(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 392 749**

(51) Int. CI.:

G05B 9/03 (2006.01)
G05B 19/042 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **09700767 .8**
(96) Fecha de presentación: **08.01.2009**
(97) Número de publicación de la solicitud: **2229609**
(97) Fecha de publicación de la solicitud: **22.09.2010**

(54) Título: **Sistema de ordenador para la evaluación de magnitudes de sensor críticas para la seguridad**

(30) Prioridad:

08.01.2008 DE 102008003515

(45) Fecha de publicación de la mención BOPI:

13.12.2012

(45) Fecha de la publicación del folleto de la patente:

13.12.2012

(73) Titular/es:

LEOPOLD KOSTAL GMBH & CO. KG (100.0%)
AN DER BELLMEREI 10
58513 LUDENSCHEID, DE

(72) Inventor/es:

EDEL, JAN

(74) Agente/Representante:

SUGRAÑES MOLINÉ, Pedro

DESCRIPCIÓN

Sistema de ordenador para la evaluación de magnitudes de sensor críticas para la seguridad

La invención se refiere a un sistema de ordenador para la evaluación de magnitudes de sensor críticas para la seguridad según el preámbulo de la reivindicación 1 ó 2.

La IEC 61508 es una norma internacional para la creación de sistemas eléctricos, electrónicos y electrónicos programables, que ejecutan una función de seguridad. La publica la Comisión Electrotécnica Internacional (*International Electrotechnical Commission* (IEC)). La IEC 61508 establece para el nivel de integración de seguridad 3 determinados valores mínimos de hardware, por ejemplo para FIT (*failure in time*, fallo en el tiempo) y SFF (*safe failure fraction*, fracción de fallo seguro) que por regla general sólo pueden conseguirse mediante medidas de software adicionales. En particular la prueba para el aseguramiento frente a errores de cálculo de la CPU constituye una parte importante de la prueba total de la integridad de seguridad.

Hasta ahora se utilizan dos chips de microcontrolador diferentes o al menos dos trayectorias de cálculo que discurren en paralelo en un chip para el aseguramiento frente a errores de cálculo. A veces se emplean también trayectorias de cálculo que discurren de manera invertida, que se describen por ejemplo en la publicación alemana para información de solicitud de patente DE 42 19 457 A1. Una solución con dos chips resulta cara en el campo de la producción en masa y mediante las soluciones anteriores la seguridad funcional en un chip sólo pudo comprobarse de forma limitada o sólo con hardware adicional, ya que la CPU en caso de errores internos en las trayectorias de cálculo que discurren de forma paralela o invertida calcula igual de incorrectamente. Por tanto, dado el caso errores de CPU pueden quedar sin descubrir. Falta la prueba simple de que la CPU no haya calculado de la misma forma incorrecta en ambas trayectorias de cálculo y que para la comparación de los resultados están presentes dos resultados idénticos pero incorrectos o que en caso de trayectorias de cálculo invertidas la CPU por ejemplo omite ambas trayectorias de cálculo por error y se comparan directamente dos magnitudes de entrada.

El objetivo de la invención es crear un sistema de ordenador para la evaluación de magnitudes de sensor críticas para la seguridad que consiga de forma demostrable una integridad de seguridad especialmente elevada de la CPU sin depender de una prueba CPU laboriosa separada.

Este objetivo se soluciona según la invención en cada caso mediante las características identificadoras de la reivindicación 1 y de la reivindicación 2.

Según la invención está previsto que al sistema de ordenador pertenezcan al menos dos sensores que en un estado de sistema que va a detectarse emitan magnitudes de sensor diferentes en cuanto a la calidad o al menos en cuanto a la cantidad. Se supone que existe una relación funcional conocida entre las magnitudes de salida de ambos sensores.

La magnitud de sensor de un primer sensor está presente en una entrada de un ordenador que a partir de la misma calcula una magnitud de salida que está disponible para fines de uso práctico, por ejemplo como magnitud de control para un elemento de ajuste. A partir de esta magnitud de salida se calcula en un paso adicional una magnitud de comparación que corresponde a la magnitud de sensor esperada del segundo sensor. Esta magnitud de comparación se transmite del ordenador a un comparador externo que compara la magnitud de comparación con la magnitud de sensor real del segundo sensor totalmente desconocida para el ordenador para comprobar una posible coincidencia. Un resultado de comparación positivo es a este respecto un signo de la integridad de seguridad de la CPU y de un correcto proceso de cálculo de la magnitud de salida y de la magnitud de comparación. Al mismo tiempo se mantiene la prueba conocida por el estado de la técnica con respecto a la correcta función de sensores implicados que en principio se proporciona por un comparador.

