(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 561 311**

(51) Int. CI.:

G05B 23/02 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.05.2013 E 13166291 (8)**

(97) Fecha y número de publicación de la concesión europea: **09.12.2015 EP 2674826**

(54) Título: **Validación y visualización de análisis de fallos**

(30) Prioridad:

15.06.2012 US 201213524173

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.02.2016

(73) Titular/es:

THE BOEING COMPANY (100.0%)
100 North Riverside Plaza
Chicago, IL 60606-2016, US

(72) Inventor/es:

PETRI, TYLER JUNICHI;
FOGARTY, DANIEL J.;
JONES, DAVID HARDING;
MORAN, ALLISON y
KING, KEVIN NICHOLAS

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Validación y visualización de análisis de fallos

ANTECEDENTES

La presente descripción hace referencia de manera general a presentaciones de datos de análisis de fallos y, en particular, a presentaciones diferenciadas de datos de análisis de fallos para diferentes implicados de una manera que facilite la consistencia de los datos entre las presentaciones.

Los avances en el diseño de muchos sistemas complejos tales como los de las industrias aeroespacial, de automoción, marina y electrónica han conducido al desarrollo de numerosos sistemas dependientes entre sí. A menudo, los fallos o averías de uno o más de estos sistemas afectan, de manera directa o indirecta, a otros sistemas. Además, a menudo es necesario, como parte de un proceso de certificación, un análisis de estos fallos/averías y de sus efectos directos e indirectos. Típicamente estos análisis son realizados manualmente por grupos de analistas de sistemas, sin referencia a un sistema o proceso capaz de facilitar dichos análisis.

Los datos procedentes de los análisis de fallos se pueden representar como representaciones gráficas que transmiten la información con mayor claridad que el texto. Los registros (por ejemplo, representaciones gráficas, planes de pruebas) desarrollados a partir de estos datos se pueden utilizar para evaluar la aceptabilidad de análisis de fallos con sistemas federados así como con sistemas integrados. En la actualidad, estos registros pueden ser creados por diferentes organizaciones de ingeniería, cada una con su propia perspectiva y sus propios intereses, por medio de métodos manuales, que consumen mucho tiempo, y los cuales pueden ser propensos a errores y pueden carecer de consistencia y de integración y controles suficientes.

En programas de aeronaves con sistemas federados, los análisis de fallos pueden ser sencillos, y suelen involucrar a un número limitado de sistemas con efectos en cascada a nivel de la aeronave fáciles de entender. Los registros utilizados para evaluar la aceptabilidad de los análisis de fallos con sistemas federados suelen estar limitados a lo que un experto en sistemas individual considera suficiente, y la evaluación de fallos puede ser realizada por un número limitado de gente.

Por otro lado, cuando los análisis de fallos se realizan sobre sistemas complejos de la aeronave con arquitecturas muy integradas, dichos análisis de fallos pueden involucrar a muchos sistemas con efectos complejos en cascada e impactos a nivel de la aeronave que no son fáciles de entender sin una imagen completa del evento. Para realizar una evaluación válida de un análisis de fallos en este entorno, hay muchos más implicados que deben estar involucrados que los que serían necesarios para evaluar un fallo en el entorno de un sistema federado. Cada uno de estos implicados puede estar particularmente interesado en una presentación concreta del evento de fallo (todas las cuales son válidas). Todas las presentaciones del evento de fallo se deben considerar junto con todos los implicados para garantizar que se ha realizado una evaluación correcta y que la aeronave mantendrá un nivel de seguridad adecuado. Las prácticas más antiguas son suficientes para aeronaves con sistemas federados (por ejemplo, los expertos en sistemas individuales utilizan presentaciones que ellos consideran suficientes para evaluar escenarios de fallo normalmente contenidos dentro de su sistema), pero no son suficientes para la actual generación de aeronaves cuando se trata de evaluar fallos.

Existe un desafío en la creación de estos productos/registros/presentaciones, los cuales típicamente han sido creados de forma manual en diversos formatos por diferentes grupos. Los desafíos son tres – mantener consistencia entre los diferentes productos, reducir los recursos/el tiempo invertidos en el desarrollo de los productos, y crear alertas de cambios.

La Patente GB2275559 describe un sistema que valida datos de alarma.

BREVE SUMARIO

Por lo general, las realizaciones de ejemplo de la presente invención están dirigidas a un sistema para la integración de datos de fallo para diferentes presentaciones de análisis de fallos, y a un método y a un medio de almacenamiento informático correspondientes. De acuerdo con realizaciones de ejemplo, a partir de datos de fallo generados a partir de análisis de fallos se pueden producir de manera automática presentaciones de casos de fallo, lo cual puede reducir, e incluso eliminar, errores/malas interpretaciones asociados a su producción manual, y puede reducir el tiempo de ingeniería necesario para su producción manual. Se puede comprobar la consistencia de los datos de fallo para de ese modo integrar los datos, lo cual a su vez puede facilitar la consistencia entre presentaciones de los datos. Esto puede permitir una mejor evaluación del caso de fallo (por ejemplo, la determinación de si un caso de fallo es aceptable o si se debe realizar un cambio para garantizar la seguridad y la funcionalidad del sistema complejo global). Las comprobaciones de consistencia de los datos de fallo también pueden garantizar la producción de un producto más seguro, más integrado, siendo necesario menos tiempo y menos recursos.

De acuerdo con un aspecto de las realizaciones de ejemplo, el sistema incluye un validador de datos y un motor de presentaciones acoplado al mismo. El validador de datos está configurado para recibir y validar datos de análisis de

fallos para un sistema complejo que incluye una pluralidad de sistemas. Los datos de análisis de fallos incluyen datos de fallo que identifican a uno o más sistemas con fallos de la pluralidad de sistemas, y también puede incluir datos de diseño que describen el sistema complejo y posibles fallos de al menos algunos de sus sistemas. En un ejemplo, los sistemas con fallos pueden incluir un sistema con fallos afectado directamente por un fallo de origen, y cualquier sistema con fallos de orden inferior afectado indirectamente por el fallo de origen. Y en un ejemplo más concreto, los sistemas del sistema complejo pueden incluir uno o más sistemas eléctricos, incluyendo los sistemas con fallos a uno o más sistemas eléctricos con fallos.

El que el validador de datos esté configurado para validar los datos de análisis de fallos puede incluir que esté configurado para realizar una o más comprobaciones de consistencia entre los datos de fallo y los datos de diseño para, de ese modo, integrar los datos de fallo para una pluralidad de diferentes presentaciones de análisis de fallos. A su vez, el motor de presentaciones está configurado para generar de manera selectiva una presentación cualquiera o más de la pluralidad de diferentes presentaciones de los datos de análisis de fallos, siendo compartidos al menos algunos de los datos de análisis de fallos entre al menos algunas de las diferentes presentaciones.

