(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 619 190**

(51) Int. CI.:

G06F 11/07 (2006.01)
G06F 11/16 (2006.01)
G09G 3/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.12.2014 E 14004441 (3)**

(97) Fecha y número de publicación de la concesión europea: **28.12.2016 EP 3040862**

(54) Título: **Método y sistema para la visualización segura de información relevante para la seguridad**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.06.2017

(73) Titular/es:

Auchmann, Matthias (100.0%)
Herrenholzgasse 29
1210 Wien, AT

(72) Inventor/es:

AUCHMANN, MATTHIAS

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Método y sistema para la visualización segura de información relevante para la seguridad

La presente invención se relaciona con un método y un sistema para la visualización segura de información relevante para la seguridad en un elemento de representación, en donde se genera una visualización segura de al menos un parámetro de entrada variable usando capas seguras.

Actualmente, los elementos de representación se usan cada vez más como unidades de visualización en muchas aplicaciones, en sistemas de monitorización y control por ejemplo. Además de esos casos, los elementos de representación son más comúnmente utilizados para visualizar información relevante para la seguridad en el campo del control de trenes o aviones, por ejemplo. Generalmente unidades de este tipo están basadas en un microcontrolador o un ordenador personal equipado con software que se ejecuta en un sistema operativo.

En ello, un fallo de visualización es considerado como un fallo relevante para la seguridad si el elemento de representación solo parece que trabaja bien o parece que muestra la información correcta, pero realmente no representa la información correcta proporcionada a la unidad de visualización, por ejemplo no muestra la velocidad actual del tren. El elemento de representación solo muestra un valor aparentemente correcto, el fallo, sin embargo, no puede ser detectado como tal por un observador.

Métodos y aparatos comunes para la aplicación de métodos para una visualización segura de información relevante para la seguridad se basan en la suposición de que el fallo de visualización resulta en una imagen obviamente falsa y así es evidente para el observador. Por ejemplo, los datos visualizados pueden estar mezclados, pueden cambiar de color, o una figura puede estar incompleta o mostrarse con forma distorsionada, tal que el observador puede claramente ver que algo está mal.

El documento DE 3411015 A1 describe un método para la visualización segura de información relevante para la seguridad, en donde un parámetro de entrada es trasformado en una secuencia de datos de imagen que representan el parámetro de entrada y la secuencia de datos de imagen es transmitida a un elemento de representación. Además, se calcula una suma de comprobación para la secuencia de datos de imagen y se compara con una suma de comprobación de referencia y se proporciona una reacción enfocada en la seguridad, si la suma de comprobación no es idéntica a la suma de comprobación de referencia.

Sin embargo, considerando un velocímetro simple con 24 bits de profundidad de píxel, que muestra por ejemplo la velocidad actual, velocidad mínima, velocidad máxima y velocidad objetivo, que tiene cuatro fuentes de entrada, si cada una de esas fuentes tiene 10 bits de resolución, el velocímetro tendría un total de 2^{40} estados posibles. Además, si cada suma de comprobación tuviera cuatro bytes, solo los datos de suma de comprobación sumarían un total de 4 Tera bytes de datos de suma de comprobación, lo que sería mucho más de lo que proporciona cualquier sistema incorporado actual. Se puede encontrar una visualización de un velocímetro ejemplar en GUI (interfaces de usuario gráficas) de trenes modernos como se describe en el estándar ERA ERTMS para “ETCS Driver Machine Interface” del Sistema de Control de Trenes Europeos (ETCS), o en complejidades similares a lo largo de la industria en aplicaciones modernas.

Incluso si un sistema incorporado pudiera ofrecer tal inmensa cantidad de memoria, el cálculo previo de sumas de comprobación sería poco práctico. Considerando que se calcularían 10 sumas de comprobación en un ordenador personal por segundo, llevaría sobre 3487 años calcular 2^{40} sumas de comprobación de referencia, lo que sería inaceptable.

El documento EP-A1-2 439 722 describe un método que comprende el paso de descomponer una visualización segura de al menos un parámetro de entrada variable en sus elementos seguros para todos los posibles estados de al menos un parámetro de entrada variable. Los datos de visualización en formato píxel relevantes para la seguridad son extraídos antes de un elemento de representación de un dispositivo de visualización. Los datos extraídos son entonces convertidos en datos de visualización comprimidos relevantes para la seguridad en un controlador y un conjunto de datos con datos de visualización de referencia comprimidos relevantes para la seguridad son almacenados en una memoria del controlador, en donde se comparan entre sí los datos de visualización de referencia comprimidos y datos de visualización comprimidos, y se visualizan las discordancias de los datos de referencia comprimidos y datos de visualización comprimidos en un dispositivo de visualización a un usuario mediante una señal.

Es un objeto de la presente invención proporcionar un método mejorada para la visualización segura de información relevante para la seguridad en un elemento de representación.

La presente invención proporciona un método para la visualización segura de información relevante para la seguridad. En ello, el método comprende lo siguiente:

En un primer paso, para todos los posibles estados de al menos un parámetro de entrada variable, una visualización segura de al menos un parámetro de entrada variable se descomponen en sus elementos base seguros, sus capas

seguras, en donde cada uno de los elementos base seguros pueden ser estáticos o representar la información de visualización en al menos un parámetro de entrada variable.

En un segundo paso, para cada uno de los elementos base seguros descompuestos y, por lo tanto, para cada una de las capas seguras, se enumera un conjunto de todos los estados posibles de visualización de elementos base seguros y se almacena en un formato adecuado en donde el conjunto de todos los estados posibles de la visualización de elementos base seguros comprende la visualización de un elemento base seguro en las visualizaciones seguras de al menos un parámetro de entrada variable para todos los estados posibles de al menos un parámetro de entrada variable. Por ejemplo, asumiendo que el al menos un parámetro de entrada variable incluye la velocidad actual de un tren, entonces las visualizaciones de todos los estados posibles de la velocidad actual del tren se enumeran y almacenan en un formato adecuado.

En un tercer paso, para cada uno de los elementos base seguros descompuestos y, por lo tanto, para cada una de las capas seguras, se transmite el conjunto de todos los estados posibles de visualización de elementos base seguros a un sistema objetivo que proporciona la visualización segura en tiempo de ejecución.

En un cuarto paso, para cada uno del al menos un parámetro de entrada variable se introduce un estado real del al menos un parámetro de entrada variable en el sistema objetivo, y para cada parámetro de entrada variable se determina el elemento base seguro correspondiente, la capa segura, y su estado correcto, por ejemplo buscando en el respectivo conjunto de todos los estados posibles de visualización del elemento base seguro.

En un quinto paso, cada capa segura correspondiente, en particular la visualización de cada elemento base seguro correspondiente, es representada, una tras otra, una superpuesta a la anterior. Este quinto paso, en particular la representación y superposición del estado del elemento base seguro correcto, genera de manera segura la visualización segura original del estado real del al menos un parámetro de entrada variable, que es entonces visualizado en un elemento de representación.

El método está basado en la descomposición de la visualización de uno o múltiples parámetros de entrada en sus elementos base. Por ejemplo, para un velocímetro simple, mostrando por ejemplo la velocidad actual de un tren, velocidad mínima, velocidad máxima y velocidad objetivo, la visualización de cuatro parámetros en un área rectangular se descompone en cuatro visualizaciones comparativamente simples, una para cada uno de los parámetros de entrada, simplificando de este modo el problema. Los conjuntos de visualizaciones de elementos base descompuestos se pueden representar con seguridad uno encima de cada uno, de este modo transformando un problema multiplicativo en un problema aditivo y así reduciendo la cantidad de estados posibles de visualización. En particular, visualizaciones simples separadas son rearmadas mediante la superposición de capas seguras para reproducir la visualización original desde el conjunto simple de elementos base. En ello, el término capa se introduce porque los elementos base individuales normalmente necesitan ser representados uno encima de los otros en un orden específico orden z para producir la visualización original, en donde un elemento se superpone a otro.

En ello, más que usar sumas de comprobación para cada posible estado de la visualización original para fines de verificación, los datos de imagen descompuestos se pueden usar directamente y representar con seguridad. En particular, la visualización segura se descompone en las fuentes respectivas, que pueden ya haberse realizado en el tiempo de diseño durante un proceso de desarrollo. En ello, una visualización de elemento base es almacenada tras la otra de este modo formando capas, cada una de las cuales luego, en tiempo de ejecución, será mostrada encima de las otras, de este modo generando una visualización segura del al menos un parámetro de entrada variable. Además, cada estado posible de una visualización de elemento base se puede transformar antes de ser almacenada para reducir la cantidad de capacidad de almacenamiento requerida para la capa de imagen. La transformación para reducir el almacenamiento puede ser un algoritmo de compresión, o almacenar la visualización del elemento base particularmente eficientemente, tal como almacenarla en un formato de gráficos de vector. De este modo, para un velocímetro simple a una profundidad de píxel RGBA de 32 bits, mostrar por ejemplo la velocidad actual de un tren, velocidad mínima, velocidad máxima y velocidad objetivo, con cuatro parámetros de entrada, y, por lo tanto, cuatro fuentes de entrada, en donde los datos críticos de seguridad son posibles estados de visualización de los cuatro parámetros de entrada, usando compresión de imagen como la transformación y asumiendo una compresión de 25k bytes para la superposición de imagen base estática y aproximadamente 3k bytes de datos comprimidos por visualización de elemento base, con cada parámetro de entrada siendo una entrada de 10 bits, un almacenamiento total de 25k bytes + 2^{10} * 3k bytes + 2^{10} * 3k bytes + 2^{10} * 3k bytes + 2^{10} * 3k bytes y, por lo tanto, se requiere una cantidad total de aproximadamente 12 Mega bytes. La suposición de los tamaños de compresión como se enunció anteriormente puede alcanzarse fácilmente con algoritmos de compresión conocidos. Cuando se usan otras formas de transformación antes de almacenar los datos de imagen de los posibles estados, tales como por ejemplo gráficos de vector, la compresión alcanzada podría ser incluso mucho mejor. Si esto se compara con el método común de sumas de comprobación de todos los $2^{10+10+10+10}=2^{40}$ estados de visualización de la visualización segura original, asumiendo que cada suma de comprobación tiene 4 Bytes, el almacenamiento requerido alcanzaría 4 Tera bytes de datos de suma de comprobación, que es aproximadamente 349525 veces peor que los 12 Mega bytes de almacenamiento de datos requeridos.

El último cálculo además indica los beneficios de la presente invención, a saber transformar el problema de visualización segura en una representación aditiva mediante medios apropiados más que usar el problema de

representación multiplicativo común, produciendo una drástica reducción en estados de visualización. Al inicio del tiempo de computación para el tiempo de diseño, ciertamente la descomposición de la visualización, la enumeración de todos los estados para cada capa y la transformación y almacenamiento de datos para las capas en una forma comprimida o un formato específico puede llevar más tiempo que el cálculo de sumas de comprobación para una única imagen, sin embargo considerando un ordenador personal que ejecuta 1 descomposición y transformación adecuadas y almacena la operación (por ejemplo compresión o representación de gráficos de vector) por segundo, para el velocímetro simple como se describió anteriormente se requiere un tiempo de computación de 4097 segundos para la extracción de todos los datos. Para soluciones conocidas actualmente, el paso de enumeración todavía tendría que ser realizado, e incluso si los cálculos de sumas de comprobación fueran más rápidas y el mismo ordenador personal fuera diez veces más rápido en el cálculo de las sumas de comprobación, siendo capaz de calcular 10 sumas de comprobación por segundo, todavía se necesitaría un tiempo de computación de aproximadamente 3487 años para calcular 2^{40} sumas de comprobación, que es debido a la inmensa cantidad de estados en la visualización original, si el problema de visualización no se descompone y así se rompe. Al contrario, una búsqueda en tiempo de ejecución de las visualizaciones de elementos base respectivos del al menos un parámetro de entrada variable y una transformación inversa correspondiente y representación del estado transformado inversamente de cada visualización de elemento base es ciertamente más caro computacionalmente que el mero cálculo de sumas de comprobación, sin embargo es fácilmente realizable con procesadores modernos o FPGA, incluso en tasas de trama que se correspondan con LCD (elementos de representación de cristal líquido) modernas. Así que los requisitos de potencia de computación en tiempo de ejecución son más altos, pero fácilmente dentro de los límites del hardware moderno.