La idea en que se basa la invención es por tanto recurrir a sensores diferentes en cuanto a la calidad o también sólo en cuanto a la cantidad que proporcionen diferentes magnitudes de medición o al menos diferentes valores y de este modo producen en cualquier momento diferentes niveles de datos durante el procesamiento, y concretamente de forma independiente del algoritmo utilizado (paralelo/invertido/inverso/complementario/de cálculo retroactivo).

En ningún momento la CPU es capaz de ofrecer la magnitud de comparación de otra forma (por ejemplo mediante copia de la primera magnitud de sensor) que no sea mediante el resultado de un cálculo que se ha realizado correctamente. Para demostrar la integridad de seguridad de CPU ahora tiene una importancia fundamental una comparación de la magnitud de comparación y de la segunda magnitud de sensor. Se comparan (dado el caso en una banda de tolerancia que compensa las posibles desviaciones como por ejemplo imprecisiones de sensor) la magnitud de comparación y el valor de una fuente de datos independiente adicional desconocido hasta ahora para el sistema de ordenador. Este valor se da por la segunda magnitud de sensor.

Dado que la segunda magnitud de sensor sólo está presente en estado crudo, esto es, de forma que no ha sido tratada por la CPU y absolutamente sin procesar, la comparación proporciona en este punto un resultado que depende únicamente de la integridad de CPU del sistema de ordenador (chip). Se supone en este caso la ausencia de errores de los dos sensores, o de sus propias CPU, que sólo puede asegurarse y comprobarse mediante medidas independientes.

Configuraciones y perfeccionamientos ventajosos de la invención se deducen de las reivindicaciones dependientes y de la descripción a continuación de un ejemplo de realización mediante el dibujo. Muestran

las figuras 1 y 2 en cada caso un ejemplo de realización de un sistema de ordenador según la invención,

las figuras 3 y 4 en cada caso un ejemplo de realización de un sistema de ordenador según el estado de la técnica,

la figura 5 un ejemplo de aplicación para un sistema de ordenador.

La figura 3 muestra un sistema de ordenador según el estado de la técnica. Se representa en este caso una representación muy simplificada del sistema de ordenador descrito en la figura 3 de la publicación alemana para información de solicitud de patente DE 42 19 457 A1. A este respecto se representan sólo los componentes necesarios para explicar el problema que lleva a la invención.

En la figura 3 se puede distinguir un elemento de cálculo de un sólo chip, esto es, un microordenador o microcontrolador, que a continuación se denomina abreviadamente ordenador MC. El ordenador MC recibe las magnitudes de sensor (e, e_R) desde dos sensores (S1, S2). Se supone que en este caso las magnitudes de sensor (e, e_R) son valores digitales, pudiendo, no obstante, proporcionar los sensores (S1, S2) en principio también señales analógicas que se digitalizan dentro del ordenador MC.

A partir de la magnitud de sensor e del primer sensor S1 el ordenador MC calcula mediante una función f1 una magnitud de salida a que se emite en una salida del ordenador MC, y que puede utilizarse por ejemplo para el control de un elemento de ajuste no representado. En un paso adicional el ordenador MC calcula mediante una función f2 a partir de la magnitud de salida a una magnitud de comparación e'. Dado que el documento DE 42 19 457 A1 describe la función f2 como la función $\overline{f1}$ invertida con respecto a la primera magnitud de entrada e con respecto a la primera función f1, se da, en caso de una correcta función del ordenador MC, una magnitud de comparación e' que coincide con la magnitud de entrada original e del primer sensor S1.

Esto puede comprobarse en el interior del ordenador mediante la comparación (e = e' ?) de las magnitudes e y e'. Además se propone una comprobación de las magnitudes de sensor primera y segunda con respecto a una posible coincidencia (e = e_R ?). Se supone por tanto que los sensores (S1, S2) denominados redundantes emiten magnitudes de sensor (e, e_R) de la misma cantidad.