En diferentes ejemplos, los datos de fallo pueden incluir cualquier dato de varios diferentes. Por ejemplo, los datos de fallo pueden incluir uno o más mensajes del sistema (por ejemplo, mensajes de alerta, mensajes de estado, mensajes de mantenimiento) generados en respuesta a los respectivos fallos de los sistemas con fallos. De forma adicional o alternativa, por ejemplo, los datos de fallo pueden incluir niveles de riesgo para los respectivos fallos de los sistemas con fallos. En otro ejemplo, los datos de fallo pueden identificar estados de potencia del uno o más sistemas eléctricos con fallos. Y en otro ejemplo adicional, los datos de fallo pueden incluir una lista de una o más funciones a nivel del sistema complejo afectadas por los sistemas con fallos.

En diferentes ejemplos, los datos de diseño pueden incluir cualquier dato de varios diferentes. Por ejemplo, los datos de diseño pueden incluir información de la interfaz lógica que describe relaciones lógicas entre los sistemas del sistema complejo. De forma adicional o alternativa, por ejemplo, los datos de diseño pueden incluir una colección de mensajes de alerta asociados a diversos sistemas del sistema complejo. Los datos de diseño pueden incluir uno o más diagramas esquemáticos que describen relaciones físicas entre el sistema complejo y sus sistemas, siendo el sistema complejo divisible en una pluralidad de zonas físicamente diferenciadas. Es más, por ejemplo, los datos de diseño pueden incluir una colección de niveles de riesgo asociados a diversos sistemas del sistema complejo. En otro ejemplo adicional, los datos de diseño pueden incluir datos de carga eléctrica que describen los estados de potencia de uno o más de los sistemas eléctricos para diferentes estados operativos del sistema complejo. Y en otro ejemplo adicional más, los datos de diseño pueden incluir una lista de una o más funciones a nivel del sistema complejo y de sistemas del sistema complejo que implementan las funciones respectivas.

En diversos ejemplos, el validador de datos puede estar configurado para realizar cualquier comprobación de consistencia de varias diferentes, incluidas por ejemplo, una o más de entre: comprobación de consistencia de la interfaz lógica, comprobación de consistencia de las alertas, comprobación de consistencia de la ubicación, comprobación de consistencia de la interfaz lógica, comprobación de consistencia de la evaluación de riesgos, comprobación de consistencia de la carga eléctrica o comprobación de consistencia de los impactos funcionales. En un ejemplo, el validador de datos puede estar configurado para realizar la comprobación de consistencia de la interfaz lógica incluyendo una comprobación de que el sistema con fallos está relacionado de manera lógica con los sistemas con fallos de orden inferior, o de que los sistemas relacionados de manera lógica con los sistemas con fallos son los sistemas con fallos de orden inferior.

La comprobación de consistencia de las alertas puede incluir una comprobación de que los uno o más mensajes de alerta generados para los sistemas con fallos se correlacionan con mensajes de alerta asociados a los respectivos sistemas con fallos de la colección de mensajes de alerta. La comprobación de consistencia de la ubicación puede incluir una comprobación de que los sistemas con fallos están situados físicamente en la misma zona del sistema complejo. En un ejemplo adicional, la comprobación de consistencia de la ubicación también puede incluir una comprobación de consistencia de la interfaz lógica, por ejemplo de la manera anteriormente indicada.

La comprobación de consistencia de los riesgos puede incluir una comprobación de que los niveles de riesgo para los respectivos fallos de los sistemas con fallos se correlacionan con niveles de riesgo asociados a los respectivos sistemas con fallos de la colección de niveles de riesgo. La comprobación de consistencia de la carga eléctrica puede incluir una comprobación de que los estados de potencia de los uno o más sistemas eléctricos con fallos se correlacionan con los datos de carga eléctrica. Y en un ejemplo, la comprobación de consistencia de los impactos funcionales puede incluir una comprobación de que los datos de fallo que incluyen a las funciones a nivel del sistema complejo afectadas por los sistemas con fallos se correlacionan con los datos de diseño que incluyen a las funciones a nivel del sistema complejo implementadas por los respectivos sistemas con fallos.

En las figuras y en el texto, en un aspecto, se describe un sistema para la integración de datos de fallo para diferentes presentaciones de análisis de fallos, incluyendo el sistema:

un validador de datos configurado para recibir y validar datos de análisis de fallos para un sistema complejo que incluye una pluralidad de sistemas, donde los datos de análisis de fallos incluyen datos de fallo y datos de

diseño, identificando los datos de fallo a uno o más sistemas con fallos de la pluralidad de sistemas, y describiendo los datos de diseño al sistema complejo y a posibles fallos de al menos algunos de sus sistemas, y donde el que el validador de datos esté configurado para validar los datos de análisis de fallos incluye que esté configurado para realizar una o más comprobaciones de consistencia entre los datos de fallo y los datos de diseño para, de ese modo, integrar los datos de fallo para una pluralidad de diferentes presentaciones de análisis de fallos; y un motor de presentaciones acoplado al validador de datos y configurado para generar de manera selectiva una presentación cualquiera o más de la pluralidad de diferentes presentaciones de los datos de análisis de fallos, siendo compartidos al menos algunos de los datos de análisis de fallos validados entre al menos algunos de los diferentes presentaciones.

De forma alternativa, el sistema puede incluir el que los sistemas con fallos incluyan un sistema con fallos directamente afectado por un fallo de origen, y cualquier sistema con fallos de orden inferior afectado de manera indirecta por el fallo de origen, el que los datos de diseño incluyan información de la interfaz lógica que describe relaciones lógicas entre los sistemas del sistema complejo, y el que el hecho de que el validador de datos esté configurado para realizar una o más comprobaciones de consistencia incluya que esté configurado para realizar una comprobación de consistencia de la interfaz lógica utilizando los datos de fallo y la información de la interfaz lógica, incluyendo la comprobación de consistencia de la interfaz lógica una comprobación de que el sistema con fallos está relacionado de manera lógica con los sistemas con fallos de orden inferior, o de que los sistemas relacionados de manera lógica con el sistema con fallos son los sistemas con fallos de orden inferior.

De forma alternativa, el sistema puede incluir el que los datos de fallo incluyan uno o más mensajes de alerta generados en respuesta a los respectivos fallos de los sistemas con fallos, y el que los datos de diseño incluyan una colección de mensajes de alerta asociados a diferentes sistemas del sistema complejo, y el que el hecho de que el validador de datos esté configurado para realizar una o más comprobaciones de consistencia incluya que esté configurado para realizar una comprobación de consistencia de las alertas utilizando los mensajes de alerta generados y la colección de mensajes de alerta, incluyendo la comprobación de consistencia de las alertas una comprobación de que los uno o más mensajes de alerta generados para los sistemas con fallos se correlacionan con mensajes de alerta asociados a los respectivos sistemas con fallos de la colección de mensajes de alerta.

