 500 µs. Cuando se calcula el tiempo de respuesta seguro en casos graves para toda la cadena del sistema, es preciso añadir los tiempos de filtrado de la señal de entrada a los tiempos de respuesta de los accionadores.

Con un tiempo de refresco probable de 200 µs, EPLsafety es con diferencia el protocolo más rápido para resolver tareas de seguridad.

¿Qué puede hacer EPLsafety por el usuario?

Los sistemas de bus de seguridad reducen la carga de trabajo del cableado y la probabilidad de errores, a la vez que mejoran la flexibilidad en la automatización de máquinas y procesos de fabricación. El problemático doble cableado que era necesario hasta ahora ya no es necesario. Los datos procedentes de los dispositivos de seguridad pueden analizarse directamente y de forma inmediata por el resto de dispositivos.

Con EPLsafety, el usuario dispone del primero y único protocolo de seguridad con capacidad en tiempo real para la automatización de máquinas y procesos de fabricación, así como de una solución para tareas que precisan de seguridad operativa. Los tiempos de respuesta obtenidos por EPLsafety son al menos diez veces mejores que los tiempos de respuesta de otros sistemas de bus de campo de seguridad.

Ethernet Powerlink es una red Ethernet industrial en tiempo real con más de 300 usuarios en todo el mundo. EPLsafety se apoya en estos sólidos cimientos y ofrece a los usuarios la máxima protección posible para sus inversiones. Los procesos de especificación y certificación realizados por el EPSG garantizan la interoperabilidad de productos de diferentes fabricantes. Los protocolos de Ethernet Powerlink no precisan de un hardware especial, ASIC, componentes de red o conmutadores. Ethernet Powerlink y EPLsafety no están patentados y están abiertos para todos los fabricantes y usuarios de productos interesados.

Franz Kaufleitner
Director de proyectos para productos de seguridad de B&R

Anton Meindl
Director comercial en el área de tecnología de controladores y bus de campo de B&R

www.br-automation.com
www.epsg.org

Referencias

- IEC 61508-1. *Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad.* Parte 1: Requisitos generales, Genf 1999.
- *Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), política para la realización de pruebas y certificación de sistemas de bus para la transferencia de mensajes de seguridad,* (GS - ET - 26), Edición 02/05.