Dado que un ordenador MC que no funciona correctamente en principio también puede proporcionar comparaciones incorrectas está previsto además un comparador V externo con respecto al ordenador MC. Este comparador V compara la magnitud de sensor e_R del segundo sensor S2 con la magnitud de comparación e' calculada. Debido a las identidades supuestas anteriormente (e = e_R y e = e') también esta comparación debe confirmar la identidad de las magnitudes comparadas (e', e_R) con los sensores (S1, S2) funcionando correctamente y un ordenador MC que trabaja sin errores.

Es problemático a este respecto que puedan quedar sin descubrir determinados errores del sistema de ordenador. Tal como indica de manera esquemática la figura 4 se da un problema si la primera magnitud de sensor e llega como magnitud de comparación e' supuestamente calculada a la salida del ordenador MC, sin que se haya realizado un cálculo. Esto puede ocurrir por ejemplo porque la primera magnitud de sensor e se introduce por lectura en un registro del ordenador MC, y se extrae por lectura de este registro en un momento posterior como magnitud de comparación e' supuestamente calculada y se proporciona a la salida del ordenador MC, sin que realmente haya tenido lugar un cálculo mediante las funciones f1 y f2.

Dado que las dos magnitudes de sensor e y e_R ya están previstas de manera idéntica en el lado de entrada, por tanto la comparación de e' y e_R realizada por el comparador V proporciona ahora también una coincidencia. Por tanto el comparador V no es capaz de descubrir el error de cálculo descrito.

Otro escenario de error se da porque el ordenador MC comete un error tanto en el cálculo de la función f1 como en el cálculo de la función f2, respectivamente, y estos errores se anulan mutuamente. Tampoco en este caso pueden detectar el error presente ni las comparaciones en el interior del ordenador ni las comparaciones en el exterior del ordenador.

Como ejemplo de ello se indica un error de signo que aparece sistemáticamente que tras dos operaciones de cálculo erróneas vuelve a anularse. Sin embargo, a este respecto la magnitud de salida a calculada mediante la primera operación de cálculo sigue siendo errónea, lo que puede tener efectos críticos para la seguridad.

Estas posibilidades de error se excluyen mediante el sistema de ordenador según la invención, tal como se explicará a continuación mediante la figura 1. Para aclarar los puntos en común y las diferencias con respecto al estado de la técnica anteriormente descrito se mantuvieron en parte las denominaciones de las figuras 3 y 4.

Es importante en primer lugar que si bien los sensores (S1, S2) emiten magnitudes de sensor redundantes (e_1, e_2), es decir, señales independientes que con respecto al estado de sistema que va a detectarse presentan un contenido de información del mismo tipo, sus valores de señal no son en ningún caso idénticos. Las magnitudes de sensor (e_1, e_2) de los sensores S1 y S2 se encuentran en una relación funcional conocida que se da mediante una función g. Esta función g puede ser casi cualquiera, sin embargo no debe ser la función de identidad, ya que esto a su vez llevaría a los problemas ya descritos.

Además la segunda magnitud de sensor e_2 sólo está prevista para una comparación externa y por tanto no se proporciona al ordenador MC.

Un tercer requisito es que la función f2 para el cálculo de la magnitud de comparación v no se da mediante la función inversa con respecto a la primera función f1, sino tiene en cuenta la relación funcional g entre la primera y la segunda magnitud de sensor (e_1, e_2). La función f2 se da a este respecto de manera ventajosa como concatenación de la función $\overline{f1}$ inversa a la función f1 con la función g:

$$v = f2\ (a) = (g \circ \overline{f1})\ (a)$$

En caso de que el cálculo se produzca de forma correcta el valor v presente en la salida coincide con el segundo valor de sensor e_2, lo que se comprueba mediante el comparador V ($v = e_2$?).

Los escenarios de error descritos anteriormente se excluyen en este caso, ya que la segunda magnitud de sensor e_2 no está presente en ningún punto del cálculo como valor de entrada, y por tanto sólo puede producirse como resultado de un cálculo que se ha producido correctamente.

La relación funcional g entre las magnitudes de sensor (e_1, e_2) de los dos sensores (S1, S2) puede darse en el caso más sencillo mediante una constante aditiva K:

$$e_2 = e_1 + K$$

Así puede estar previsto por ejemplo que en caso de sensores de ángulo el segundo sensor S2 presente un descentramiento de ángulo constante con respecto al primer sensor S1.