De forma alternativa, el sistema puede incluir el que los datos de diseño incluyan uno o más diagramas esquemáticos que describan relaciones físicas entre el sistema complejo y sus sistemas, siendo el sistema complejo divisible en una pluralidad de zonas físicamente diferenciadas, y el que el hecho de que el validador de datos esté configurado para realizar una o más comprobaciones de consistencia incluya que esté configurado para realizar una comprobación de consistencia de la ubicación utilizando los datos de fallo y uno o más diagramas esquemáticos, incluyendo la comprobación de consistencia de la ubicación una comprobación de que los sistemas con fallos están situados físicamente en la misma zona del sistema complejo.

De forma alternativa, el sistema puede incluir el que los datos de fallo incluyan niveles de riesgo para los respectivos fallos de los sistemas con fallos, y el que los datos de diseño incluyan una colección de niveles de riesgo asociados a diferentes sistemas del sistema complejo, y el que el hecho de que el validador de datos esté configurado para realizar una o más comprobaciones de consistencia incluya que esté configurado para realizar una comprobación de consistencia de la evaluación de riesgos utilizando los mensajes de riesgo para los respectivos fallos de los sistemas con fallos y la colección de mensajes de alerta, incluyendo la comprobación de consistencia de la evaluación de riesgos una comprobación de que los niveles de riesgo para los respectivos fallos de los sistemas con fallos se correlacionan con niveles de riesgo asociados a los respectivos sistemas con fallos de la colección de niveles de riesgo.

De forma alternativa, el sistema puede incluir el que los sistemas del sistema complejo incluyan uno o más sistemas eléctricos, el que los sistemas con fallos incluyan uno o más sistemas eléctricos con fallos, y el que los datos de fallo identifiquen estados de potencia de los uno o más sistemas eléctricos con fallos, el que los datos de diseño incluyan datos de carga eléctrica que describen los estados de potencia de uno o más de los sistemas eléctricos para diferentes estados operativos del sistema complejo, y el que el hecho de que el validador de datos esté configurado para realizar una o más comprobaciones de consistencia incluya que esté configurado para realizar una comprobación de consistencia de la evaluación de riesgos utilizando los datos de fallo y los datos de carga eléctrica, incluyendo la comprobación de consistencia de la carga eléctrica una comprobación de que los estados de potencia de los uno o más sistemas eléctricos con fallos se correlacionan con los datos de carga eléctrica.

De forma alternativa, el sistema puede incluir el que los datos de fallo incluyan una lista de una o más funciones a nivel de sistema complejo afectadas por los sistemas con fallos, el que los datos de diseño incluyan una lista de una o más funciones de a nivel de sistema complejo y de sistemas del sistema complejo que implementan las respectivas funciones, y el que el hecho de que el validador de datos esté configurado para realizar una o más comprobaciones de consistencia incluya que esté configurado para realizar una comprobación de consistencia de los impactos funcionales incluyendo una comprobación de que los datos de fallo que incluyen a las funciones a nivel del sistema complejo afectadas por los sistemas con fallos se correlacionan con los datos de diseño que incluyen a las funciones de a nivel de sistema complejo implementadas por los respectivos sistemas con fallos.

En un aspecto, se describe un método de integración de datos de fallo para diferentes presentaciones de análisis de fallos, incluyendo el método: recibir datos de análisis de fallos para un sistema complejo que incluye una pluralidad de sistemas, incluyendo los datos de análisis de fallos datos de fallo que identifican a uno o más sistemas con fallos de la pluralidad de sistemas, validando los datos de análisis de fallos para de ese modo integrar los datos de fallo para una pluralidad de diferentes presentaciones de análisis de fallos, y generando de manera selectiva una presentación cualquiera o más de la pluralidad de diferentes presentaciones de los datos de análisis de fallos, siendo compartidos al menos algunos de los datos de análisis de fallos validados entre al menos algunas de las diferentes presentaciones.

De forma alternativa, el método puede incluir el que los datos de análisis de fallos incluyan además datos de diseño que describen el sistema complejo y posibles fallos de al menos algunos de sus sistemas, y el que la validación de los datos de análisis de fallos incluya la realización de una o más comprobaciones de consistencia entre los datos de fallo y los datos de diseño.

De forma alternativa, el método puede incluir el que los sistemas con fallos incluyan un sistema con fallos directamente afectado por un fallo de origen, y cualesquiera sistemas con fallos de orden inferior afectados indirectamente por el fallo de origen, el que los datos de diseño incluyan información de la interfaz lógica que describa relaciones lógicas entre los sistemas del sistema complejo, y el que la realización de las una o más comprobaciones de consistencia incluya la realización de una comprobación de consistencia de la interfaz lógica utilizando los datos de fallo y la información de interfaz lógica, incluyendo la comprobación de consistencia de la interfaz lógica una comprobación de que el sistema con fallos está relacionado de manera lógica con los sistemas con fallos de orden inferior, o de que los sistemas relacionados de manera lógica con el sistema con fallos son los sistemas con fallos de orden inferior.

De forma alternativa, el método puede incluir el que los datos de fallo incluyan uno o más mensajes de alerta generados en respuesta a los respectivos fallos de los sistemas con fallos, y los datos de diseño incluyen una colección de mensajes de alerta asociados a diversos sistemas del sistema complejo, y el que la realización de una o más comprobaciones de consistencia incluya la realización de una comprobación de consistencia de las alertas utilizando los mensajes de alerta generados y la colección de mensajes de alerta, incluyendo la comprobación de consistencia de las alertas una comprobación de que los uno o más mensajes de alerta generados para los sistemas con fallos se correlacionan con mensajes de alerta asociados a los respectivos sistemas con fallos de la colección de mensajes de alerta.

De forma alternativa, el método puede incluir el que los datos de diseño incluyan uno o más diagramas esquemáticos que describen relaciones físicas entre el sistema complejo y sus sistemas, siendo el sistema complejo divisible en una pluralidad de zonas físicamente diferenciadas, y el que la realización de las una o más comprobaciones de consistencia incluya la realización de una comprobación de consistencia de la ubicación utilizando los datos de fallo y uno o más diagramas esquemáticos, incluyendo la comprobación de consistencia de la ubicación una comprobación de que los sistemas con fallos están situados físicamente en la misma zona del sistema complejo.

De forma alternativa, el método puede incluir el que los datos de fallo incluyan niveles de riesgo para los respectivos fallos de los sistemas con fallos, y el que los datos de diseño incluyan una colección de niveles de riesgo asociados a diversos sistemas del sistema complejo, y

el que la realización de una o más comprobaciones de consistencia incluya la realización de una comprobación de consistencia de la evaluación de riesgos utilizando los niveles de riesgo para los respectivos fallos del sistema con fallos y la colección de mensajes de alerta, incluyendo la comprobación de consistencia de la evaluación de riesgos una comprobación de que los niveles de riesgo para los respectivos fallos de los sistemas con fallos se correlacionan con niveles de riesgo asociados a los respectivos sistemas con fallos de la colección de niveles de riesgo.