Por lo tanto, se proporciona un método mejorado para la visualización segura de información relevante para la seguridad compleja en un elemento de representación en cuanto a requisitos de almacenamiento y tiempo de computación de tiempo de diseño. También el método no está restringido a un velocímetro representado como datos de imagen RGBA, más bien se pueden concebir todas las formas posibles de visualización en varios espacios de color o representaciones de datos. Mediante el método de la presente invención se pueden usar visualizaciones arbitrarias y complejas, dado que se pueden simplificar muy eficientemente aun en un modo genérico. También, mientras que la reconstrucción real de la visualización original en tiempo de ejecución está bien adaptada a cómo las librerías GUI modernas usan el orden z y mezcla alfa y/o enmascaramiento alfa para implementar la visualización en primer lugar, la complejidad del hardware y/o software necesarios se reduce drásticamente en comparación con las librerías GUI modernas y sus sistemas operativos subyacentes y el hardware requerido. Por lo tanto, el método es suficientemente simple para implementar de forma que puede incluso descargarse a pequeñas unidades de procesamiento incorporadas, tal como la parte relevante de seguridad del método es razonablemente pequeño y así fácilmente certificable, y aun capaz de virtualmente todas las visualizaciones comunes realizadas por computadoras personales completas con hardware y software complejos. Además, el método se puede usar para mejorar el rendimiento de presentación de gráficos, también, sin ningún fondo de seguridad.

En ello, el conjunto de todos los estados posibles de visualizaciones de elementos base seguros se pueden almacenar por ejemplo como una imagen en un espacio de color como RGBA (Rojo Verde Azul Alfa), que es un espacio de color común para imágenes computerizadas, en donde el canal alfa habilita a los píxeles a ser transparentes, traslúcidos y opacos. El conjunto de todos los estados posibles de visualizaciones de elementos base seguros generado por la descomposición de visualizaciones seguras podría también transformarse opcionalmente en un modo adecuado antes de almacenarse, por ejemplo comprimirse. Además, el conjunto de todos los estados posibles de visualizaciones se pueden almacenar en el orden z (el orden de superponer objetos de dos dimensiones en una visualización) en el cual ocurren en la visualización segura original. El primer y segundo pasos son normalmente, pero no necesariamente, realizados una vez para una visualización de una GUI (Interfaz de Usuario Gráfica) dada, y son realizadas normalmente pero no necesariamente en tiempo de diseño. En ello, el estado de elemento base seguro correcto se puede superponer en el orden z en el cual fueron almacenados en el segundo paso. Además, si un formato de imagen capaz de píxeles traslúcidos o transparentes, un medio de superposición para realizar la superposición necesita implementar la mezcla alfa. La mezcla alfa es el proceso de combinar un color de píxel en primer plano traslucido con un color de píxel de fondo, produciendo por lo tanto un nuevo color mezclado para el píxel resultante. Opcionalmente, la superposición se puede también procesar mediante la implementación de enmascarado alfa. El enmascarado alfa es el proceso de aplicar una máscara alfa binaria adicional por capa, en particular si la capa depende de dos o más parámetros de entrada variables. Dado que una máscara alfa tiene solo un bit por píxel, es rápido y eficiente de almacenar, sin embargo puede simplificar significativamente algunos tipos de visualizaciones, especialmente cuando la máscara alfa a aplicar puede depender de una o más parámetros de entrada variables. En ello, la transformación inversa opcional necesita hacerse para revertir la transformación realizada cuando se almacenó el conjunto de todos los estados posibles de visualizaciones de elementos base seguros generados por la descomposición de visualizaciones seguras, si tal transformación se hizo, y podría consistir en la descompresión de una imagen RGBA. También, un sistema de descomposición en tiempo de diseño para descomponer los elementos base de visualización en tiempo de diseño y el sistema objetivo se pueden ser dispositivos separados o se pueden integrar en el mismo dispositivo, siendo así partes de un único dispositivo.

En algunas realizaciones, para todos los estados posibles del al menos un parámetro de entrada variable podría haber también datos no críticos de seguridad a ser mostrados, en donde los datos no críticos de seguridad son

transmitidos a la unidad de elemento de representación y en donde la técnica de introducir al menos un parámetro de entrada variable en el sistema objetivo, determinar las capas seguras correspondientes del al menos un parámetro de entrada variable y buscar el estado correcto en el conjunto de todos los estados posibles de visualizaciones de elementos base seguros, y representar sucesivamente cada capa segura, por ejemplo la visualización de cada elemento base seguro, uno tras otro, uno superponiéndose al anterior, produciendo finalmente la visualización segura completa del al menos un parámetro de entrada variable, comprende lo siguiente: Los datos no críticos de seguridad son representados primero. Entonces los datos no críticos de seguridad son superpuestos sucesivamente por las capas seguras, mediante la representación sucesiva de cada capa segura, por ejemplo la visualización de cada elemento base seguro, uno tras otro, uno superponiéndose al anterior, produciendo finalmente la visualización segura completa del al menos un parámetro de entrada variable. Esto resulta en una mayor reducción de requisitos de almacenamiento y tiempo de computación, dado que los datos no críticos de seguridad por ejemplo no tienen que ser descompuestos y almacenados. En ello, los datos no críticos de seguridad pueden comprender contenido no crítico de seguridad, por ejemplo, un color de fondo o botones con esquinas redondeadas o transparentes. Mientas que los colores de fondo o esquinas redondeadas que son superpuestas con información relevante de seguridad son ejemplos muy comunes de partes no críticas de seguridad, también se pueden concebir en ciertos escenarios que se usen datos no críticos de seguridad en capas con orden z más que 0. Además, los datos no críticos de seguridad podrían también transmitirse al sistema objetivo y mostrarse en el orden z adecuado.

En ello, elementos de visualización no críticos de seguridad se pueden descomponer y transformar y procesar en el mismo modo que los elementos base seguros, también. Esto podría hacerse para mejorar la pureza arquitectónica o si es beneficioso desde un punto de vista de rendimiento.

Además, en algunas realizaciones, se usa un algoritmo de compresión como el paso de transformación para los elementos del conjunto de todos los estados posibles de visualizaciones de elementos base seguros generados mediante la descomposición de visualizaciones seguras para comprimir por separado datos de imagen, y se usa un algoritmo de descompresión correspondiente como la transformación inversa en tiempo de ejecución. El algoritmo de compresión puede ser un algoritmo de compresión sin pérdidas, en particular un algoritmo de compresión que permita que los datos originales sean perfectamente reconstruidos desde los datos comprimidos, pero podría también ser un algoritmo de compresión con pérdida de datos, en particular un algoritmo que permite la reconstrucción de una aproximación de los datos originales, como se usa comúnmente para datos de imagen o video, si la seguridad no se ve afectada significativamente. Esto significa que el método de introducir al menos un parámetro de entrada variable, determinar los elementos base seguros correspondientes del al menos un parámetro de entrada variable y buscar el estado correcto en el conjunto de todos los elementos base seguros generados por la descomposición de visualizaciones seguras, una tras otra, una superponiéndose a la anterior, produciendo finalmente la visualización segura completa del al menos un parámetro de entrada variable, además comprende los pasos de descomprimir los datos de cada capa segura antes de representarlos como la transformación inversa. Las utilidades de compresión de archivos, que son programas que aplican un algoritmo de compresión de archivos para formar desde uno, a una serie de archivos, y crear un archivo de archivos, son conocidos en la técnica y son, por lo tanto, bastante fáciles de implementar. Las utilidades de compresión de archivos convencionales tienen una característica de extracción que usa el algoritmo original usado para comprimir y crear el archivo, para extraer adecuadamente y recuperar los archivos desde el archivo y, así, estas utilidades de compresión de archivos convencionales pueden usarse para comprimir cada uno de los elementos del conjunto de datos críticos de seguridad extraídos. Además, las utilidades de compresión de archivos son capaces de colocar múltiples archivos en un archivo de archivos, con un tamaño de archivo menor que la suma de los archivos en él y, así, la cantidad de capacidad de almacenamiento se puede reducir más. También, hay algoritmos de compresión conocidos en la técnica que son específicamente eficientes cuando se usan con datos de imagen.

Como un ejemplo de un algoritmo de compresión de imágenes sin pérdidas que está bien adecuado para datos de imagen y también es particularmente eficiente y fácil de implementar en un sistema incorporado, el algoritmo de compresión puede ser un algoritmo de tabla de búsqueda de color con codificación de longitud de secuencia, para comprimir sucesivamente los elementos respectivos. En la teoría de codificación, una tabla de búsqueda es usada comúnmente para mantener símbolos más largos frecuentes en los datos originales, reemplazar los símbolos más largos en los datos originales por índices de tabla de búsqueda más cortos, por lo tanto comprimiendo los datos originales. En el caso de datos de imagen, los colores son candidatos adecuados a ser usados como símbolos en las tablas de búsqueda. La codificación de longitud de secuencia es una forma muy simple de compresión de datos en la cual secuencias de datos son almacenados como un único valor de dato y cuenta, más que la secuencia original. Esto es más útil en datos que contienen muchas de esas secuencias, por ejemplo imágenes de gráficos simples como iconos, dibujos de líneas, por ejemplo los números y letras en el dial proyectado de un velocímetro convencional. Por lo tanto, dado que muchos datos de imagen, especialmente para las capas, tienen mayormente píxeles transparentes, usar una tabla de búsqueda de color para cada capa y combinarla con codificación de longitud de secuencia es una técnica muy eficiente, resultando usualmente en tasas de compresión del 10% de los datos originales para la imagen base, y sobre el 2% para una capa típica. Además, tal algoritmo puede implementarse fácilmente en hardware y es factible para tanto procesadores de propósito general como FPGA.

Además, en algunas realizaciones, el paso de transformación para el conjunto de todos los estados posibles de visualizaciones de elementos base seguros puede ser convertir cada elemento del conjunto de todos los elementos seguros generados mediante la descomposición de visualizaciones seguras en un formato de gráficos de vector, que

es particularmente eficiente en términos de requisitos de almacenamiento, y puede también ser implementado eficientemente como la transformación inversa en la etapa de representación en tiempo de ejecución.

Además, el tercer paso de transmitir los elementos base seguros descompuestos, opcionalmente transformados y almacenados y, por lo tanto, datos críticos de seguridad podría incluir formas para asegurar la integridad de los datos de los datos transmitidos, mediante técnicas conocidas tales como firmas o sumas de comprobación de transmisión.

En algunas realizaciones, el tercer paso de transmitir los elementos base seguros descompuestos y almacenados, podría incluir una inspección relevante para la seguridad o paso de verificación para los datos almacenados, por ejemplo, mediante inspección manual, semiautomática o automática. Esto está destinado a mejorar la seguridad, servir como una así llamada barrera de seguridad, o introducir seguridad mediante algún tipo de inspección, en particular una barrera de seguridad que cruza desde un dominio no seguro a uno seguro. Durante el paso de inspección/verificación se podrían añadir firmas para la autentificación.

También se pueden usar espacios de color capaces de tener píxeles traslúcidos y transparentes en el segundo paso. En esas realizaciones, un medio de superposición para superponer las capas seguras necesita implementar mezcla alfa. La mezcla alfa es el proceso de combinar un color de píxel de primer plano traslúcido con un color de píxel de fondo, por lo tanto produciendo un nuevo color mezclado para el píxel resultante.

Opcionalmente, cada capa puede también ser procesada mediante el enmascarado alfa. El enmascarado alfa es el proceso de aplicar una máscara alfa binaria adicional por capa, en particular si la capa depende de dos o más parámetros de entrada variables. Dado que una máscara alfa tiene solo un bit por píxel, es rápido y eficiente de almacenar, sin embargo puede simplificar significativamente algunos tipos de visualizaciones, especialmente cuando la máscara alfa a aplicar pude depender de uno o más parámetros de entrada variables.

Además, el orden z usado para superponer los datos, puede o estar predefinido o fijado, pero podría ser una opción de configuración o podría incluso depender de parámetros de entrada variables y así cambiar en tiempo de ejecución. Por ejemplo, si la velocidad actual de un tren excede un valor predefinido, la visualización correspondiente y, por lo tanto, el elemento base seguro correspondiente puede ser mostrado encima de las otras visualizaciones de elementos base seguros.

Además, los datos de imagen y, por lo tanto, cada elemento del conjunto de todos los estados posibles de visualizaciones de elementos base pueden ser almacenados por separado. En adelante, almacenado por separado significa que cada elemento puede almacenarse en un área separada de una memoria segura, por ejemplo una memoria no volátil, que es una memoria de ordenador que puede mantener información almacenada aun cuando no está alimentada. Mediante el almacenaje por separado de cada elemento del conjunto de todos los estados posibles de visualizaciones de elementos base seguros el tiempo de acceso para leer cada elemento del conjunto de todos los elementos base seguros generados mediante la descomposición de visualizaciones seguras se puede acortar. El tiempo de acceso es el tiempo que un dispositivo informático requiere para acceder el archivo por ejemplo, para leer o escribir.

