(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 711 726**

(51) Int. CI.:

G06F 11/16 (2006.01)
G06F 11/14 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **22.02.2016 PCT/EP2016/053647**

(87) Fecha y número de publicación internacional: **15.09.2016 WO16142159**

(96) Fecha de presentación y número de la solicitud europea: **22.02.2016 E 16708372 (4)**

(97) Fecha y número de publicación de la concesión europea: **21.11.2018 EP 3245591**

(54) Título: **Sistema informático de seguridad de tipo relevante**

(30) Prioridad:

11.03.2015 DE 102015204337

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.05.2019

(73) Titular/es:

SIEMENS MOBILITY GMBH (100.0%)
Otto-Hahn-Ring 6
81739 München, DE

(72) Inventor/es:

HARSCH, WALDEMAR

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Sistema informático de seguridad de tipo relevante

Conforme a la reivindicación 1, la presente invención hace referencia a un sistema informático de seguridad de tipo relevante, particularmente un sistema de seguridad ferroviario, con al menos dos canales hardware; en donde los resultados de control de memoria de los canales son enviados al menos a un comparador, el cual da como salida una respuesta de error cuando los resultados de control de memoria no coinciden.

La siguiente descripción se refiere fundamentalmente a un sistema de seguridad ferroviario, sin que por ello la invención esté restringida a esta aplicación especial. Por el contrario, la invención puede ser utilizada para diferentes sistemas informáticos de seguridad de tipo relevante, por ejemplo para procesos de fabricación industrial o para vehículos de todo tipo.

Los sistemas de seguridad ferroviarios deben cumplir requisitos de técnica de seguridad muy altos; en donde cada vez más está preestablecido el nivel más alto de seguridad SIL 4. Los niveles de seguridad están definidos por la Norma CENELEC EN50129, que van desde SIL 0 (no seguro desde el punto de vista de la técnica de señalización) hasta SIL 4 (en alto grado seguro desde el punto de vista de la técnica de señalización). Entre los sistemas de seguridad de tipo relevante están incluidos aquí también subsistemas cuyo comportamiento de errores pueden ser considerados por separado. Por ejemplo, la activación de una señal luminosa individual en una vía férrea puede representar un sistema de seguridad de tipo relevante.

Al concepto de seguridad de sistemas informáticos, corresponde según la norma CENELEC EN50128 junto a la pluralidad de canales del hardware, también un control de memoria; en donde, o bien directamente el contenido almacenado, o sea el campo de códigos y datos relevante, inclusive las pilas, o bien las sumas de verificación formadas a partir de ello, conforman los resultados de control de memoria de los canales individuales, los cuales se comparan y ante una diferencia dan como salida una respuesta de error. La comparabilidad de los resultados de control de memoria supone que en todos los canales opera el mismo software. Para determinar con seguridad que efectivamente existe una igualdad de software, los correspondientes compiladores deben validar los canales individuales. La validación de un compilador nuevo implica tiempos y costes extremadamente considerables. A ello, se le suman costes anuales de mantenimiento durante el ciclo de innovación para nuevos compiladores. Hasta ahora, el uso de compiladores diversitarios no es posible porque los compiladores diversitarios generan diferentes diseños de memoria, de modo que los resultados de control de memoria de los canales no pueden ser comparados unos con otros.

El documento D1 = DE 10 2011 053 580 A1 revela un ordenador y una arquitectura funcional conforme a los cuales los valores de entrada se envían de manera paralela a una ruta de control, la cual contiene módulos funcionales de software individuales; y a una ruta de vigilancia, la cual está estructurada correspondientemente diversitaria. La ruta de vigilancia implementa un módulo funcional SW correspondientemente diversitario con respecto al módulo funcional SW original; en donde se utiliza un algoritmo diferente al de la ruta de control. Mediante un comparador de núcleos implementado en hardware, se comparan a nivel de procesador las diferencias de cálculo granulares de ambos núcleos. Si mediante el comparador de núcleos se establece alguna diferencia, entonces se produce una desconexión de sistema del sistema total.

Conforme a esto, la presente invención tiene por objeto sugerir un sistema informático de seguridad de tipo relevante, de la clase mencionada en la introducción, que posibilite el uso de compiladores diversitarios.

Conforme a la invención, el objeto se resuelve porque cada canal presenta al menos dos programas de software diversitarios creados por compiladores, cuyos resultados de control de memoria son enviados al comparador; en donde los resultados de control de memoria del primer programa de software del primer y del segundo canal se comparan entre sí; y los resultados de control de memoria del segundo programa de software del primer y del segundo canal se comparan entre sí.