De forma alternativa, el método puede incluir el que los sistemas del sistema complejo incluyan uno o más sistemas eléctricos, los sistemas con fallos incluyan uno o más sistemas eléctricos con fallos, y los datos de fallo identifican estados de potencia de los uno o más sistemas eléctricos con fallos, el que los datos de diseño incluyan datos de carga eléctrica que describen los estados de potencia de uno o más de los sistemas eléctricos para diferentes estados operativos del sistema complejo, y el que la realización de las una o más comprobaciones de consistencia incluya la realización de una comprobación de consistencia de la carga eléctrica utilizando los datos de fallo y datos de carga eléctrica, incluyendo la comprobación de consistencia de la carga eléctrica una comprobación de que los estados de potencia de los uno o más sistemas eléctricos con fallos se correlacionan con los datos de carga eléctrica.

De forma alternativa, el método puede incluir el que los datos de fallo incluyan una lista de una o más funciones a nivel del sistema complejo afectadas por los sistemas con fallos, incluyendo los datos de diseño una lista de una o más funciones a nivel del sistema complejo y de sistemas del sistema complejo que implementan las funciones respectivas, y

el que la realización de las una o más comprobaciones de consistencia incluye la realización de una comprobación de consistencia de los impactos funcionales que incluye una comprobación de que los datos de fallo que incluyen a las funciones a nivel del sistema complejo afectadas por los sistemas con fallos se correlacionan con los datos de diseño que incluyen a las funciones a nivel del sistema complejo implementados por los respectivos sistemas con fallos.

En un aspecto, se describe un medio de almacenamiento informático que tiene partes de código de programa informático almacenadas en su interior que, en respuesta a su ejecución por un procesador, provocan que un aparato al menos: reciba y valide datos de análisis de fallos para un sistema complejo que incluye una pluralidad de sistemas, donde los datos de análisis de fallos incluyen datos de fallo y datos de diseño, identificando los datos de fallo a uno o más sistemas con fallos de la pluralidad de sistemas, y describiendo los datos de diseño al sistema complejo y a posibles fallos de al menos algunos de sus sistemas, y donde el que se haga que el aparato valide los datos de análisis de fallos incluye que se haga que realice una o más comprobaciones de consistencia entre los datos de fallo y los datos de diseño para, de ese modo, integrar los datos de fallo para una pluralidad de diferentes presentaciones de análisis de fallo, y generar de manera selectiva una presentación cualquiera o más de la pluralidad de diferentes presentaciones de los datos de análisis de fallo, siendo compartidos al menos algunos de los datos de análisis de fallos validados entre al menos algunas de las diferentes presentaciones.

De forma alternativa, el medio de almacenamiento informático puede incluir el que los sistemas con fallos incluyan un sistema con fallos afectado directamente por un fallo de origen, y cualquier sistema con fallos de orden inferior indirectamente afectado por el fallo de origen, el que los datos de diseño incluyan información de la interfaz lógica que describa relaciones lógicas entre los sistemas del sistema complejo, y el que el hecho de que se haga que el aparato realice una o más comprobaciones de consistencia incluya que se haga que realice una comprobación de consistencia de la interfaz lógica utilizando los datos de fallo y la información de la interfaz lógica, incluyendo la comprobación de consistencia de la interfaz lógica una comprobación de que el sistema con fallos está relacionado de manera lógica con los sistemas con fallos de orden inferior, o de que los sistemas relacionados de manera lógica con el sistema con fallos son los sistemas con fallos de orden inferior.

De forma alternativa, el medio de almacenamiento informático puede incluir el que los datos de fallo incluyan uno o más mensajes de alerta generados en respuesta a los respectivos fallos de los sistemas con fallos, y los datos de diseño incluyen una colección de mensajes de alerta asociados a diversos sistemas del sistema complejo, y el hecho de que se haga que el aparato realice una o más comprobaciones de consistencia incluya que se haga que realice una comprobación de consistencia de las alertas utilizando los mensajes de alerta generados y la colección de mensajes de alerta, incluyendo la comprobación de consistencia de las alertas una comprobación de que los uno o más mensajes de alerta generados para los sistemas con fallos se correlacionan con mensajes de alerta asociados a los respectivos sistemas con fallos de la colección de mensajes de alerta.

De forma alternativa, el medio de almacenamiento informático puede incluir el que los datos de diseño incluyan uno o más diagramas esquemáticos que describan relaciones físicas entre el sistema complejo y sus sistemas, siendo el sistema complejo divisible en una pluralidad de zonas físicamente diferenciadas, y el que el hecho de que se haga que el aparato realice una o más comprobaciones de consistencia incluya que se haga que realice una comprobación de consistencia de la ubicación utilizando los datos de fallo y uno o más diagramas esquemáticos, incluyendo la comprobación de consistencia de la ubicación una comprobación de que los sistemas con fallos están situados físicamente en la misma zona del sistema complejo.

De forma alternativa, los datos de fallo incluyen niveles de riesgo para los respectivos fallos de los sistemas con fallos, y los datos de diseño incluyen una colección de niveles de riesgo asociados a diversos sistemas del sistema complejo, y donde el que se haga que el aparato realice una o más comprobaciones de consistencia incluye que se haga que realice una comprobación de consistencia de la evaluación de riesgos utilizando los niveles de riesgo para los respectivos fallos de los sistemas con fallos y la colección de mensajes de alerta, incluyendo la comprobación de consistencia de la evaluación de riesgos una comprobación de que los niveles de riesgo para los respectivos fallos de los sistemas con fallos se correlacionan con niveles de riesgo asociados a los respectivos sistemas con fallos de la colección de niveles de riesgo.

De forma alternativa, el medio de almacenamiento informático puede incluir el que los sistemas del sistema complejo incluyan uno o más sistemas eléctricos, los sistemas con fallos incluyan uno o más sistemas eléctricos con fallos, y los datos de fallo identifiquen estados de potencia del uno o más sistemas eléctricos con fallos, el que los datos de diseño incluyan datos eléctricos que describan los estados de potencia de uno o más de los sistemas eléctricos para diferentes estados operativos del sistema complejo, y el que el hecho de que se haga que el aparato realice una o más comprobaciones de consistencia incluya que se haga que realice una comprobación de consistencia de la carga eléctrica utilizando los datos de fallo y datos de carga eléctrica, incluyendo la comprobación de consistencia de la carga eléctrica una comprobación de que los estados de potencia de los uno o más sistemas eléctricos con fallos se correlacionan con los datos de carga eléctrica.