Aunque la visualización segura del estado real del al menos un parámetro de entrada variable se puede generar mediante la transformación inversa sucesiva y opcional y entonces representación y superposiciones de los elementos base seguros, las capas, de los datos críticos de seguridad originales descompuestos, en algunas realizaciones el método puede además comprender lo siguiente: Cada una de las visualizaciones de elementos base requeridas son comparadas con una versión del elemento base seguro respectivo del conjunto de todos los estados posibles de visualizaciones de elementos base seguros que son mostrados respectivamente en un elemento de representación. Además, se proporciona una reacción enfocada en la seguridad, si al menos uno de las visualizaciones de elementos base seguros requeridas no es idéntica a la versión del elemento base seguro respectivo que es mostrada eficazmente en el elemento de representación. En ello, la comparación se puede llevar a cabo en una de muchas formas adecuadas, por ejemplo por comparación de ancho de píxel, por ejemplo píxel a píxel, o por partes relevantes de los datos de píxel tales como para solo ciertos componentes de color, o mediante el cálculo de sumas de comprobación de las capas esperadas y las reales, y comparando las sumas de comprobación, o haciendo algún tipo de correspondencia de patrones. Mediante la comprobación de un elemento del conjunto de todos los estados posibles de visualizaciones de elementos base contra una versión del elemento respectivo del conjunto de todos los estados posibles de visualizaciones de elementos base que son mostrados eficazmente, es necesario admitir una tolerancia, y proporcionar una reacción enfocada en la seguridad si una capa esperada no es idéntica a la versión de la capa respectiva que es mostrada eficazmente, se introduce una alta eficiencia y arquitectura de visualización segura con dos canales, donde el canal hacia delante hace la visualización real y el canal de verificación proporciona o mejora la integridad en un modo relevante para la seguridad mediante la comparación de la visualización actual con la visualización esperada. Si no está disponible el acceso a las representaciones de elementos base separados o capas del canal hacia delante para la verificación del canal, la verificación del canal puede representar la visualización del al menos un parámetro de entrada variable mediante la representación sucesiva y superposición de los elementos base seguros, las capas, de los datos críticos de seguridad originales descompuestos en una memoria intermedia sombra, y puede entonces comparar la visualización resultante con lo que realmente se está mostrando, otra vez con un medio de comparación adecuado,

tal como algún tipo de comparación de ancho de píxel, comparación de suma de comprobación o correspondencia de patrones, por ejemplo.

En ello, la reacción enfocada en la seguridad puede ser apagar el elemento de representación. En ello, el elemento de representación puede apagarse completamente o hasta un cierto grado. Sin embargo, todos los métodos que indican claramente un fallo crítico de seguridad a un observador son adecuados como reacciones enfocadas en la seguridad, por ejemplo proporcionar marcado de datos, enmascaramiento o distorsión o apagado del HMI.

También se proporciona un sistema para la visualización segura de una información relevante para la seguridad, proporcionando un primer medio que compara un medio de descomposición para realizar el primer paso, en particular para todos los estados posibles de al menos una descomposición del parámetro de entrada variable de la visualización segura del al menos un parámetro de entrada variable en sus elementos base seguros, las capas seguras, y unos medios de enumeración, transformación y almacenamiento para realizar el segundo paso, en particular enumerando, transformando opcionalmente y entonces almacenando todos los posibles estados de cada capa en un conjunto de todos los estados posibles de visualizaciones de elementos base.

Un segundo medio implementa el tercer paso y comprende un medio de transmisión y un medio opcional de inspección.

Un tercer medio presenta una entrada de al menos un parámetro de entrada variable, implementa un procesamiento del parámetro de entrada y comprende un medio de determinación para determinar para cada uno del al menos un parámetro de entrada variable los elementos base seguros correspondientes, las capas seguras, y su estado correcto dependiendo de un estado real del al menos un parámetro de entrada variable, y un medio de superposición, transformación inversa opcional y entonces representación de un elemento base seguro tras otro, uno superponiéndose al anterior, por ejemplo en el orden z en el cual fueron almacenados, usando si es necesario mezclado alfa y/o enmascaramiento alfa. También, el tercer medio comprende un medio de visualización, para mostrar la visualización resultante.

El sistema con sus tres medios por lo tanto genera una visualización segura del al menos un parámetro de entrada variable. El primer medio podría por ejemplo ser un ordenador personal, el segundo medio podría ser un volumen de almacenamiento, tal como una memoria USB, una tarjeta SD, una memoria flash de tipo NAND o un disco duro, o algún tipo de conexión directa, por ejemplo Ethernet o WLAN, y los datos a ser transmitidos podrían ser inspeccionados opcionalmente por otro ordenador personal opcional que podría abrir y mostrar los datos transmitidos desde el volumen de almacenamiento o antes o durante la transmisión a través de la conexión directa. El tercer medio podría ser un HMI de algún tipo, usualmente un sistema incorporado que presenta un procesador o una FPGA o ambos, y un elemento de representación TFT, como se encuentra comúnmente en aplicaciones industriales, de trenes, de automóviles y de aviones, pero podría ser también un ordenador personal.

En algunas realizaciones, se usa un sistema que combina los tres medios en una unidad de computación potente que realiza todos los pasos anteriores.

Así, el sistema presentado para la visualización segura de información relevante para la seguridad está basado en la descomposición de la visualización de al menos un parámetro de entrada variable en sus elementos base, las capas, por lo tanto también descomponiendo el problema. Los conjuntos de visualizaciones de elementos base descompuestos se pueden representar de forma segura encima de cada uno en tiempo de ejecución, transformando por lo tanto un problema multiplicativo en un problema aditivo y así reduciendo la cantidad de estados de visualizaciones posibles. Más que usar sumas de comprobación para verificar la visualización para cada estado posible de la visualización original, los datos de imagen descompuestos son usados directamente y bien representados de manera segura en una unidad de computación segura, o usados en combinación con algún tipo de comparación de ancho de píxel, correspondencia de patrones o sumas de comprobación para fines de verificación, pero para la ahora reducida cantidad de estados de visualización del problema descompuesto más que para la posiblemente enorme cantidad original de estados de visualización. La descomposición del problema está bien adaptada a cómo las librerías GUI usan el orden z y mezcla alfa y/o enmascarado alfa para implementar la visualización en primer lugar, y se puede realizar en una unidad relevante de seguridad pequeña y simple para hacer la representación, o una arquitectura de 2 canales en el canal de verificación para añadir o mejorar la seguridad. Además, cada estado posible de visualizaciones de elementos base de seguridad puede transformarse antes de ser almacenado para reducir la cantidad de capacidad de almacenamiento requerida para la capa de imagen. La transformación para reducir el requisito de almacenamiento podría ser un algoritmo de compresión, o almacenar la visualización de elemento base de manera particularmente eficiente, tal como almacenarlo como gráficos de vectores. Por lo tanto, para un velocímetro simple con una profundidad de píxel RGBA de 32 bits, mostrando por ejemplo la velocidad actual, velocidad mínima, velocidad máxima y velocidad objetivo de un tren, con cuatro parámetros de entrada y, por lo tanto, cuatro fuentes de entrada, en donde los datos críticos de seguridad son posibles estados de visualización de los cuatro parámetros de entrada, usando compresión de imagen como la transformación y asumiendo una compresión de 25k bytes para la superposición de imagen base estática y aproximadamente 3k bytes de datos comprimidos por visualización de elemento base, con cada parámetro de entrada siendo una entrada de 10 bits, un almacenamiento total de 25k bytes + 2^{10} * 3k bytes + 2^{10} * 3k bytes + 2^{10} * 3k bytes + 2^{10} * 3k bytes y, por lo tanto, se requiere una cantidad total de aproximadamente 12 Mega bytes. Cuando

se usan otras formas de transformación antes de almacenar los datos de imagen de los posibles estados, tales como por ejemplo gráficos de vector, la compresión alcanzada podría ser incluso mucho mejor. Si esto se compara con el método común de computar sumas de comprobación de todos los $2^{10+10+10+10}=2^{40}$ estados de visualización de la visualización segura original, asumiendo que cada suma de comprobación tiene 4 Bytes, el almacenamiento requerido alcanzaría 4 Tera bytes de datos de suma de comprobación, que es aproximadamente 349525 veces peor que los 12 Mega bytes de almacenamiento de datos requeridos. El último cálculo muestra claramente los beneficios del presente sistema para la visualización segura de información relevante para la seguridad, no solo haciendo el sistema más eficiente por un factor enorme, sino también habilitando visualizaciones seguras que antes habrían sido imposibles. Además, el sistema es suficientemente simple de implementar que puede incluso descargarse a pequeñas unidades de procesamiento incorporadas, y la parte relevante de seguridad del método es razonablemente pequeña y así fácilmente certificable.

En algunas realizaciones, pueden haber también datos no críticos de seguridad incluidos en la visualización, en donde los datos no críticos de seguridad son transmitidos al tercer medio del sistema por los medios de transmisión, y en donde el sistema además comprende un medio para incorporar datos de visualización no críticos de seguridad en los datos de visualización que están siendo mostrados en el elemento de representación. Esta tarea podría realizarse bien representando los datos no críticos de seguridad y entonces superponiendo las capas críticas de seguridad, o incorporando los datos no críticos de seguridad en el paso de superposición en orden z diferente a 0. Como una alternativa, para mejorar la pureza de la arquitectura, o como una realización mejorada, elementos de visualización no críticos de seguridad podrían descomponerse y transformarse y procesarse de la misma manera que los elementos de visualización seguros. Tomando un sistema que opera en un tren como un ejemplo, el velocímetro podría mostrar datos de visualización seguros, pero podría compartir el elemento de representación con la temperatura del aire acondicionado y un texto que mostrara por ejemplo el nombre de la siguiente estación, siendo estos dos últimos no críticos de seguridad. Estos datos no críticos de seguridad podrían transmitirse al tercer medio desde un sistema externo, o el tercer medio mismo, por ejemplo un ordenador HMI moderno, puede consistir tanto en una parte no relevante para la seguridad, tal como un sistema de procesamiento, como en una parte relevante para la seguridad, tal como un controlador de elemento de representación seguro implementado por ejemplo en una FPGA u otro procesador, con la parte no relevante para la seguridad representando la temperatura del aire acondicionado y el texto de la siguiente estación, y la parte relevante para la seguridad superponiendo el velocímetro relevante para la seguridad. En esto la parte no crítica de seguridad del sistema, podría proporcionar colores de fondo o puede proporcionar visualización de fondo que brille a través de esquinas redondeadas incluso de visualizaciones relevantes para la seguridad como un velocímetro seguro rectangular, en donde el velocímetro seguro se representa superpuesto encima de los datos no críticos de seguridad mediante la parte relevante para la seguridad del sistema, pero las esquinas del velocímetro seguro rectangular pueden contener datos transparentes y traslúcidos, en donde la mezcla alfa en la parte superpuesta del método permite que los datos no críticos de seguridad brillen a través. Usar mezcla alfa durante la superposición como se ha descrito permite escenarios muy complejos de datos relevantes para la seguridad y no relevantes para la seguridad mezclados. También, el enmascarado alfa podría opcionalmente usarse para cortar o dejar brillar solo partes específicas del fondo no seguro, con la máscara alfa incluso dependiendo de uno o más parámetros de entrada variables.

La parte segura del tercer medio podría también realizarse como parte de un controlador de gráficos externo, una parte de un controlador de gráficos integrado en una unidad de elemento de representación o como un dispositivo autónomo también.

La parte no segura y la parte segura podrían no solo estar incorporadas en el tercer medio todas juntas sino también podrían implementarse en una unidad de procesamiento con otros medios para separar la visualización segura y la visualización no segura, tal como por ejemplo mediante métodos de particionamiento por software.

En algunas realizaciones, el primer medio comprende una primera unidad de almacenamiento, en donde los medios de enumeración, transformación y almacenamiento usan un algoritmo de compresión almacenado en la primera unidad de almacenamiento para comprimir de manera separada cada estado posible de cada capa antes de almacenarla. Además, el medio de superposición usa un algoritmo de descompresión respectivo, que es en particular la transformación inversa respectiva del algoritmo de compresión usado, almacenado en una segunda unidad de almacenamiento en el tercer medio, para descomprimir los estados posibles comprimidos de cada capa antes de superponer los elementos base seguros representados. Las utilidades de compresión de archivos, que son programas que aplican un algoritmo de compresión de archivos para formar uno, a una serie de archivos, y crear un archivo de archivos, son conocidos en la técnica y son, por lo tanto, bastante fáciles de implementar. Utilidades de compresión de archivos convencionales tienen una característica de extracción que usa el algoritmo original usado para comprimir y crear el archivo, para extraer adecuadamente y recuperar los archivos desde el archivo y, así, estas utilidades de compresión de archivos convencionales pueden usarse para comprimir cada uno de los elementos base seguros descompuestos. Además, las utilidades de compresión de archivos son capaces de colocar múltiples archivos en un archivo de archivos, con un tamaño de archivo menor que la suma de los archivos en él y, así, la cantidad de capacidad de almacenamiento se puede reducir más. También, hay algoritmos de compresión conocidos en la técnica que son específicamente eficientes cuando se usan con datos de imagen.