De manera alternativa puede estar previsto también que la segunda magnitud de sensor e_2 sea un múltiplo k de la primera magnitud de sensor e_1:

$$e_2 = k\ e_1$$

Evidentemente puede existir también una relación mucho más compleja entre las magnitudes de sensor (e_1, e_2). En particular pueden estar previstos también dos sensores que determinan las magnitudes de sensor según diferentes principios de medición físicos, de modo que se da desde el principio una relación más o menos compleja entre las magnitudes de sensor (e_1, e_2).

En la figura 5 se representa un sistema de sensores para la detección de un ángulo de giro, en el que puede aplicarse de manera ventajosa el sistema de ordenador propuesto. Una rueda de accionamiento 1, cuyo ángulo de giro debe determinarse, acciona en este caso dos ruedas de medición (2, 3) con diferentes radios. Con cada una de las ruedas de medición (2, 3) está conectado un imán (4, 5) que puede girarse junto con la respectiva rueda de

medición (2, 3) con respecto a un sensor Hall (6, 7) dispuesto de manera estacionaria. Los ángulos de giro detectados por los dos sensores Hall (6, 7) se diferencian por tanto en un factor constante, que se da a partir de las diferentes relaciones de transmisión de las dos ruedas de transmisión (2, 3) con respecto a la rueda de accionamiento 1.

La figura 2 indica de manera esquemática un perfeccionamiento ventajoso del sistema de ordenador representado en la figura 1. En el sistema de ordenador según la figura 1 se supone que se da la integridad de seguridad del verdadero comparador V al final de la cadena de procesamiento o debe aportarse la prueba estandarizada de ello por separado.

Se supone que la relación funcional entre las magnitudes de sensor primera y segunda (e_1, e_2) puede representarse mediante una concatenación de dos funciones h y g, de modo que es válido:

$$e_2 = (h \circ g)\ (e_1)$$

Dentro del ordenador MC se realiza el cálculo ya descrito mediante la figura 1 que en este caso lleva a la primera magnitud de comparación

$$v_1 = f2(a) = (g \circ \overline{f1})\ (a)$$

Sin embargo, dado que la relación funcional entre la primera y la segunda magnitud de sensor (e_1, e_2) en este caso ya no se da mediante g sino mediante la concatenación h○ g, la primera magnitud de comparación v_1, que llega al comparador V, no es adecuada para compararse con la segunda magnitud de sensor e_2.

El comparador V calcula por tanto mediante la función h a partir de la primera magnitud de comparación v_1 a través de la relación

$$v_2 = h(v_1)$$

una segunda magnitud de comparación v_2 que debido a las relaciones

$$= h \circ (g \circ \overline{f1})\ (a)$$
$$= (h \circ g) \circ \overline{f1}\ (a)$$
$$= (h \circ g)\ (e_1)$$
$$= e_2$$

en caso de un funcionamiento correcto del ordenador MC y del comparador V debe coincidir con la segunda magnitud de sensor e_2.

A partir de un resultado de comparación positivo puede concluirse por tanto que tanto el ordenador MC como el comparador V realizan cálculos correctos. De este modo esta variante de realización permite una comprobación de función simultánea tanto del ordenador MC como de las trayectorias de cálculo del comparador V.

Símbolos de referencia

MC	ordenador (microcontrolador)
S1, S2	sensores
V	comparador
A	magnitud de salida
e, e_R, e_1, e_2	magnitudes de sensor
e’	magnitud de comparación
f1, f2, g, h	funciones
$f1$	función inversa (con respecto a la función f1)
v	magnitud de comparación
v_1	primera magnitud de comparación
v_2	segunda magnitud de comparación
K	constante aditiva
k	factor constante
1	rueda de accionamiento
2, 3	ruedas de medición
4, 5	imanes
6, 7	sensores Hall

REIVINDICACIONES

1. Sistema de ordenador para la evaluación de magnitudes de sensor críticas para la seguridad, con al menos un primer sensor (S1), que emite una primera magnitud de sensor (e, e_1), y con un segundo sensor (S2), que emite una segunda magnitud de sensor (e_R, e_2), con un ordenador (MC), y con un comparador (V) independiente del ordenador (MC),
mediante el que el ordenador (MC) calcula a partir de la primera magnitud de sensor (e, e_1) mediante una primera función (f1) una magnitud de salida (a),
mediante el que el ordenador calcula a partir de la magnitud de salida (a) mediante una segunda función (f2) una magnitud de comparación (e', v, v_1),
y mediante el que la magnitud de comparación (e', v, v_1) y la segunda magnitud de sensor (e_R, e_2), están presentes en la entrada del comparador (V),
caracterizado porque
la segunda magnitud de sensor (e_2) no es una magnitud de entrada del ordenador (MC),
porque la segunda magnitud de sensor (e_2) y la primera magnitud de sensor (e_1) se encuentran en una relación dada por una tercera función (g) ($e_2=g(e_1)$), no siendo la tercera función (g) la función de identidad,
porque la segunda función (f2) se da mediante una concatenación de la tercera función (g) con la primera función ($\overline{f1}$) invertida (f2 = g O $\overline{f1}$),
y porque el comparador (V) compara la magnitud de comparación (v) con la segunda magnitud de sensor (e_2).