De forma alternativa, el medio de almacenamiento informático incluye el que los datos de fallo incluyan una lista de una o más funciones a nivel del sistema complejo afectadas por los sistemas con fallos, el que los datos de diseño incluyan una lista de una o más funciones a nivel del sistema complejo y de sistemas del sistema complejo que implementan las respectivas funciones, y el que el hecho de que se haga que el aparato realice una o más comprobaciones de consistencia incluya que se haga que realice una comprobación de consistencia de los impactos funcionales que incluye una comprobación de que los datos de fallo que incluyen a las funciones a nivel del sistema complejo afectadas por los sistemas con fallos se correlacionan con los datos de diseño que incluyen a las funciones a nivel del sistema complejo implementadas por los respectivos sistemas con fallos.

En otros aspectos de las realizaciones de ejemplo, se proporcionan un método y un medio de almacenamiento informático para crear diferentes presentaciones de análisis de fallos consistentes para un sistema complejo.

Los rasgos, funciones y ventajas analizados anteriormente se pueden conseguir de forma independiente en diferentes realizaciones de ejemplo o se pueden combinar en otras realizaciones de ejemplo adicionales, de las cuales se pueden ver detalles adicionales con referencia a la siguiente descripción y dibujos.

BREVE DESCRIPCIÓN DEL/DE LOS DIBUJO(S)

Habiendo descrito de esta forma en términos generales realizaciones de ejemplo de la invención, se hará ahora referencia a los dibujos adjuntos, los cuales no están dibujados necesariamente a escala, y en los cuales:

La Figura 1 es una ilustración de un análisis de fallos de acuerdo con una realización de ejemplo;
La Figura 2 es una ilustración de un sistema de recogida de datos de acuerdo con una realización de ejemplo;
La Figura 3 es una ilustración de un sistema de presentación de datos de acuerdo con una realización de ejemplo;
Las Figuras 4 a 8 ilustran de forma esquemática diferentes comprobaciones de consistencia que se pueden realizar sobre datos de análisis de fallos de acuerdo con realizaciones de ejemplo; y
Las Figuras 9 a13 ilustran de forma esquemática modelos de presentación apropiados de acuerdo con realizaciones de ejemplo.

DESCRIPCIÓN DETALLADA

Se describirán ahora con mayor detalle algunas realizaciones de la presente invención haciendo referencia en lo que sigue a los dibujos adjuntos, en los cuales se muestran algunas de las realizaciones de la invención, pero no todas. Efectivamente, las diferentes realizaciones de la invención se pueden implementar de muchas formas distintas y no se debería interpretar que están limitadas a las realizaciones descritas en este documento; más bien, estas realizaciones de ejemplo se proporcionan para que esta descripción sea minuciosa y completa, y transmita totalmente el alcance de la descripción a aquellas personas que tengan experiencia en la técnica. Asimismo, algo que se puede mostrar o describir como si estuviera por encima de otro elemento (a menos que se indique otra cosa) puede estar por debajo en vez de por encima, y viceversa; y de manera similar, algo mostrado o descrito como si estuviera a la izquierda de otro elemento puede estar a la derecha en vez de a la izquierda, y viceversa. Números de referencia similares hacen referencia a elementos similares a lo largo de toda la descripción.

Las realizaciones de ejemplo de la presente invención están relacionadas de forma general con la presentación de datos de análisis de fallos y, en particular, con la creación de presentaciones de análisis de fallos diferentes y consistentes, para un sistema complejo. Las realizaciones de ejemplo se describirán principalmente en conjunto con aplicaciones aeroespaciales. Sin embargo, se debería entender que las realizaciones de ejemplo se pueden utilizar en conjunto con una variedad de otras aplicaciones, tanto de dentro como de fuera de la industria aeroespacial. A este respecto, las realizaciones de ejemplo se pueden utilizar en conjunto con sistemas complejos, tales como en el caso de las industrias aeroespacial, de automoción, marina y electrónica. El acceso a datos de fallo precisos y consistentes es importante porque puede afectar a múltiples aspectos de operaciones de equipos, incluidos seguridad, operaciones, mantenimiento, soporte a ingeniería y similares.

En un sistema complejo, tal como por ejemplo una aeronave, los datos de análisis de fallos pueden estar relacionados con uno o más fallos. Un sistema complejo puede estar compuesto generalmente por uno o más componentes, subsistemas o similares (cada uno de ellos denominado generalmente “subsistema”), estando cada subsistema compuesto por una o más partes, e incluyendo cada parte uno o más rasgos. A este respecto, las partes del sistema complejo pueden estar ensambladas para formar varios subsistemas, los cuales a su vez pueden estar ensamblados para formar el sistema complejo. En el contexto de una aeronave, una o más partes o subsistemas pueden estar diseñados como un componente modular de la aeronave, denominado a menudo unidad sustituible en línea (LRU), pudiendo una única aeronave incluir varias LRUs y otras partes o subsistemas. A cualquier elemento de entre el propio sistema complejo o cualquiera de sus subsistemas, partes (de subsistemas), rasgos (de partes) o similares se les puede denominar en ocasiones, de forma general, “sistema”.

Haciendo ahora referencia a la Figura 1, se ilustra un sistema 100 de análisis de fallos de acuerdo con realizaciones de ejemplo de la presente invención. El sistema puede incluir cualquier subsistema de varios diferentes (cada uno un sistema individual) para realizar una o más funciones u operaciones con respecto a datos de análisis de fallos. Como se muestra, por ejemplo, el sistema puede incluir un sistema 102 de recogida de datos y/o un sistema 104 de

presentación de datos. Aunque se muestran como parte del sistema de análisis de fallos, en vez de esto, uno o más de entre el sistema de recogida de datos y/o el sistema de presentación de datos puede ser independiente del sistema de análisis de fallos pero estar en comunicación con él. También se debería entender que uno o más de los subsistemas puede funcionar u operar como un sistema independiente sin tener en cuenta a otros subsistemas. Y además, se debería entender que el sistema de análisis de fallos puede incluir uno o más subsistemas adicionales o alternativos a los mostrados en la Figura 1.

Como se describe en este documento, los datos de análisis de fallos pueden incluir datos de fallo y/o datos de diseño, y pueden estar relacionados con uno o más fallos de un sistema complejo. Como se describe en este documento, un fallo puede hacer referencia a una avería, a una degradación o a un fallo. Generalmente, puede ser posible visualizar los datos de análisis de fallos de forma electrónica y/o impresa (o imprimible); y a este respecto, los datos de análisis de fallos pueden incluir uno o más de contenido en forma de texto, en forma gráfica u otro contenido visual tal como imágenes fijas, video o similar.

Para cada uno de los uno o más casos de fallo del sistema complejo, los datos de fallo pueden identificar o describir (siendo estos dos términos sinónimos en este documento, y en ocasiones utilizándose de forma general “identificar”) un fallo a nivel de sistema y, en diferentes casos, uno o más efectos del fallo a nivel de sistema. En un ejemplo, los datos de fallo pueden ser apropiados para su utilización en cualquiera de varios diferentes análisis de fallos de aeronaves, tales como evaluación de riesgos particular (PRA), análisis de amenazas, análisis de seguridad zonal, análisis de modos de fallo y efectos (FMEA) a nivel del sistema, FMEA a nivel del avión (también conocido como FMEA de sistemas múltiples), análisis de fallos debidos a causas comunes (CCA) o similares.