Como un ejemplo de un algoritmo de compresión de imágenes sin pérdidas que está bien adecuado para datos de imagen y también es particularmente eficiente y fácil de implementar en un sistema incorporado, el algoritmo de

compresión cuyo código se almacena en la primera unidad de almacenamiento puede ser un algoritmo de tabla de búsqueda de color con codificación de longitud de secuencia, para comprimir sucesivamente los elementos respectivos. En la teoría de codificación, una tabla de búsqueda es usada comúnmente para mantener símbolos más largos frecuentes en los datos originales, reemplazar los símbolos más largos en los datos originales por índices de tabla de búsqueda más cortos, por lo tanto comprimiendo los datos originales. En el caso de datos de imagen, los colores son candidatos adecuados a ser usados como símbolos en las tablas de búsqueda. La codificación de longitud de secuencia es una forma muy simple de compresión de datos en la cual secuencias de datos son almacenados como un único valor de dato y cuenta, más que la secuencia original. Esto es más útil en datos que contienen muchas de esas secuencias, por ejemplo imágenes de gráficos simples como iconos, dibujos de líneas, por ejemplo los números y letras en el dial proyectado de un velocímetro convencional. Por lo tanto, dado que muchos datos de imagen, especialmente para las capas, tienen mayormente píxeles transparentes, usar una tabla de búsqueda de color para cada capa y combinarla con codificación de longitud de secuencia es una técnica muy eficiente, resultando usualmente en tasas de compresión del 10% de los datos originales para la imagen base, y sobre 2% para una capa típica. Además, tal algoritmo puede implementarse fácilmente en hardware y es factible para tanto procesadores de propósito general como FPGA.

Para todos los estados posibles del al menos un parámetro de entrada variable también podrían haber datos no críticos de seguridad a ser mostrados.

En algunas realizaciones, el tercer medio comprende una unidad de almacenamiento no volátil para almacenar los elementos base seguros transmitidos y una cuarta unidad de almacenamiento para almacenar los datos no críticos de seguridad. Puede haber además un controlador de gráficos, que gestiona la tercera unidad de almacenamiento o volátil así como la cuarta unidad de almacenamiento, para conmutar un flujo de datos entre los datos no críticos de seguridad y las capas críticas de seguridad. En particular, el controlador de gráficos seguros está conectado a la memoria no volátil, que contiene los datos de imagen de capa comprimida y a la cuarta unidad de almacenamiento, que podría ser un sistema no seguro y contiene datos no críticos de seguridad. Por lo tanto, el controlador de gráficos seguros puede gestionar las capas seguras él mismo, separando datos seguros y no seguros en la memoria de elemento de representación, y mostrando datos seguros encima de los datos no seguros. En ello, cada uno de los elementos del conjunto de todos los estados posibles de visualizaciones de elementos base seguros, en particular cada uno de los posibles estados de cada capa se puede almacenar en un área separada de la tercera unidad de almacenamiento no volátil, para acelerar el tiempo de acceso para leer cada visualización de elemento base seguro desde la tercera unidad de almacenamiento no volátil, y para facilitar la implementación.

Además, en algunas realizaciones, la unidad de almacenamiento comprende una unidad de almacenamiento, que comprende una parte no segura para almacenar datos no críticos de seguridad y una parte segura para almacenar los elementos base seguros. Dado que muchos sistemas no seguros tienen su propia memoria no volátil, esta memoria no volátil se puede usar y el sistema no seguro puede entregar los datos superpuestos seguros bajo pedido. Por lo tanto, comparando con dos unidades de almacenamiento diferente para los datos no críticos de seguridad y los datos críticos de seguridad, esta solución es más barata en términos de costes de hardware, pero requiere complejidad computacional adicional, para eliminar la memoria no volátil segura para los datos críticos de seguridad. Puede haber un controlador de gráficos seguros, también, para gestionar el flujo de datos gráficos. En particular, los datos críticos de seguridad se pueden encriptar con una clave de encriptación conocida por el controlador de gráficos seguros solo, o algunos otros medios para asegurar la integridad de los datos. Por lo tanto, el sistema no seguro puede ser un suministrador factible de datos seguros, añadiendo el coste de complejidad computacional y algorítmica aumentado, pero ahorrando un componente hardware. Si el sistema no seguro no cumple su deber de proporcionar datos de capa seguros de una manera oportuna, el controlador de gráficos seguros podría todavía conmutar a un estado seguro, por ejemplo borrando el elemento de representación o activando alguna otra función de seguridad, para alcanzar el objetivo de seguridad y, por lo tanto, la visualización segura de la información relevante para la seguridad.

Estos objetos se alcanzan aplicando las características mostradas en las reivindicaciones independientes 1 a 14. Las reivindicaciones dependientes se refieren a las realizaciones preferidas de la presente invención.

Se describirán ahora las realizaciones de la invención con referencia a los dibujos.

La figura 1 ilustra un sistema para la visualización segura de una información relevante para la seguridad según una primera realización.

La figura 2 ilustra un sistema para la visualización segura de una información relevante para la seguridad según una segunda realización.

La figura 3 ilustra un diagrama de flujo de un método para la visualización segura de una información relevante para la seguridad según una tercera realización.

Las figuras 4A-C ilustran una visualización segura de la velocidad real, velocidad mínima, velocidad máxima y velocidad objetivo de un tren en un cuadro de un velocímetro según la presente invención.

Las figuras 5A y B ilustran el uso de enmascaramiento alfa según la presente invención.

La figura 1 ilustra un sistema 1 para la visualización segura de una información relevante para la seguridad según una primera realización.

El sistema 1 mostrado comprende un primer medio 2, un segundo medio 3 y un tercer medio 4.

En ello, el primer medio 2 mostrado comprende un medio 5 de descomposición para realizar para todos los estados posibles de al menos un parámetro de entrada variable la descomposición de una visualización segura del al menos un parámetro de entrada variable en sus elementos base seguros, las capas seguras y unos medios 6 de enumeración, transformación y almacenamiento para enumerar, opcionalmente transformar y entonces almacenar todos los estados posibles de cada capa, en particular un conjunto de todos los estados posibles de visualizaciones de elementos base.

El segundo medio 3 mostrado comprende un medio 7 de transmisión para transmitir los estados posibles almacenadas para cada capa desde el primer medio 2 al tercer medio 4. En ello, el medio 7 de transmisión puede por ejemplo ser un volumen de almacenamiento, tal como una memoria USB, una tarjeta SD, una memoria flash de tipo NAND o un disco duro, o algún tipo de conexión directa, por ejemplo Ethernet o WLAN.

Además, el tercer medio 4 mostrado comprende un medio 8 de determinación para determinar las capas seguras correspondientes a un estado real del al menos un parámetro de entrada variable introducido en el tercer medio 4 y el estado correcto de las capas seguras determinadas dependiendo del al menos un parámetro de entrada variable, y un medio 9 de superposición para representar una capa determinada tras la otra, una superponiéndose a la anterior. Si el espacio de color usado presenta un canal alfa, la mezcla alfa se puede usar para hacer la superposición más poderosa. El enmascarado alfa puede usarse opcionalmente en cada capa, independientemente del espacio de color usado. Además, el tercer medio 4 mostrado comprende un medio 10 de visualización para mostrar la visualización resultante. En ello, según la realización de la figura 1, el medio 10 de visualización puede comprender por ejemplo un elemento de representación 11 TFT.

Según la realización de la figura 1, el al menos un parámetro de entrada variable comprende la velocidad actual de un tren, en donde en una visualización segura de la velocidad actual del tren se muestra también una velocidad mínima, velocidad máxima y velocidad objetivo del tren. Además, un estado real del al menos un parámetro V de entrada variable, por ejemplo una velocidad actual del tren, velocidad mínima, velocidad máxima o velocidad objetivo, es comunicada a e introducida en el tercer medio 4. En ello, el estado real de la velocidad actual del tren se puede originar desde y ser determinado por un ordenador principal, por ejemplo un control de tren realizado por ordenador, en el cumplimiento de los estándares y regulaciones de seguridad comunes.

El sistema 1 mostrado está basado en la descomposición de la visualización de uno o más parámetros de entrada múltiples en sus elementos base. En particular, para un velocímetro simple, mostrar por ejemplo la velocidad actual, velocidad mínima, velocidad máxima y velocidad objetivo de un tren, la visualización de cuatro parámetros en un área rectangular se descompone en cuatro visualizaciones comparativamente simples, una para cada uno de los parámetros de entrada, simplificando de este modo el problema. Los conjuntos de visualizaciones de elementos base descompuestos pueden entonces representarse con seguridad uno encima de los otros, transformando de este modo un problema multiplicativo en un problema aditivo y reduciendo así la cantidad de estados de visualización posibles. En particular, las visualizaciones más simples separadas son rearmadas mediante la superposición de capas seguras para reproducir la visualización original desde el conjunto simple de elementos base. En ello, el término capa se introduce porque los elementos base individuales normalmente necesitan ser representados unos encima de otros en un orden z específico para producir la visualización original, en donde un elemento se superpone sobre otro.

En ello, más que usar sumas de comprobación para cada estado posible de la visualización original con fines de verificación, los datos de imagen descompuestos se pueden usar directamente y representar de forma segura. En particular, la visualización segura se descompone en las fuentes respectivas, que pueden estar ya hechas en tiempo de diseño durante un proceso de desarrollo. En ello, una visualización de elemento base es almacenada tras otra formando capas de este modo, cada una de las cuales es luego, en tiempo de ejecución, mostrada encima de la otra, generando de este modo una visualización segura del al menos un parámetro de entrada variable.

En la realización mostrada en la figura 1, el primer medio 2 además comprende una primera unidad 12 de almacenamiento, en la cual se almacena código para un algoritmo de compresión. En ello, los medios 6 de enumeración, transformación y almacenamiento usan el algoritmo de compresión almacenado en la primera unidad 12 de almacenamiento para comprimir por separado cada elemento del conjunto de todos los estados posibles de visualizaciones de elementos base seguros antes de almacenarlas. Además, el tercer medio 4 comprende una segunda unidad 13 de almacenamiento, en la cual se almacena código para un algoritmo de descompresión, que es en particular la transformación inversa del algoritmo de compresión cuyo código está almacenado en la primera unidad 12 de almacenamiento, y los medios 9 de superposición mostrados en la figura 1 usan este algoritmo de descompresión para descomprimir los elementos comprimidos del conjunto de todos los estados posibles de las visualizaciones de elementos base seguros y después para superponer sucesivamente las visualizaciones de elementos base seguros, en particular las capas seguras que se corresponden con el estado real del al menos un

parámetro de entrada variable, de este modo generando la visualización segura del estado real del parámetro de entrada variable, en particular la velocidad del tren, velocidad mínima, velocidad máxima, y velocidad objetivo.

En ello, el algoritmo de compresión usado cuyo código está almacenado en la primera unidad 12 de almacenamiento es un algoritmo de tabla de búsqueda de color con codificación de longitud de secuencia, para sucesivamente extraer y comprimir los elementos respectivos.

Según la realización de la figura 1, para todos los estados posibles del al menos un parámetro de entrada variable hay también datos no críticos de seguridad a ser mostrados, también, en donde los datos no críticos de seguridad son transmitidos directamente al tercer medio 4. Además, el tercer medio 4 mostrado en la figura 1 comprende una tercera unidad 14 de almacenamiento no volátil para almacenar cada uno de los elementos base seguros descompuestos del conjunto de todos los estados posibles de visualizaciones de elementos base y una cuarta unidad 15 de almacenamiento para almacenar datos no críticos de seguridad. La figura 1 también muestra un controlador 16 de gráficos seguros, que gestiona la tercera unidad 14 de almacenamiento no volátil así como la cuarta unidad 15 de almacenamiento, para conmutar un flujo de datos gráficos entre los datos no críticos de seguridad y las capas críticas de seguridad. Por lo tanto, el controlador 16 de gráficos seguros puede gestionar las capas seguras él mismo, separando datos seguros y no seguros en la memoria del elemento de representación, y mostrar datos seguros encima de los datos no seguros.

En ello, según la realización de la figura 1, cada uno de los elementos del conjunto de todos los estados posibles de visualizaciones de elementos base seguros es almacenado en un área separada de la tercera unidad 14 de almacenamiento no volátil, para acelerar el tiempo de acceso para leer cada elemento del conjunto de datos críticos de seguridad extraídos de la tercera unidad 14 de almacenamiento no volátil.

La figura 2 ilustra un sistema 20 para la visualización segura de una información relevante para la seguridad según una segunda realización. En ello, idénticas características estructurales como en la realización mostrada en la figura 1 se identifican por símbolos de referencia idénticos.

Según la realización de la figura 2, el tercer medio 4 comprende solo una unidad para almacenar los datos no críticos de seguridad así como el conjunto de todos los estados posibles de visualizaciones de elementos base seguros, en particular una quinta unidad 21 de almacenamiento, que comprende un área 22 de almacenamiento no seguro para almacenar los datos no críticos de seguridad y un área 23 de almacenamiento seguro para almacenar las capas críticas de seguridad. La figura 2 también muestra un controlador 24 de gráficos conectado a la quinta unidad 21 de almacenamiento, para gestionar el flujo de datos gráficos. En particular, los datos críticos de seguridad son encriptados con una clave de encriptación conocida solo por el controlador 24 de gráficos seguros. Por lo tanto, el sistema no seguro puede ser un suministrador factible de datos seguros, añadiendo el coste de complejidad computacional y algorítmica aumentado, pero ahorrando un componente hardware. Los datos no críticos almacenados en el área 22 podrían también ser derivados desde una fuente que fuera completamente externa al sistema.