2. Sistema de ordenador para la evaluación de magnitudes de sensor críticas para la seguridad, con al menos un primer sensor (S1), que emite una primera magnitud de sensor (e, e_1), y con un segundo sensor (S2), que emite una segunda magnitud de sensor (e_R, e_2), con un ordenador (MC), y con un comparador (V) independiente del ordenador (MC),
mediante el que el ordenador (MC) calcula a partir de la primera magnitud de sensor (e, $e_{1)}$ mediante una primera función (f1) una magnitud de salida (a),
mediante el que el ordenador calcula a partir de la magnitud de salida (a) mediante una segunda función (f2) una magnitud de comparación (e', v, v_1),
y mediante el que la magnitud de comparación (e', v, v_1) y la segunda magnitud de sensor (e_R, e_2) están presentes en la entrada del comparador (V),
caracterizado porque
la segunda magnitud de sensor (e_2) no es una magnitud de entrada del ordenador (MC),
porque la relación entre la segunda magnitud de sensor (e_2) y la primera magnitud de sensor (e_1) puede representarse mediante dos funciones concatenadas entre sí (h O g), no dándose mediante la función de identidad ninguna de las funciones concatenadas entre sí (h, g) y tampoco la relación (h O g) representada mediante la concatenación entre las magnitudes de sensor (e_1, e_2),
porque el ordenador (MC) utiliza una de las funciones concatenadas (g) para calcular una primera magnitud de comparación (v_1),
y porque el comparador (V) calcula a partir de la primera magnitud de comparación (v_1) mediante la otra de las funciones concatenadas entre sí (h) una segunda magnitud de comparación (v_2), y la utiliza para compararla con la segunda magnitud de sensor (e_2).

3. Sistema de ordenador según la reivindicación 1, **caracterizado porque** la segunda magnitud de sensor (e_2) se diferencia de la primera magnitud de sensor (e_1) por una constante aditiva (K).

4. Sistema de ordenador según la reivindicación 1, **caracterizado porque** la segunda magnitud de sensor (e_2) se diferencia de la primera magnitud de sensor (e_1) por un factor constante (k).

5. Sistema de ordenador según la reivindicación 1, **caracterizado porque** el primer sensor (S1) y el segundo sensor (S2) detectan diferentes magnitudes físicas.

Fig. 1

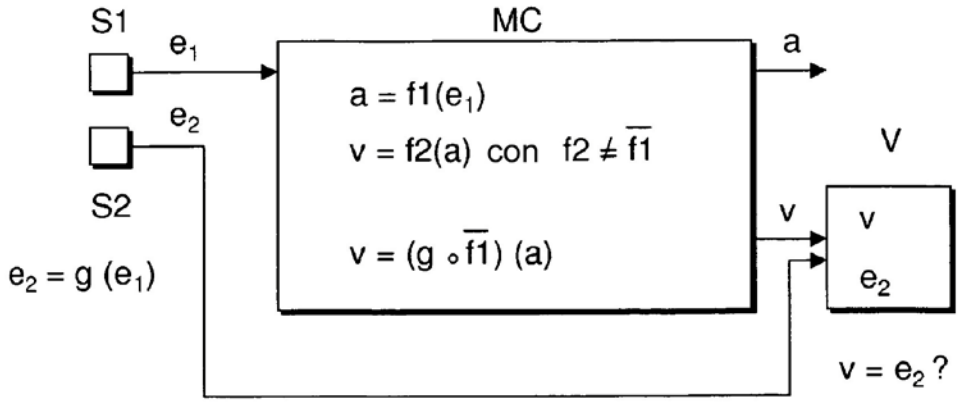
S1
e1
MC
a
a = f1(e1)
e2
v = f2(a) con f2 ≠ f1
V
S2
v
v
v = (g ∘ f1) (a)
e2 = g (e1)
e2
v = e2 ?