Los efectos de un fallo a nivel de sistema pueden incluir uno o más efectos directos y, en diversos casos, uno o más efectos indirectos, cada uno de los cuales se puede manifestar él mismo como un fallo. A este respecto, un efecto directo puede ser cualquier efecto primario (o de origen) que sea resultado directo de un fallo de origen a nivel de sistema. Un efecto indirecto puede ser cualquier efecto secundario (o de segundo orden), cualquier efecto terciario (o de tercer orden), cualquier efecto cuaternario (o de cuarto orden) y así sucesivamente que sean resultados indirectos de un fallo de origen a nivel de sistema, y que sean resultados directos de un efecto directo o de otro efecto indirecto. En un ejemplo, los efectos indirectos se pueden manifestar ellos mismos como fallos de orden inferior. Por ejemplo, un efecto indirecto se puede manifestar él mismo como cualquier fallo secundario (o de segundo orden), cualquier fallo terciario (o de tercer orden), cualquier fallo cuaternario (o de cuarto orden) y así sucesivamente. Un efecto puede estar asociado a una combinación de casos de fallo, otros efectos o combinaciones de ambos, que sólo se producen cuando se produce la combinación. Por ejemplo, un cierto efecto directo se puede producir sólo cuando se producen dos fallos, o un cierto efecto indirecto se puede producir sólo cuando se producen dos efectos directos y/o dos efectos indirectos.

Una aeronave, por ejemplo, puede experimentar un fallo de un bus eléctrico o del sistema de navegación de la aeronave. Este fallo puede producir a su vez efectos directos tales como efectos hidráulicos, efectos en la navegación y/o efectos en la aviónica, uno cualquiera o más de uno de los cuales puede producir uno o más efectos indirectos. Por ejemplo, un efecto hidráulico puede producir un efecto sobre el control de vuelo, el cual a su vez puede producir un efecto de vibración del fuselaje.

Los datos de fallo para un caso de fallo pueden identificar un fallo y uno o más efectos o fallos de orden inferior provocados por él, y pueden incluir además uno o más mensajes de alerta tales como mensajes de alerta para la tripulación, mensajes de estado, mensajes de mantenimiento o similares que se pueden haber generado en respuesta a un fallo (fallo de origen o de orden inferior). Por ejemplo, un mensaje de alerta puede ser un mensaje de alerta accionable para la tripulación que se muestra a la tripulación de vuelo para indicar una falta de presurización adecuada de la cabina. Un ejemplo de un mensaje de alerta para la tripulación de este tipo es un mensaje EICAS (sistema de indicación de los motores y de alerta a la tripulación).

Los datos de fallo pueden incluir una o más acciones compensatorias (por ejemplo, conmutar a energía alternativa, hacer descender la aeronave) que pueden haber sido emprendidas en respuesta a un fallo, por ejemplo por la tripulación o por uno o más sistemas del sistema complejo. Los datos de fallo pueden incluir una descripción del efecto adicional, que puede estar relacionado con uno o más efectos adicionales del respectivo fallo (por ejemplo, pérdida de iluminación, falta de extensión del tren de aterrizaje normal, pérdida de visualización). Los datos de fallo pueden incluir además un mapeado o correlación entre cada fallo a nivel de sistema y un estado funcional de un respectivo sistema. En un ejemplo, los estados funcionales puede venir dados por categorías, por ejemplo por las siguientes categorías en orden decreciente de funcionalidad: “totalmente funcional”, “degradado”, y “con fallos”.

Los datos de fallo también pueden incluir una probabilidad y un nivel de riesgo para cada fallo o para cada sistema con fallos (sistema con fallos o sistema con fallos de orden inferior), y pueden incluir además un riesgo a nivel del sistema complejo global. A este respecto, la probabilidad puede indicar la posibilidad de que el fallo se produzca en vuelo, y el nivel de riesgo puede indicar el efecto del fallo sobre los ocupantes y/o sobre las operaciones del sistema complejo. En un ejemplo, los niveles de riesgo se pueden representar de forma numérica, por ejemplo en orden de “uno” a “cinco” en nivel de riesgo creciente. En otro ejemplo, los niveles de riesgo pueden venir dados por

categorías, por ejemplo por las siguientes categorías en orden creciente de nivel de riesgo: “ningún efecto sobre la seguridad”, “menor”, “grave”, “peligroso” y “catastrófico”.

Más aún, los datos de fallo pueden incluir una lista de una o más funciones a nivel de sistema complejo afectadas por cada fallo. En un ejemplo, funciones a nivel de la aeronave que pueden verse afectadas por un fallo pueden incluir integridad estructural, estabilidad y control, conciencia operativa, control ambiental, generación y distribución de energía, carga, mantenimiento y maniobrabilidad en tierra, control en tierra o similares.

También como parte de los datos de análisis de fallos, los datos de diseño pueden incluir información que describa el sistema complejo y posibles fallos de al menos algunos de sus sistemas. Por ejemplo, los datos de diseño pueden incluir uno o más diagramas esquemáticos del sistema complejo y/o de sus sistemas, los cuales pueden describir las relaciones físicas entre sistemas. De forma adicional o alternativa, por ejemplo, los datos de diseño pueden incluir información de la interfaz lógica, la cual puede describir relaciones lógicas entre sistemas, y donde dichas relaciones lógicas pueden estar reflejadas mediante interfaces lógicas entre los respectivos sistemas. Un ejemplo de información de la interfaz lógica es la proporcionada por un documento de control de interfaces (ICD). Además, por ejemplo, los datos de diseño pueden incluir una lista de una o más funciones a nivel del sistema complejo y de uno o más sistemas del sistema complejo que implementan las respectivas funciones.

En otro ejemplo, los datos de diseño pueden incluir datos de carga eléctrica, los cuales pueden describir el estado de potencia de uno o más sistemas eléctricos (por ejemplo, alimentado, no alimentado, alimentado de forma intermitente) en diversos estados operativos del sistema complejo. En el contexto de una aeronave, en ciertos estados operativos (por ejemplo, en tierra, arranque, apagado de un motor, etc.), un sistema eléctrico puede estar en diversos estados de potencia (por ejemplo, a media potencia, a un cuarto de potencia, etc.). En estas situaciones, ciertos sistemas pueden estar alimentados mientras que otros sistemas pueden no estar alimentados. Por lo tanto, los datos de diseño pueden indicar qué sistemas están en “interrupción de la carga” (por ejemplo, energía desconectada de algunos equipos para mantener funcionalidad básica en ciertos escenarios). En un ejemplo, entonces, los datos de carga eléctrica se pueden dar en una o más listas de “interrupción de la carga”.