Además, según la realización de la figura 2, el medio 7 de transmisión del segundo medio 3 comprende un medio 25 de inspección para realizar una inspección relevante para la seguridad o verificación de los datos almacenados, por ejemplo, mediante inspección manual, semiautomática o automática. Esto está destinado a mejorar la seguridad, servir como una así llamada barrera de seguridad, o introducir seguridad mediante algún tipo de inspección, en particular una barrera de seguridad que cruza desde un dominio no seguro a uno seguro. Durante el paso de inspección/verificación se podrían añadir firmas para la autentificación.

En ello, aunque la visualización segura del estado real del al menos un parámetro de entrada variable se puede generar mediante la transformación inversa sucesiva y opcional y entonces representación y superposiciones de los elementos base seguros, las capas, de los datos críticos de seguridad originales descompuestos, el sistema 20 puede además comprender un segundo medio 26 de inspección para realizar los siguiente: Cada una de las visualizaciones de elementos base determinadas del conjunto de todos los estados posibles de visualizaciones de elementos base seguros correspondientes con el estado real del al menos un parámetro de entrada variable es comparada con una versión del elemento base seguro respectivo del conjunto de todos los estados posibles de visualizaciones de elementos base seguros que son mostrados eficazmente mostrados. Además, se proporciona una reacción enfocada en la seguridad, si al menos una de las visualizaciones de elementos base seguros requeridas no es idéntica a la versión del elemento base seguro respectivo que es mostrada eficazmente. En ello, la comparación se puede llevar a cabo en una de muchas formas adecuadas, por ejemplo por comparación de ancho de píxel, por ejemplo píxel a píxel, o por partes relevantes de los datos de píxel tales como para solo ciertos componentes de color, o mediante el cálculo de sumas de comprobación de las capas esperadas y las reales, y comparando las sumas de comprobación, o haciendo algún tipo de correspondencia de patrones. Mediante la comprobación de un elemento del conjunto de todos los estados posibles de visualizaciones de elementos base contra una versión del elemento respectivo del conjunto de todos los estados posibles de visualizaciones de elementos base que son mostrados eficazmente, es necesario admitir una tolerancia, y proporcionar una reacción enfocada en la seguridad si una capa esperada no es idéntica a la versión de la capa respectiva que es mostrada eficazmente, se introduce una alta eficiencia y arquitectura de visualización segura con dos canales, donde el canal hacia delante hace la visualización real y el canal de verificación proporciona o mejora la integridad en un modo

relevante para la seguridad mediante la comparación de la visualización actual con la visualización esperada. Si no está disponible el acceso a las representaciones de elementos base separados o capas del canal hacia delante para la verificación del canal, la verificación del canal puede representar la visualización del al menos un parámetro de entrada variable mediante la representación sucesiva y superposición de los elementos base seguros, las capas, de los datos críticos de seguridad originales descompuestos en una memoria intermedia sombra, y puede entonces comparar la visualización resultante con lo que realmente se está mostrando, otra vez con un medio de comparación adecuado, tal como algún tipo de comparación de ancho de píxel, comparación de suma de comprobación o correspondencia de patrones, por ejemplo.

En ello, la reacción enfocada en la seguridad puede ser apagar el medio 10 de representación. En ello, el medio 10 de representación puede apagarse completamente o hasta un cierto grado. Sin embargo, todos los métodos que indican claramente un fallo crítico de seguridad a un observador son adecuados como reacciones enfocadas en la seguridad, por ejemplo proporcionar marcado de datos, enmascaramiento o distorsión o apagado del sistema todo junto.

La figura 3 ilustra un diagrama de flujo de un método 30 para la visualización segura de una información relevante para la seguridad según una tercera realización.

Como se muestra en la figura 3, en un primer paso 31, para todos los estados posibles de al menos un parámetro de entrada variable, una visualización segura de al menos un parámetro de entrada variable se descomponen en sus elementos base seguros, sus capas seguras, en donde cada uno de los elementos base seguros pueden ser estáticos o representar la información de visualización en al menos un parámetro de entrada variable.

Como además se ilustra, en un segundo paso 32, para cada uno de los elementos base seguros descompuestos y, por lo tanto, para cada una de las capas seguras, se enumera un conjunto de todos los estados posibles de visualización de elementos base seguros y se almacena en un formato adecuado en donde el conjunto de todos los estados posibles de la visualización de elementos base seguros comprende la visualización de un elemento seguro en las visualizaciones seguras de al menos un parámetro de entrada variable para todos los estados posibles de al menos un parámetro de entrada variable. Por ejemplo, asumiendo que el al menos un parámetro de entrada variable incluye la velocidad actual de un tren, entonces las visualizaciones de todos los estados posibles de la velocidad actual del tren se enumeran y almacenan en un formato adecuado.

En un tercer paso 33, para todos los estados posibles del al menos un parámetro de entrada variable cada uno de los elementos base seguros descompuestos y, por lo tanto, para cada capa segura, se transmite el conjunto de todos los estados posibles de visualización de elementos base seguros generados mediante la descomposición de visualizaciones seguras a un sistema objetivo que proporciona la visualización segura en tiempo de ejecución.

En un cuarto paso 34, un estado real del al menos un parámetro de entrada variable se introduce en el sistema objetivo, y para cada parámetro de entrada variable se determinan y se buscan en el respectivo conjunto de todos los estados posibles de visualización del elemento seguro el elemento base seguro correspondiente, la capa segura, y su estado correcto.

Además, como se muestra en la figura 3, cada capa segura correspondiente, en particular la visualización de cada elemento base seguro correspondiente, es representada desde el conjunto de todos los estados posibles de visualizaciones de elementos base seguros en un quinto paso 35, una tras la otra, una superponiéndose a la anterior. Este quinto paso 35, en particular la representación y superposición de los estados de elementos base seguros correctos, genera de forma segura la visualización segura original del estado real del al menos un parámetro de entrada variable, que es entonces mostrado en un elemento de representación.

Así, el método 30 de la figura 3 se basa en datos de imagen extraídos en vez del uso de sumas de comprobación. En particular, la visualización segura se descompone en las fuentes respectivas, que se pueden realizar durante el proceso de desarrollo. En ello, una imagen es extraída tras la otra formando de ese modo capas, cada una de las cuales es luego, durante el tiempo de ejecución, mostrada encima de la otra, generando de ese modo una visualización segura del al menos un parámetro de entrada variable. Si el espacio de color usado presenta un canal alfa, la mezcla alfa se puede usar para hacer la superposición más poderosa. El enmascarado alfa puede usarse opcionalmente en cada capa, independientemente del espacio de color usado. Dado que la máscara alfa solo tiene un bit por píxel, es rápido y eficiente de almacenar, sin embargo puede simplificar significativamente algunos tipos de visualizaciones, especialmente cuando la máscara alfa a aplicar puede depender de uno o más parámetros de entrada variables.

Las figuras 4A a C ilustran una visualización segura de la velocidad de un tren en un cuadro de un velocímetro según la presente invención.

En particular, la figura 4A ilustra un cuadro 40 de un velocímetro que representa la velocidad de un tren.

Como se muestra en la figura 4A, el cuadro 40 de un velocímetro comprende una imagen 41 base en la forma de un fondo opaco e información opaca alfanumérica con muchos píxeles transparentes 42, 43, 44, 45 en el fondo opaco. En ello, la información alfanumérica 42, 43, 44, 45 incluyen un puntero 42 que indica la velocidad real del tren, una

primera barra 43 que indica una velocidad objetivo deseada del tren, una segunda barra 44 que indica la velocidad mínima del tren y un triángulo 45 que indica la velocidad máxima del tren. Así, la figura 4A muestra un velocímetro que tiene cuatro fuentes de entrada. Además, el cuadro 40 de un velocímetro mostrado cumple con los requisitos del Sistema de Control de Trenes Europeos (ETCS).

En ello, para evitar un fallo relevante para la seguridad, tiene que asegurarse una visualización segura de la velocidad actual del tren, velocidad mínima, velocidad máxima y velocidad objetivo. En ello, los métodos conocidos se basan en el cálculo de sumas de comprobación para una secuencia de datos de imagen que representan la velocidad actual del tren, velocidad mínima, velocidad máxima y velocidad objetivo y compara la suma de comprobación calculada con una suma de comprobación de referencia. Entonces se proporciona una reacción enfocada en la seguridad, si la suma de comprobación no es idéntica a la suma de comprobación de referencia.

Sin embargo, considerando el velocímetro mostrado en la figura 4A, que muestra la velocidad actual de un tren, velocidad mínima, velocidad máxima y velocidad objetivo, que tiene cuatro fuentes de entradas, si cada una de las fuentes tiene 10 bits de resolución, el velocímetro tendría un total de 2^{40} estados posibles. Además, si cada suma de comprobación tuviera cuatro bytes, solo los datos de sumas de comprobación sumaría un total de 4 Tera bytes de datos de sumas de comprobación, lo que sería mucho más de lo que cualquier sistema incorporado podría proporcionar.

Aun sí un sistema incorporado pudiera presentar tal enorme cantidad de memoria, el cálculo previo de las sumas de comprobación sería impracticable. Considerando que un ordenador personal pudiera calcular 10 sumas de comprobación por segundo, le llevaría 34865 años calcular 2^{40} sumas de comprobación, lo que sería inaceptable.

Por lo tanto, según la presente invención, como se muestra en la figura 4B, cada uno de los elementos 41, 42, 43, 44, 45 es extraído por separado formando de ese modo capas seguras, cada una de las cuales será después, en tiempo de ejecución, mostrada encima de las otras, generando de este modo una visualización segura de la velocidad actual del tren, velocidad mínima, velocidad máxima y velocidad objetivo. Así, según la presente invención, la visualización segura se descompone en las fuentes respectivas, que pueden estar hechas durante el proceso de desarrollo. Por lo tanto, para un velocímetro simple con 24 bits de profundidad de píxel, que muestra por ejemplo la velocidad actual, velocidad mínima, velocidad máxima y velocidad objetivo, teniendo así cuatro fuentes de entrada, en donde los datos críticos de seguridad son posibles estados de las capas, en particular la información alfanumérica 42, 43, 44, 45, solo hay $2^0 + 2^{10} + 2^{10} + 2^{10} + 2^{10}$ estados posibles para la visualización del velocímetro. Por lo tanto, considerando 25k bytes para la imagen base comprimida y aproximadamente 3k bytes de datos comprimidos por capa, un almacenamiento total de 25k bytes + 2^{10} * 3k bytes + 2^{10} * 3k bytes + 2^{10} * 3k bytes + 2^{10} * 3k bytes y, por lo tanto, se requiere una cantidad total de aproximadamente 12M bytes, lo que es sobre 333333 veces mejor que una suma total de 4 Tera bytes de datos de sumas de comprobación. Además, en efecto la extracción de los datos de imagen puede llevar más tiempo que el cálculo de las sumas de comprobación, pero considerando un ordenador personal que ejecuta 1 extracción por segundo, se requiere un tiempo de computación de 4097 segundos para la extracción de todos los datos, lo cual es mucho mejor que un tiempo de computación de 34865 años para calcular 2^{40} sumas de comprobación. Por lo tanto, se proporciona un método mejorado para la visualización segura de información relevante para la seguridad en un elemento de presentación sobre requisitos de almacenamiento y tiempo computacional.

La figura 4C ilustra un paso de superposiciones sucesivas de los elementos 41, 42, 43, 44, 45 extraídos, generando de este modo la visualización 40 segura del cuadro de un velocímetro real.

Las figuras 5A y B ilustran el uso de enmascaramiento alfa según la presente invención.

En particular, la figura 5A ilustra una barra 50 que indica el área de velocidad objetivo de un tren, en donde un borde 51 izquierdo de la barra 50 indica el valor de velocidad mínima del tren de aproximadamente 40km/h y un borde 52 derecho de la barra 50 indica el valor de velocidad máxima del tren de aproximadamente 80km/h.

Por lo tanto, la barra 50 mostrada depende de dos parámetros de entrada variables. Así, aun si ésta barra 50 fuera un elemento base separado y, por lo tanto, una capa segura, el valor de la velocidad mínima del tren y el valor de la velocidad máxima del tren no se podrían separar el uno del otro, y el número de estados se multiplicaría.

Por lo tanto, una máscara alfa binaria adicional se puede usar por capa, en particular una máscara alfa de 1 bit por píxel. En ello, una máscara alfa binaria denota una máscara de supresión que es aplicada por capa. En ello, un bit en la máscara alfa se corresponde con un píxel en la capa, en donde si el bit es 0 entonces el píxel correspondiente será simplemente tratado como si tuviera un valor A de 0.

La figura 5B ilustra una descomposición de la barra 50 mediante el enmascarado alfa.