De esta manera, se generan resultados de control de memoria comparables en al menos dos canales del sistema informático de seguridad de tipo relevante, también en el uso de programas de software diversitarios creados por al menos dos compiladores. Se suprimen los tiempos y los costos de validación para asegurar que los programas de software son idénticos. En el caso de un sistema de dos canales, están proporcionados por ejemplo dos programas de software creados por compiladores diversitarios, cuyos resultados de control de memoria se comparan cuasi transversalmente entre sí. En este caso, los resultados de control de memoria del primer programa de software que opera en el primer canal se comparan con los resultados de control de memoria del primer programa de software que opera en el segundo canal; y los resultados de control de memoria del segundo programa de software que opera en el primer canal se comparan con los resultados de control de memoria del segundo programa de software que opera en el segundo canal.

Conforme a la reivindicación 2, está previsto que cada canal y cada programa de software presenten precisamente un módulo de salida común; en donde los módulos de salida común de todos los canales estén conectados con un comparador de salida. Esto significa que el primer canal emite sólo los datos traducidos por el primer compilador, y el segundo canal emite sólo los datos traducidos con el segundo compilador. Los datos en el primer canal, traducidos por el segundo compilador, y los datos en el segundo canal, traducidos por el primer compilador están conectados con un pequeño módulo de salida. Por el contrario, estos datos se suprimen con una función vacía (dummy), de modo que está garantizado que no es posible generar una información de salida con un único canal que pudiera ser interpretada de manera fiable como una técnica de señalización. Los módulos de salida, por su parte, no tienen que ser controlados por separado, ya que dichos módulos sólo tienen una función de salida y no generan datos de seguridad de tipo relevante, cuya alteración podría tener peligrosas repercusiones.

A continuación, la presente invención se explica en detalle mediante un ejemplo de ejecución representado figurativamente.

La figura muestra esquemáticamente los componentes más importantes de un sistema informático de seguridad de tipo relevante.