Los datos de diseño también pueden incluir, por ejemplo, una colección de mensajes de alerta que se pueden generar para diferentes sistemas asociados, y/o la lógica de acuerdo con la cual se pueden configurar los respectivos mensajes. En un ejemplo, los mensajes de alerta pueden ser priorizados de acuerdo con una necesidad de acción creciente, como por ejemplo “aviso”, “precaución” y “alerta”. En otro ejemplo, los datos de diseño pueden incluir una colección de acciones compensatorias que se pueden emprender en respuesta a un fallo, y/o la lógica de acuerdo con la cual se pueden emprender las respectivas acciones. En otro ejemplo adicional, los datos de diseño pueden incluir una colección de niveles de riesgo que se pueden proporcionar para el sistema complejo y/o para diversos sistemas asociados, y/o conjuntos de fallos para los cuales se pueden configurar diferentes niveles de riesgo. En un ejemplo, los niveles de riesgo y los conjuntos de fallos pueden ser proporcionados por datos de evaluación de seguridad del sistema (SSA) y/o de evaluación de riesgos funcionales (FHA).

Como se explica con mayor detalle más adelante, el sistema 102 de recogida de datos del sistema 100 de análisis de fallos puede estar configurado de manera general para recoger y validar datos de fallo para, de ese modo, integrar los datos de fallo para diferentes presentaciones de datos de análisis de fallos, los cuales pueden incluir al menos algunos de los datos de fallo y de los datos de diseño. Y el sistema 104 de presentación de datos puede estar configurado de manera general para generar de manera selectiva una cualquiera o más de una pluralidad de diferentes presentaciones de datos de análisis de fallos, siendo compartidos al menos algunos de los datos de análisis de fallos entre al menos algunos de los diferentes presentaciones. La presentación se puede presentar visualmente; y en un ejemplo, la presentación visual de una presentación puede ser visualizable por ejemplo en una interfaz gráfica de usuario (GUI) presentada por una pantalla de visualización. En otro ejemplo, la presentación visual puede ser imprimible por ejemplo por una impresora configurada para generar una impresión de la presentación. En ocasiones, a la presentación visual de una presentación se le puede denominar simplemente la presentación.

Los análisis de fallos son una práctica habitual en industrias enfocadas a sistemas complejos, tal como la industria aeroespacial lo está para las aeronaves. La evaluación de la clasificación de riesgo global (por ejemplo, “a nivel de sistema complejo”) y la aceptabilidad de casos de fallo concretos puede implicar a muchos implicados, cada uno de los cuales requiere su propia presentación de eventos. Cada presentación de un implicado puede proporcionar una explicación parcial o incompleta de un caso de fallo concreto. Por lo tanto, realizaciones de ejemplo de la presente invención pueden crear presentaciones de fallo individuales y definir reglas y comprobaciones de consistencia para integrar datos de análisis de fallos que subyacen tras los presentaciones de tal manera que se puede hacer una evaluación completa de un caso de fallo.

Se hará ahora referencia a las Figuras 2 y 3, las cuales ilustran ejemplos más concretos de un sistema de recogida de datos y de un sistema de presentación de datos apropiados, respectivamente, de acuerdo con realizaciones de ejemplo de la presente invención.

La Figura 2 ilustra un sistema 200 de recogida de datos, el cual en una realización de ejemplo puede corresponder al sistema 102 de recogida de datos. Como se muestra, el sistema de recogida de datos puede incluir un validador de datos configurado para recibir datos de análisis de fallos incluyendo datos de fallo y/o datos de diseño. El validador de datos puede estar configurado para recibir los datos de análisis de fallos procedentes de cualquiera de varias fuentes diferentes, y los cuales pueden estar formateados de cualquier manera de varias diferentes. Por ejemplo, el validador de datos puede estar configurado para recibir datos de fallo para uno o más casos de fallo procedentes directamente de un operador, por ejemplo a través de técnicas de introducción de datos. En otro ejemplo, el validador de datos puede estar configurado para recibir datos de fallo procedentes directamente de un sistema complejo que falla, el cual puede estar provisto de uno o más sensores o sistemas integrados configurados para transmitir una señal en caso de que él o uno de sus sistemas experimente un fallo. En otro ejemplo adicional, el validador de datos puede estar configurado para recibir datos de fallo procedentes de un almacenamiento apropiado como por ejemplo un almacenamiento en ficheros, un almacenamiento en bases de datos, un almacenamiento en la nube o similares.

Cuando el validador 202 de datos recibe datos de análisis de fallos, o después de recibirlos, el citado validador de datos puede estar configurado para validar al menos una parte de los datos de análisis de fallos, incluyendo la realización de una o más comprobaciones de consistencia entre los datos de fallo y los datos de diseño. En el caso de que el validador de datos valide con éxito los datos de análisis de fallos, el validador de datos puede estar configurado para comunicar los datos de fallo y los datos de diseño a respectivos almacenamientos 204, 206 para su almacenamiento y posterior recuperación. El almacenamiento puede ser residente con el sistema 200 de recogida de datos, o puede ser independiente del sistema de recogida de datos y estar en comunicación con él. Los datos de análisis de fallos pueden ser formateados y almacenados de cualquier manera de varias diferentes y, por lo tanto, su almacenamiento puede ser de cualquier tipo de varios diferentes. Ejemplos de tipos de almacenamiento apropiados incluyen almacenamiento en ficheros, almacenamiento en bases de datos, almacenamiento en la nube o similares.

En el caso de que el validador 202 de datos no consiga validar con éxito cualquier parte de los datos de análisis de fallos, el validador de datos puede estar configurado para señalizar con una bandera los respectivos datos de análisis de fallos, y puede estar además configurado para comunicar una indicación de que existe una bandera. En un ejemplo, la indicación de que existe una bandera se puede comunicar a una GUI en la cual se puede visualizar, o a una impresora para generar una impresión de ella. En otro ejemplo, la indicación de que existe una bandera se puede comunicar a otro sistema, aparato o similar de acuerdo con cualquier técnica de mensajería de varias diferentes, tal como por ejemplo correo electrónico, mensajería instantánea o similar.

El validador 202 de datos puede estar configurado para validar o realizar una o más comprobaciones de consistencia sobre al menos una parte de los datos de análisis de fallos de cualquier manera de varias diferentes. En un ejemplo, como se muestra en la Figura 4, el validador de datos puede estar configurado para realizar una comprobación de consistencia de la interfaz lógica utilizando la información de la interfaz lógica de los datos de fallo que describe las interfaces lógicas entre sistemas del sistema complejo. Las interfaces lógicas entre un sistema y otro u otros sistemas pueden indicar sistemas en los que, en el caso de fallo del respectivo sistema, se debería esperar que se produjeran efectos (por ejemplo, un efecto propiamente dicho, una reducción de redundancia, “ningún efecto”, etc.). Entonces, para un caso de fallo que identifica a un sistema con fallos (directamente afectado) y a uno o más sistemas con fallos de orden inferior (indirectamente afectados), el validador de datos puede estar configurado para comprobar que el sistema con fallos está relacionado de manera lógica con todos los sistemas con fallos de orden inferior, y/o que todos los sistemas relacionados de forma lógica del sistema con fallos son sistemas con fallos de orden inferior.