Como se muestra en la figura 5B, usando el enmascarado alfa la barra 50 se puede visualizar dependiendo del valor de velocidad máxima del tren y una máscara 53 alfa es dependiente de la velocidad mínima del tren. Primero, la barra se dibuja desde 0km/h a 80km/h, y entonces la máscara 53 alfa es aplicada para borrar la parte entre 0km/h y 40km/h, representando la visualización prevista de una barra en un intervalo entre 40km/h y 80km/h. Dado que la visualización se ha descompuesto en dos pasos, los estados se han sumado en vez de multiplicado.

REIVINDICACIONES

1. Método para la visualización segura de información relevante para la seguridad, comprendiendo el método (30) los siguientes pasos:

- para todos los estados posibles de al menos un parámetro de entrada variable, descomponer una visualización segura del al menos un parámetro de entrada variable en sus elementos (31) base seguros;

- para cada uno de los elementos base seguros descompuestos, enumerar y almacenar un conjunto de todos los posibles estados de visualizaciones de elementos base seguros (32);

- para cada uno de los elementos base seguros descompuestos, transmitir el conjunto de todos los estados posibles de visualizaciones de elementos base seguros a un sistema objetivo que proporciona visualización segura en tiempo de ejecución (33);

- para cada uno del al menos un parámetro de entrada variable introducir un estado real del al menos un parámetro de entrada variable en el sistema objetivo y, para cada uno del al menos un parámetro de entrada variable, determinar una visualización de elemento base seguro correspondiente al estado real del al menos un parámetro de entrada variable y su estado correcto para el conjunto de todos los estados posibles de la visualización (34) de elemento base seguro;

- sucesivamente representar y superponer cada uno de las visualizaciones de elementos base seguros correspondientes encima de las otras en un medio de representación del sistema objetivo, generando de este modo una visualización segura del estado real del al menos un parámetro (35) de entrada variable.

2. El método según la reivindicación 1, en donde el paso de enumerar y almacenar un conjunto de todos los estados posibles de visualizaciones de elementos base seguros para cada uno de los elementos (32) base seguros descompuestos comprende transformar cada elemento del conjunto de todos los estados posibles de visualizaciones de elementos base seguros en un formato adecuado antes de almacenar los elementos base seguros descompuestos, y en donde el paso de representar sucesivamente y superponer cada una de las visualizaciones de elementos base seguros encima de las otras en un medio de representación en el sistema objetivo, generando de ese modo una visualización segura del estado real del al menos un parámetro (35) de entrada variable comprende el uso de transformación inversa respectiva.

3. El método según la reivindicación 2, en donde el paso de transformar cada elemento del conjunto de estados posibles de visualizaciones de elementos base seguros en un formato adecuado comprende usar un algoritmo de compresión y en donde la transformación inversa respectiva es un algoritmo de descomprensión respectivo.

4. El método según la reivindicación 3, en donde el algoritmo de compresión es un algoritmo de tabla de búsqueda de color con codificación de longitud de secuencia.

5. El método según la reivindicación 2, en donde el paso de transformar cada elemento del conjunto de todos los estados posibles de visualizaciones de elementos base seguros en un formato adecuado comprende transformar cada uno de los elementos del conjunto de todos los estados posibles de visualizaciones de elementos base seguros en un formato de gráficos de vector y en donde la transformación inversa respectiva usada en el paso de representar sucesivamente y superponer cada una de las visualizaciones de elementos base seguros encima de las demás en un medio de representación en el sistema objetivo, generando de este modo una visualización segura del estado real del al menos un parámetro (35) de entrada variable comprende interpretar el formato de gráficos de vector.

6. El método según una de las reivindicaciones 1 a 5, en donde el paso de enumerar y almacenar un conjunto de todos los estados posibles de visualizaciones de elementos base seguros para cada uno de los elementos (32) base seguros descompuestos comprende el paso de almacenar el conjunto de todos los estados posibles de visualizaciones de elementos base seguros en un espacio de color que está particularmente bien adaptado para la tarea de visualización.

7. El método según una de las reivindicaciones 1 a 6, en donde para todos los estados posibles del al menos un parámetro de entrada variable la visualización segura del al menos un parámetro de entrada variable comprende datos no críticos de seguridad, en donde los datos no críticos de seguridad son transmitidos al sistema objetivo y en donde el paso de representar sucesivamente y superponer cada uno de las visualizaciones de elementos base seguros correspondiente encima de las demás en un medio de representación del sistema objetivo, generando de este modo una visualización segura del estado real del al menos un parámetro (35) de entrada variable comprende:

- representar y mostrar los datos no críticos de seguridad;

- superponer sucesivamente los datos no críticos de seguridad mostrados con cada una de las visualizaciones de elementos base seguros correspondientes.

8. El método según una de las reivindicaciones 1 a 7, en donde el paso de enumerar y almacenar un conjunto de todos los estados posibles de visualizaciones de elementos base seguros para cada uno de los elementos (32) base seguros descompuestos comprende el paso de almacenar el conjunto de todos los estados posibles de visualizaciones de elementos base seguros en un espacio de color RGBA que en particular presenta un canal alfa, y en donde el paso de representar sucesivamente y superponer cada una de las visualizaciones de elementos base seguros correspondientes encima de las demás en un medio de representación del sistema objetivo, generando de este modo una visualización segura del estado real del al menos un parámetro (35) de entrada variable comprende usar mezcla alfa.

9. El método según una de las reivindicaciones 1 a 8, en donde el paso de enumerar y almacenar un conjunto de todos los estados posibles de visualizaciones de elementos base seguros para cada uno de los elementos (32) base seguros descompuestos comprende usar enmascarado alfa, y en donde el paso de representar sucesivamente y superponer cada una de las visualizaciones de elementos base seguros correspondientes encima de las demás en un medio de representación del sistema objetivo, generando de este modo una visualización segura del estado real del al menos un parámetro (35) de entrada variable comprende usar enmascarado alfa para generar la visualización de elementos base seguros.

10. El método según una de las reivindicaciones 1 a 9, en donde el paso de enumerar y almacenar un conjunto de todos los estados posibles de visualizaciones de elementos base seguros para cada uno de los elementos (32) base seguros descompuestos comprende usar un orden z no estático y en donde el paso de representar sucesivamente y superponer cada una de las visualizaciones de elementos base seguros correspondientes encima de las demás en un medio de representación del sistema objetivo, generando de este modo una visualización segura del estado real del al menos un parámetro (35) de entrada variable comprende usar el orden z no estático para generar la visualización de elementos base seguros.

11. El método según una de las reivindicaciones 1 a 10, en donde el paso de transmitir el conjunto de todos los estados posibles de visualizaciones de elementos base seguros a un sistema objetivo que proporciona visualización segura en tiempo de ejecución para cada uno de los elementos (33) base seguros descompuestos, comprende asegurar la integridad de los datos de los datos transmitidos y/o añadir un paso de inspección manual, semiautomática o automática para mejorar la integridad de seguridad de los datos.

12. El método según una de las reivindicaciones 1 a 11, en donde el método (30) además comprende:

- comparar cada uno de las visualizaciones de elementos base seguros con una versión del elemento base seguro que es mostrada eficazmente;

- proporcionar una reacción enfocada en la seguridad, si uno de las visualizaciones de elementos base seguros no es idéntica a la versión del elemento base seguro correspondiente que es mostrada eficazmente.

13. El método según la reivindicación 12, en donde la reacción enfocada en la seguridad comprende apagar el medio de representación del sistema objetivo.

14. Sistema para la visualización segura de información relevante para la seguridad comprendiendo un primer medio (2), que comprende medios (5) de descomposición para realizar para todos los estados posibles de al menos un parámetro de entrada variable la descomposición de una visualización segura del al menos un parámetro de entrada variable en sus elementos base seguros, y unos medios (6) de enumeración, transformación y almacenamiento para realizar para cada uno de los elementos base seguros descompuestos enumeración y almacenamiento de un conjunto de todos los estados posibles de visualizaciones de elementos base seguros, y un segundo medio (3), que comprende un medio (7) de transmisión para cada uno de los elementos base seguros descompuesto el conjunto de todos los estados posibles de visualizaciones de elementos base seguros a un tercer medio (4) que proporciona visualización segura en tiempo de ejecución, en donde para cada uno del al menos un parámetro de entrada variable un estado real del al menos un parámetro de entrada variable es introducido en el tercer medio (4) y en donde el tercer medio (4) comprende un medio (8) de determinación para determinar para cada uno del al menos un parámetro de entrada variable la visualización de elemento base seguro correspondiente que se corresponde con el estado real del al menos un parámetro de entrada variable y su estado correcto del conjunto de todos los estados posibles de visualizaciones de elementos base seguros, y un medio (9) de superposición para representar y superponer sucesivamente cada una de las visualizaciones de elementos base seguros encima de los demás en un medio (10) de representación del tercer medio(4), generando de este modo una visualización segura del estado real del al menos un parámetro de entrada variable.

15. El sistema según la reivindicación 14, en donde para todos los estados posibles del al menos un parámetro de entrada variable la visualización segura del al menos un parámetro de entrada variable comprende datos no críticos de seguridad, en donde los datos no críticos de seguridad son transmitidos al tercer medio (4) mediante el medio (7) de transmisión y en donde el tercer medio (4) comprende un medio para incorporar los datos no críticos de seguridad en los datos de visualización que son mostrados en el medio (10) de visualización.

16. El sistema según la reivindicación 15, en donde el tercer medio (4) comprende una unidad (14) de almacenamiento no volátil para almacenar cada uno de los elementos base seguros descompuestos el conjunto de

todos los estados posibles de visualizaciones de elementos base seguros, una cuarta unidad (15) de almacenamiento para almacenar los datos no críticos de seguridad y un controlador (16) de gráficos para gestionar la tercera unidad (14) de almacenamiento no volátil y la cuarta unidad (15) de almacenamiento mediante la conmutación de un flujo de datos entre la tercera unidad (14) de almacenamiento no volátil y la cuarta unidad (15) de almacenamiento en tal forma, que los datos no críticos de seguridad se pueden representar y mostrar primero y son entonces superpuestos con cada una de las visualizaciones de elementos base seguros correspondientes.

17. El sistema según la reivindicación 15, en donde el tercer medio (4) comprende una unidad (21) de almacenamiento, que comprende un área (23) de almacenamiento seguro para almacenar para cada uno de los elementos base seguros descompuestos el conjunto de todos los estados posibles de visualizaciones de elementos base seguros y un área (22) de almacenamiento no seguro para almacenar los datos no críticos de seguridad y un controlador (24) de gráficos para gestionar la quinta unidad (21) de almacenamiento mediante la conmutación de un flujo de datos entre el área (23) de almacenamiento seguro de la quinta unidad (21) de almacenamiento y el área (22) de almacenamiento no seguro de la quinta unidad (21) de almacenamiento en tal modo, que los datos no críticos de seguridad se pueden representar y mostrar primero y entonces son superpuestos con cada una de las visualizaciones de elementos base seguros correspondientes.

18. El sistema según una de las reivindicaciones 14 a 17, en donde el primer medio (2), el segundo medio (3) y el cuarto medio (4) se combinan en una unidad computacional.