Fig. 2

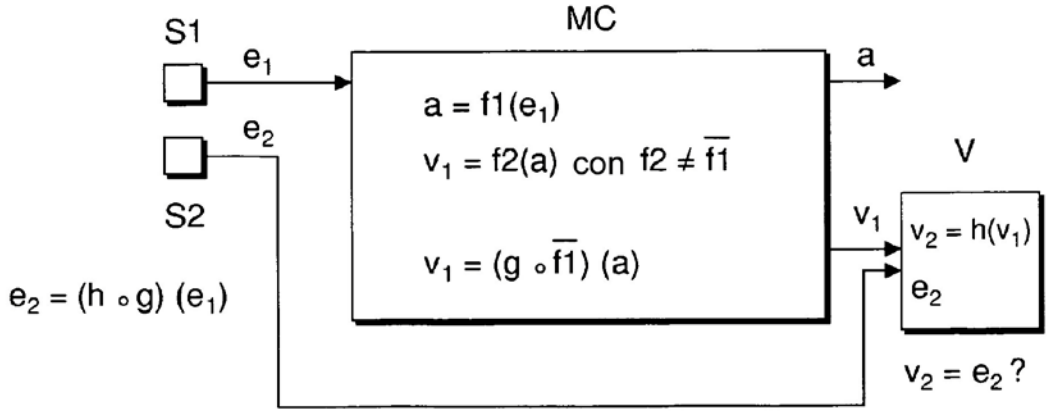
S1
MC
e1
a
a = f1(e1)
e2
v1 = f2(a) con f2 ≠ f1
V
S2
v1
v2 = h(v1)
v1 = (g ∘ f1) (a)
e2 = (h ∘ g) (e1)
e2
v2 = e2 ?

Fig. 3 Estado de la técnica

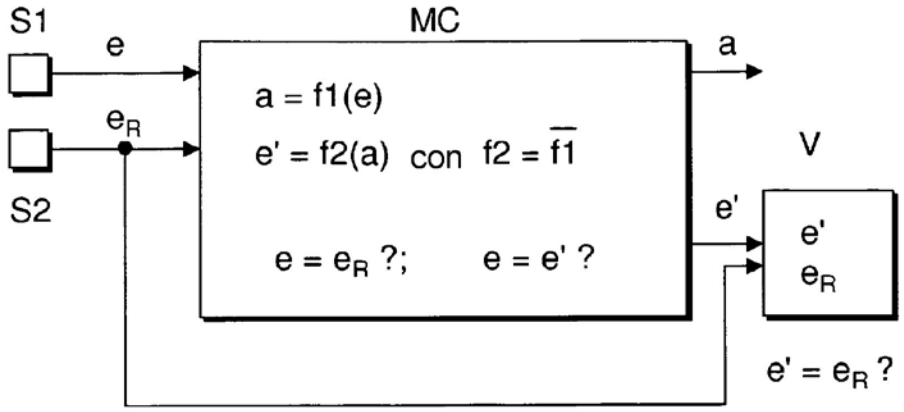

Fig. 4 Estado de la técnica

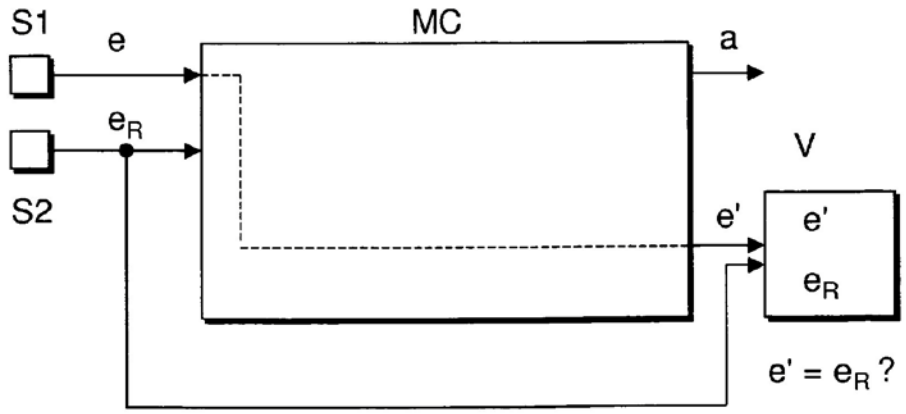

Fig. 5