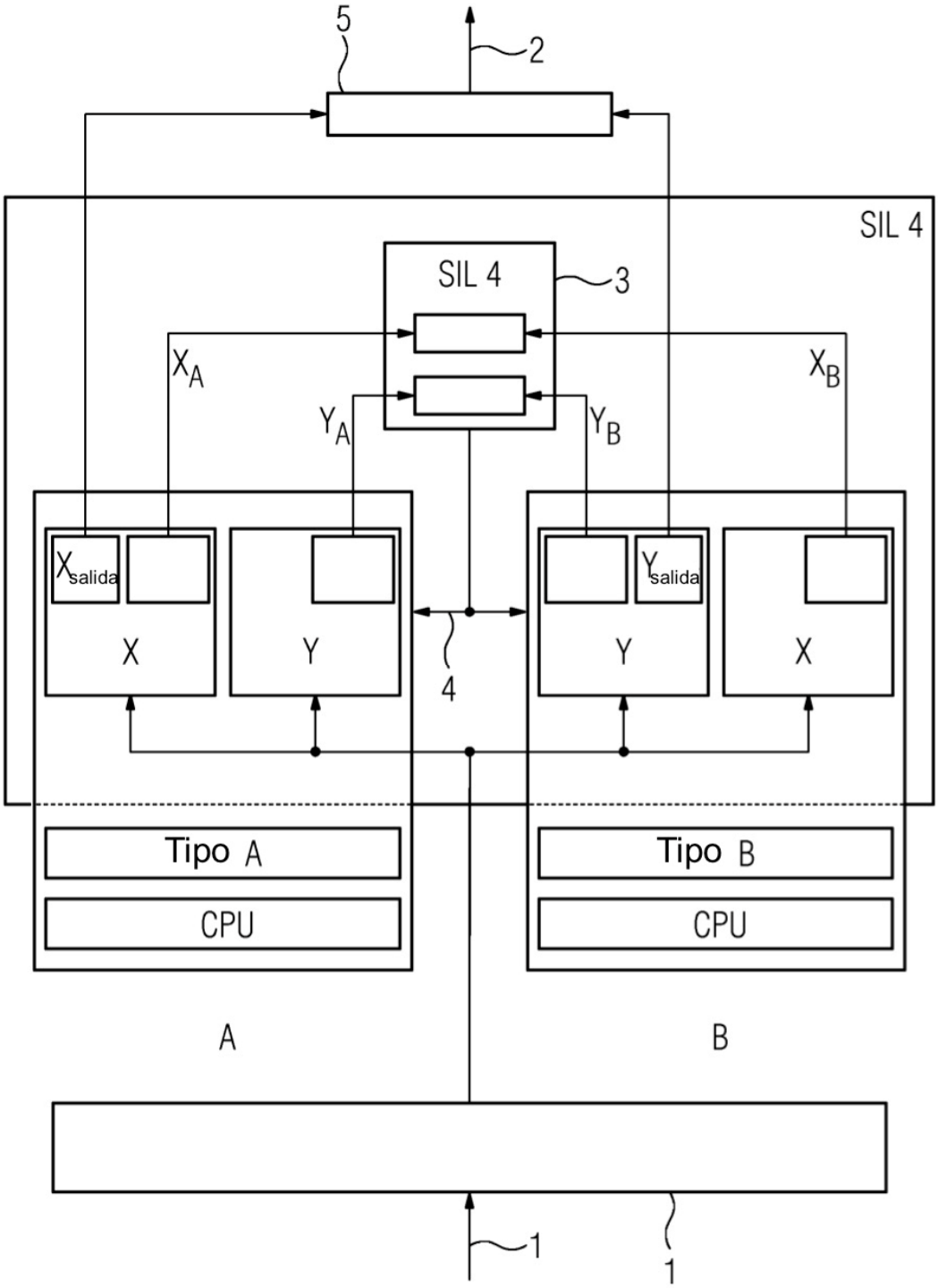
Está representado un sistema informático con dos canales A y B, los cuales presentan respectivamente una unidad central de procesamiento CPU y un sistema operativo Tipo A, o bien Tipo B. Ambos canales A y B procesan los mismos datos de entrada 1 y frente a un procesamiento de datos sin errores, los compilan en datos de salida 2 idénticos. En el caso de los datos de entrada 1 se puede tratar por ejemplo del estado de elemento de elementos de campo, como agujas, señales, pasos a nivel etc. de un sistema de seguridad ferroviario, los cuales se compilan en ambos canales A y B en datos de salida 2 para indicar los estados de elemento en un monitor con seguridad desde el punto de vista de la técnica e señalización, o sea SIL 4. Para ello, cada canal A y B están provistos de programas de software diversitarios, los cuales se crean por un compilador X y por un segundo compilador Y. Los compiladores X e Y generan resultados de control de memoria X_A, Y_A y Y_B, X_B en los dos canales A y B. Los resultados de control de memoria X_A, Y_A, Y_B, y X_B, por ejemplo sumas de verificación, se envían a un comparador SIL 4 3. El mismo realiza una comparación de los resultados de control de memoria X_A y X_B con respecto al primer programa de software del compilador 1; y una comparación de los resultados de control de memoria YA y YB con respecto al segundo programa de software del compilador Y. Ante una diferencia de los datos de control de memoria X_A y X_B con respecto al primer programa de software, creado por el compilador X, y/o de los datos de control de memoria Y_A y Y_B con respecto al segundo programa de software, creado por el compilador Y, se presenta un error de procesamiento de datos en el primer canal A y/o en el segundo canal B, de modo que el comparador 3 genera, a través de una reacción en ambos canales A y B, una respuesta de error 4 del sistema informático de seguridad de tipo relevante, preferentemente una desconexión segura desde el punto de vista de la técnica de señalización. Si el comparador 3 detecta un procesamiento de datos sin error en ambos canales A y B, entonces un módulo de salida X_{SALIDA} del primer programa de software, generado mediante el compilador X, del primer canal A y un módulo de salida Y_{SALIDA} del segundo programa de software, generado mediante el compilador y, del segundo canal B generan respectivamente informaciones de salida, las cuales son enviadas a un comparador de salida 5 y ante una coincidencia forman los datos de salida. Los otros dos programas de software, o sea el del segundo compilador Y en el primer canal A y el del primer compilador X en el segundo canal B, no generan datos de salida, sino que sirven solamente para la comparación de los resultados de control de memoria Y_A y X_B con los resultados de control de memoria X_A y Y_B generados respectivamente por el otro canal B y A. De esta manera, se presenta la posibilidad de utilizar programas de software diversitarios en compiladores X y Y, por lo cual se puede suprimir una validación de compilador extremadamente costosa.

REIVINDICACIONES

1. Sistema informático de seguridad de tipo relevante, particularmente un sistema de seguridad ferroviario, con al menos dos canales hardware (A; B), en donde los resultados de control de memoria de los canales (A; B) son enviados al menos a un comparador (3), el cual da como salida una respuesta de error (4) cuando los resultados de control de memoria no coinciden;

caracterizado porque cada canal (A; B) presenta al menos dos programas de software diversitarios creados por compiladores (X, Y), cuyos resultados de control de memoria (X_A, Y_A; Y_B, X_B) son enviados al comparador (3); en donde los resultados de control de memoria (X_A; X_B) del primer programa de software del primer y del segundo canal (A; B) se comparan entre sí y los resultados de control de memoria (Y_A; Y_B) del segundo programa de software del primer y del segundo canal (A; B) se comparan entre sí.

2. Sistema informático de seguridad de tipo relevante según la reivindicación 1, caracterizado porque cada canal (A; B) y cada programa de software presentan precisamente un módulo de salida (X_{SALIDA}; Y_{SALIDA}) común; en donde los módulos de salida común (X_{SALIDA}; Y_{SALIDA}) de todos los canales (A; B) están conectados con un comparador de salida (5).


5
2
SIL 4
SIL 4
3
X_A
X_B
Y_A
Y_B
X_{salida}
Y_{salida}
X
Y
4
Y
X
Tipo A
CPU
Tipo B
CPU
A
B
1
1