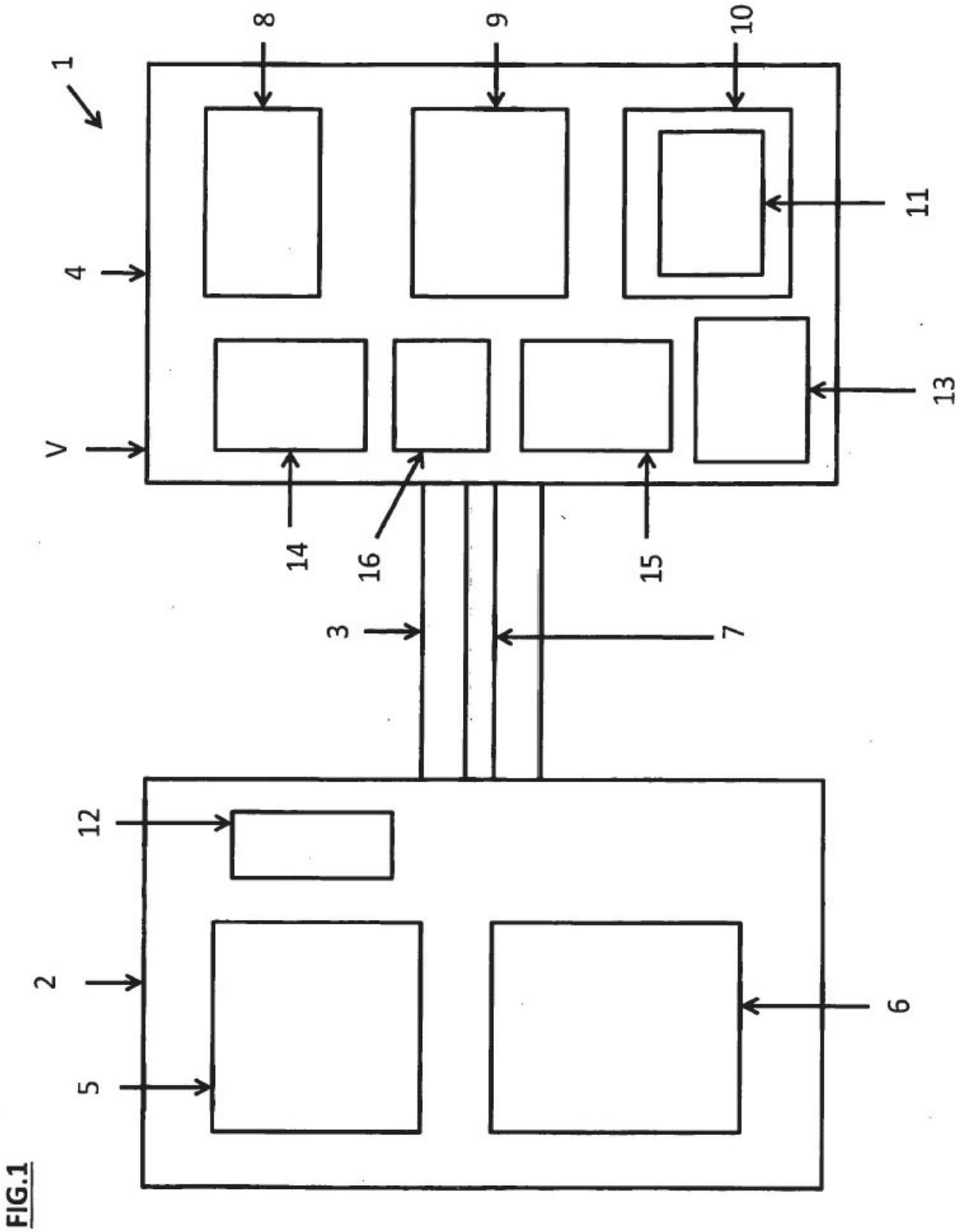


FIG.1

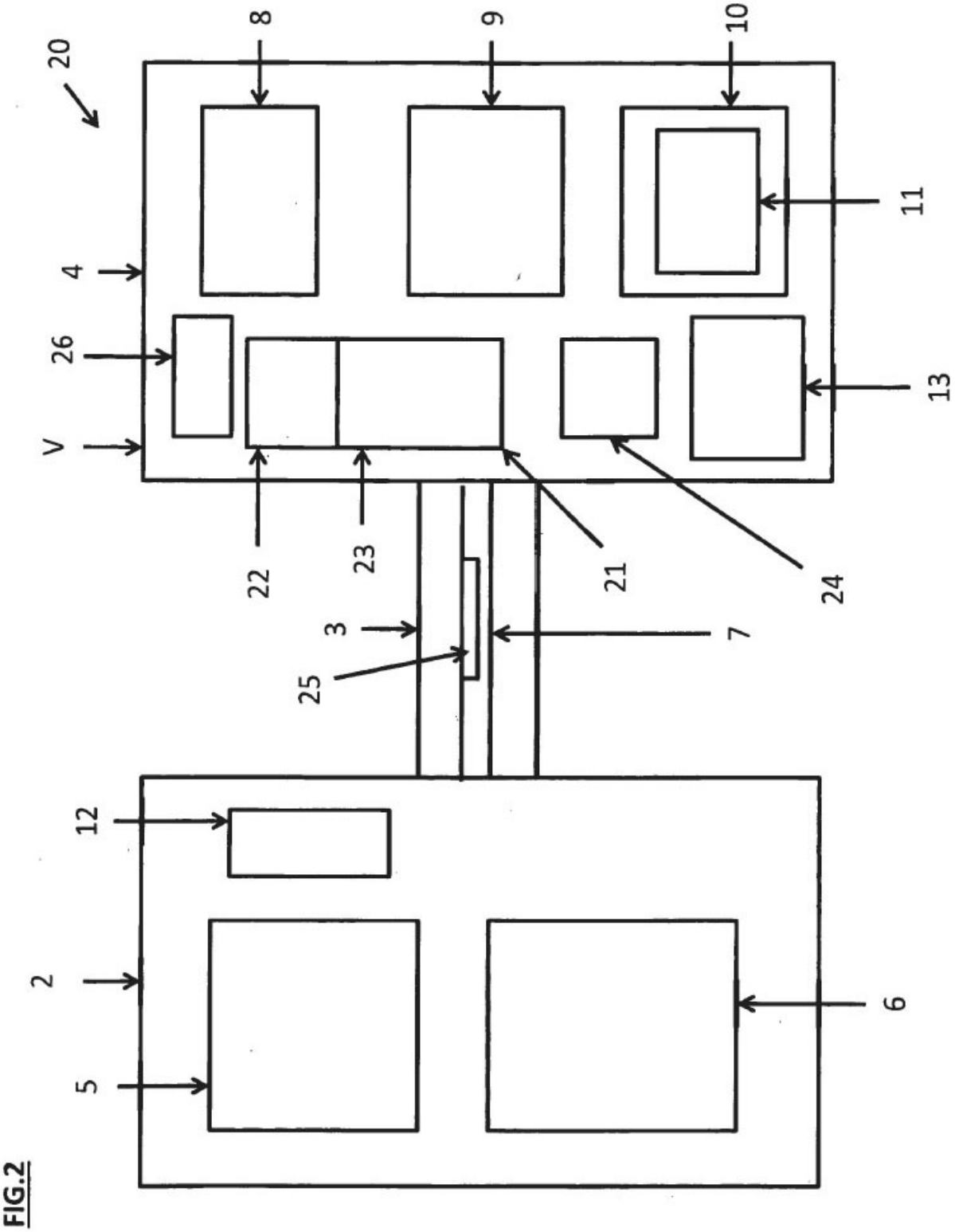
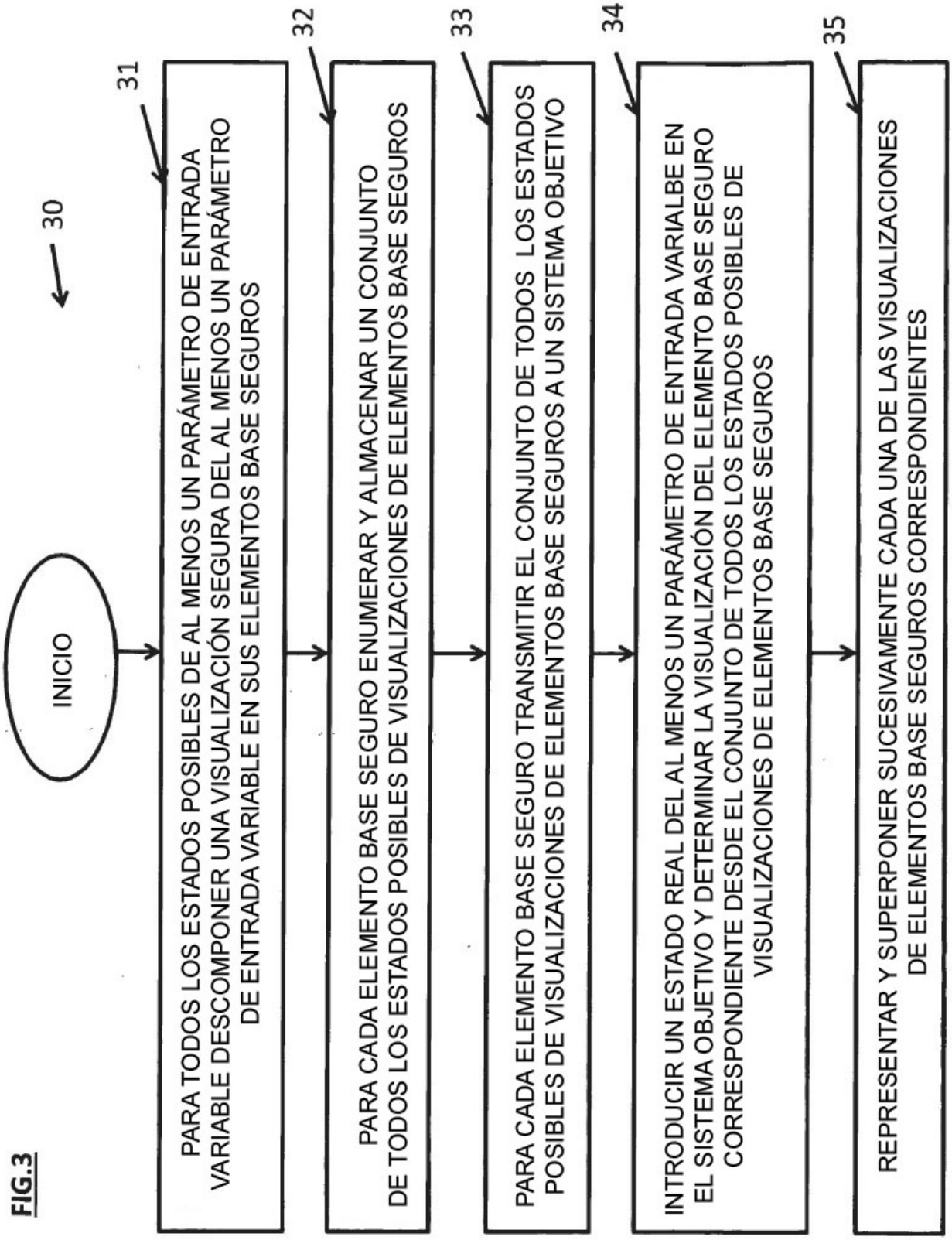


FIG.2

FIG.3


30
INICIO
31
PARA TODOS LOS ESTADOS POSIBLES DE AL MENOS UN PARÁMETRO DE ENTRADA VARIABLE DESCOMPONER UNA VISUALIZACIÓN SEGURA DEL AL MENOS UN PARÁMETRO DE ENTRADA VARIABLE EN SUS ELEMENTOS BASE SEGUROS
32
PARA CADA ELEMENTO BASE SEGURO ENUMERAR Y ALMACENAR UN CONJUNTO DE TODOS LOS ESTADOS POSIBLES DE VISUALIZACIONES DE ELEMENTOS BASE SEGUROS
33
PARA CADA ELEMENTO BASE SEGURO TRANSMITIR EL CONJUNTO DE TODOS LOS ESTADOS POSIBLES DE VISUALIZACIONES DE ELEMENTOS BASE SEGUROS A UN SISTEMA OBJETIVO
34
INTRODUCIR UN ESTADO REAL DEL AL MENOS UN PARÁMETRO DE ENTRADA VARIALBE EN EL SISTEMA OBJETIVO Y DETERMINAR LA VISUALIZACIÓN DEL ELEMENTO BASE SEGURO CORRESPONDIENTE DESDE EL CONJUNTO DE TODOS LOS ESTADOS POSIBLES DE VISUALIZACIONES DE ELEMENTOS BASE SEGUROS
35
REPRESENTAR Y SUPERPONER SUCESIVAMENTE CADA UNA DE LAS VISUALIZACIONES DE ELEMENTOS BASE SEGUROS CORRESPONDIENTES

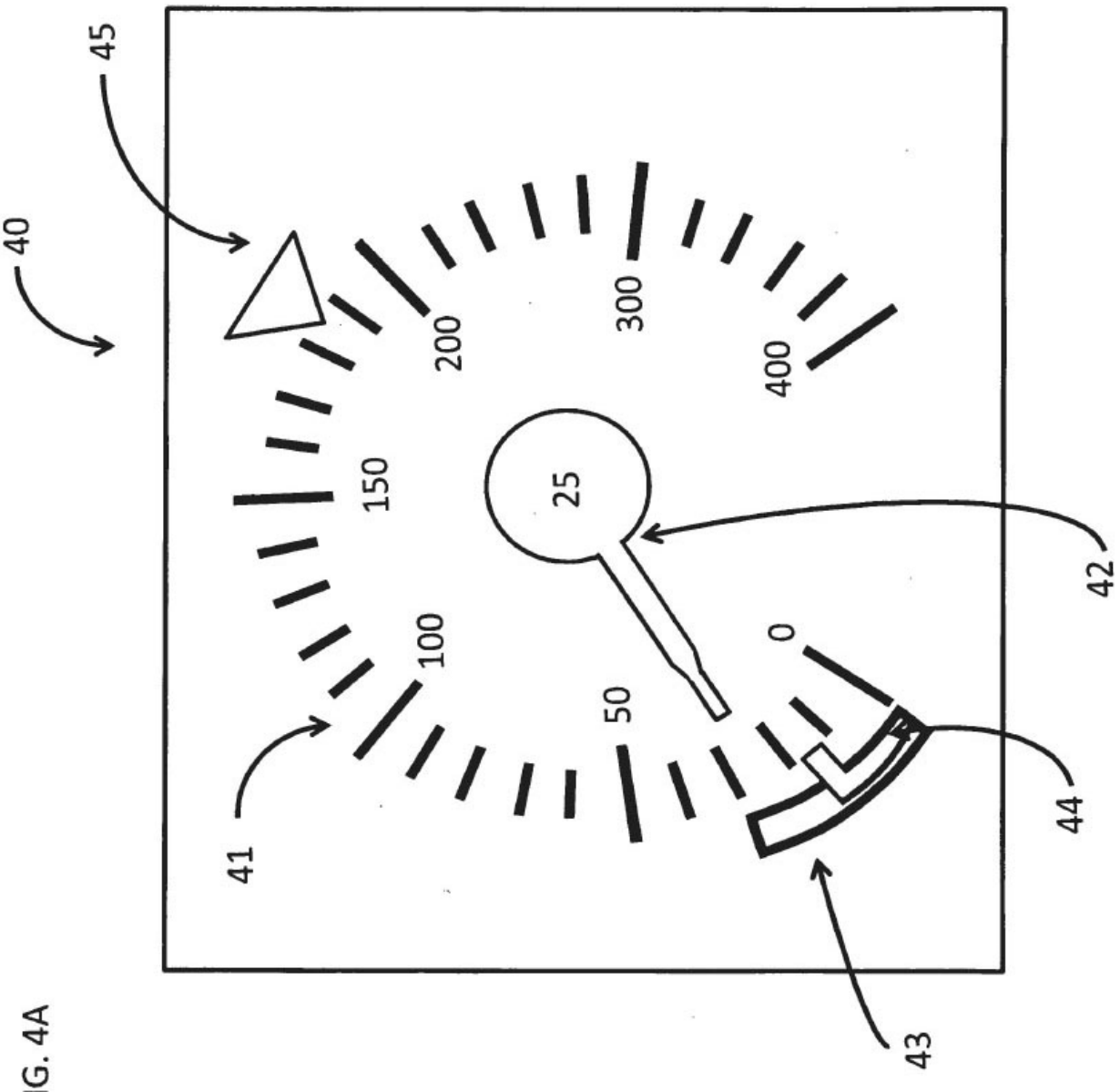


FIG. 4A

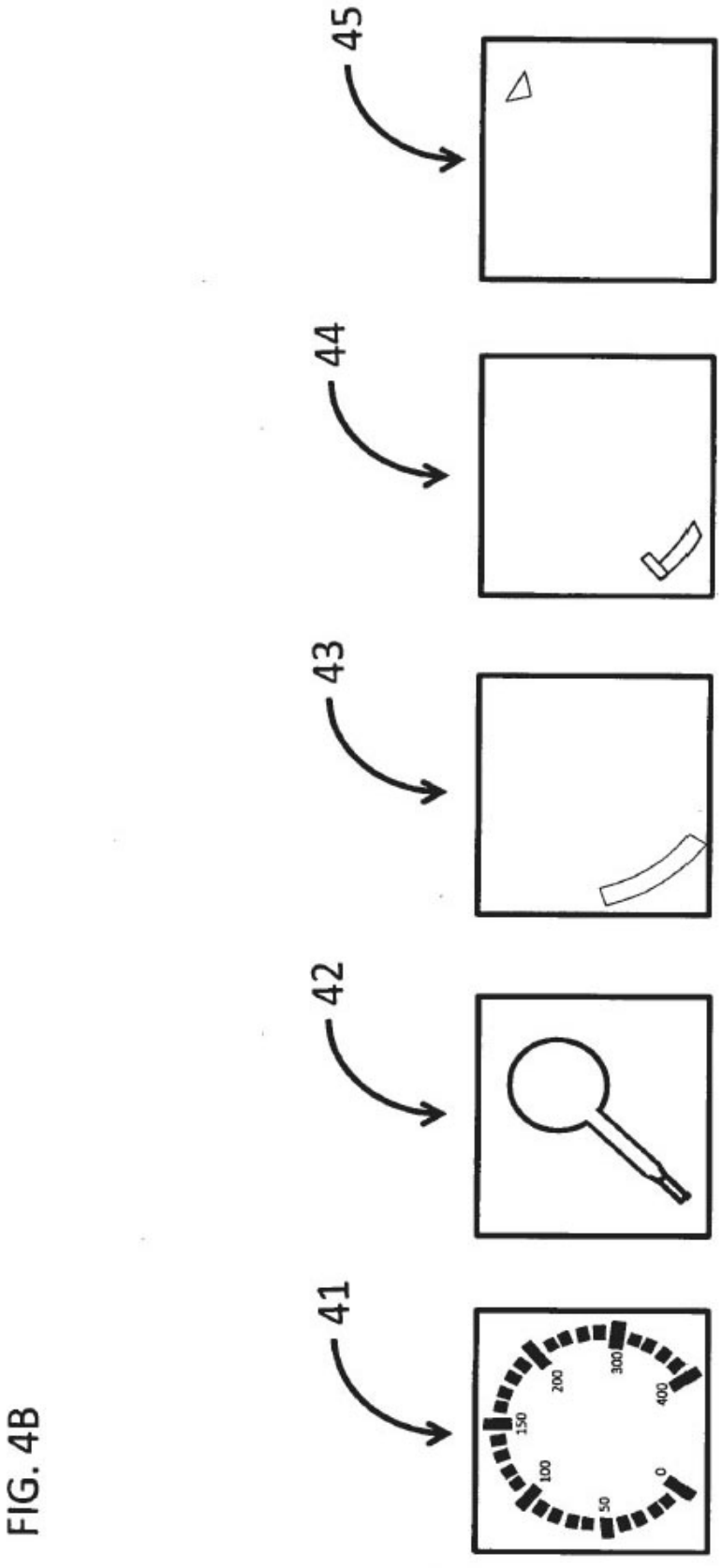


FIG. 4B

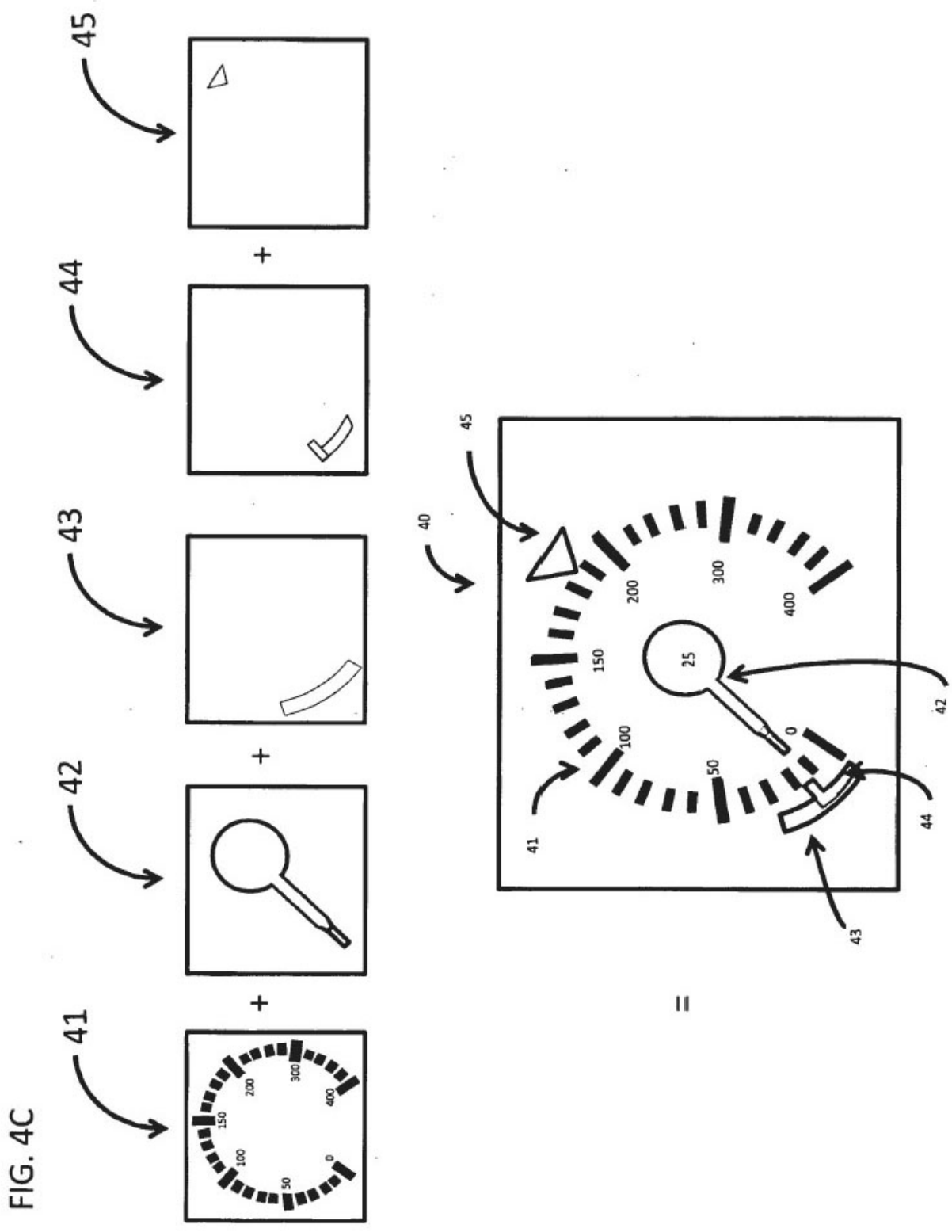
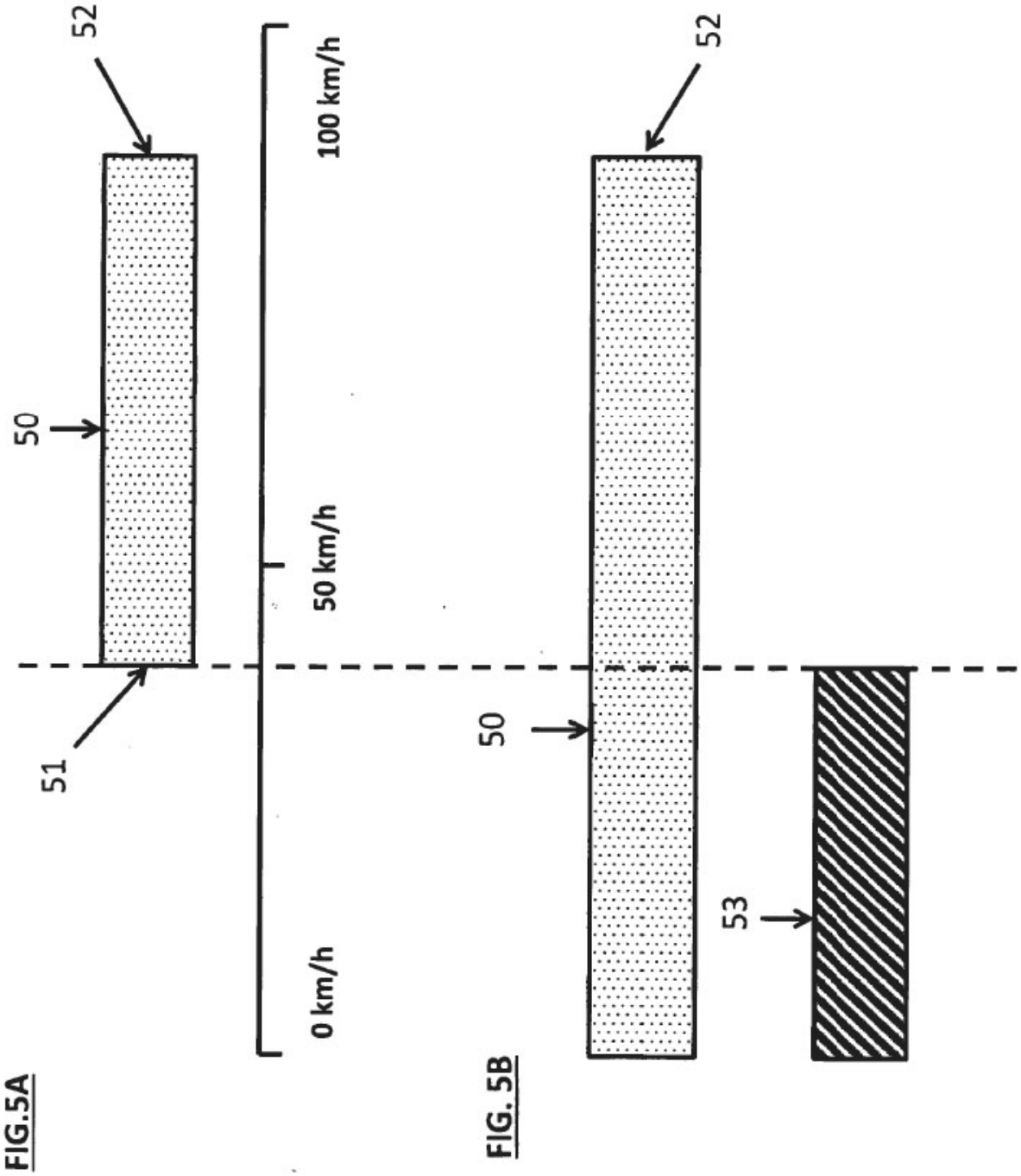


FIG. 4C


52
100 km/h
50
50 km/h
51
0 km/h
FIG.5A
52
50
53
FIG. 5B