En otro ejemplo, como se muestra en la Figura 5, el validador 202 de datos puede estar configurado para realizar una comprobación de consistencia de las alertas para la tripulación utilizando los datos de fallo y la colección de mensajes de alerta que se pueden proporcionar para diversos sistemas asociados del sistema complejo. En un ejemplo más concreto, los datos de fallo para un caso de fallo pueden incluir uno o más mensajes de alerta que pueden ser enviados o generados para el fallo y/o uno o más de sus efectos, y los cuales pueden estar asociados al sistema con fallos y/o a uno o más sistemas con fallos de orden inferior. Los datos de diseño pueden incluir, de manera similar, una colección de mensajes de alerta que se pueden proporcionar para sistemas asociados del sistema complejo. Por lo tanto, el validador de datos puede comprobar que cualquier mensaje de alerta generado para un sistema con fallos o para un sistema con fallos de orden inferior se correlaciona con un mensaje de alerta asociado al respectivo sistema con fallos de la colección de mensajes de alerta.

En otro ejemplo, como se muestra en la Figura 6 en el contexto de una aeronave, el validador 202 de datos puede estar configurado para realizar una comprobación de consistencia de la ubicación utilizando los datos de fallo, uno o más diagramas esquemáticos del sistema complejo y/o de sus sistemas, y/o información de interfaz lógica. Un sistema puede estar conectado a su ubicación física dentro del sistema complejo, el cual puede estar dividido en varias zonas físicamente diferenciadas. Algunos análisis de fallos tales como los análisis PRA (por ejemplo, análisis de choque con aves, análisis de explosión del rotor –*rotoburst*-, etc.), asumen fallos en todos los sistemas situados dentro de una zona concreta. A su vez, los sistemas afectados en la zona concreta pueden tener efectos “en cascada” sobre los sistemas relacionados de manera lógica con ellos, los cuales pueden estar en la misma zona o en otra. Por lo tanto, el validador de datos puede comprobar que los sistemas con fallos y los sistemas con fallos de

orden inferior en un caso de fallo están situados físicamente en la misma zona del sistema complejo, y puede señalizar con una bandera cualquier fallo que falte o que esté incompleto para sistemas situados dentro de la zona respectiva. El validador de datos puede entonces realizar una comprobación de consistencia de la interfaz lógica para sistemas relacionados de manera lógica situados en otras zonas del sistema complejo, por ejemplo de la manera descrita anteriormente con respecto a la Figura 4.

Como se muestra en la Figura 7, el validador 202 de datos puede estar configurado para realizar una comprobación de consistencia de la evaluación de riesgos utilizando los datos de fallo y la colección de niveles de riesgos que se pueden proporcionar para el sistema complejo y/o para algunos de sus sistemas, pudiendo dicha colección ser proporcionada en un ejemplo mediante datos SSA y/o FHA. Los sistemas individuales del sistema complejo pueden proporcionar datos de fallo de sus respectivos sistemas y efecto del riesgo local (efecto y riesgo asociados a su sistema) – el riesgo a nivel del sistema complejo (por ejemplo, al nivel de la aeronave) puede no ser transparente a partir de los efectos a nivel de sistema y riesgos a nivel de sistema asociados.

En relación con a la comprobación de consistencia de la evaluación de riesgos, se puede realizar por lo tanto un análisis a nivel de sistema complejo para determinar el efecto global, el cual puede ser reflejado por un riesgo a nivel de sistema complejo. El validador 202 de datos puede estar configurado para comprobar que el riesgo a nivel de sistema complejo asociado a un fallo no es menor que un riesgo a nivel de sistema individual (por ejemplo, que un riesgo a nivel de sistema complejo es calificado como “grave” mientras que uno de sus sistemas lo califica como “peligroso”). En un caso en el que el nivel de riesgo del sistema complejo sea menor que el de uno de sus sistemas, el validador de datos puede señalizar con una bandera el caso de fallo. Esta situación se puede remediar en un ejemplo incrementando el riesgo a nivel de sistema complejo o reduciendo el mayor riesgo a nivel del sistema.

De forma adicional o alternativa, por ejemplo, la comprobación de consistencia de la evaluación de riesgos puede incluir que el validador 202 de datos compruebe que el nivel de riesgo local para un sistema con fallos o para un sistema con fallos de orden inferior es consistente con el nivel o niveles de riesgo del sistema que se pueden proporcionar para el respectivo sistema (por ejemplo, a partir de datos FHA). Es decir, el validador de datos puede comprobar que el nivel de riesgo local para sistemas con fallos o para sistemas con fallos de orden inferior se correlaciona con niveles de riesgo asociados a los respectivos sistemas de la colección de niveles de riesgo. En un caso en el que el nivel de riesgo local no es consistente, el caso de fallo se puede señalizar con una bandera. En un ejemplo, esta condición inaceptable se puede remediar modificando el riesgo local para el análisis de fallos o modificando los datos FHA del sistema.

En un ejemplo adicional, el validador 202 de datos puede estar configurado para realizar una comprobación de consistencia de la carga eléctrica utilizando los datos de fallo y los datos de carga eléctrica, los cuales de nuevo se proporcionan en una o más listas de “interrupción de la carga”. En algunos análisis de fallo, los sistemas eléctricos pueden verse afectados y, en estos casos, los datos de fallo pueden identificar a los estados de potencia (por ejemplo, alimentado o no alimentado) de estos sistemas eléctricos con fallos. Basándose en el efecto de potencia eléctrica y en el estado de “interrupción de la carga” asociado, sistemas de la lista de “interrupción de la carga” pueden estar “interrumpidos” o con fallos a efectos del análisis. Esta comprobación de consistencia puede garantizar que todos los sistemas de la lista de interrupción de la carga para casos de fallo concretos estén representados de manera apropiada en los análisis de fallo. Es decir, esta comprobación de consistencia puede incluir una comprobación de que los estados de potencia de uno o más sistemas eléctricos con fallos se correlacionan con los datos de carga eléctrica. Las discrepancias se pueden señalizar con banderas para su revisión y corrección/eliminación.

En un ejemplo adicional más, como se muestra en la Figura 8, el validador 202 de datos puede estar configurado para realizar una comprobación de consistencia de los impactos funcionales utilizando los datos de fallo y los datos de diseño. En un ejemplo más concreto, los datos de fallo para un caso de fallo pueden incluir una lista de una o más funciones a nivel del sistema complejo afectadas por los sistemas con fallos o por los sistemas con fallos de orden inferior. De manera similar, los datos de diseño incluyen una lista de función o funciones a nivel de sistema complejo y del sistema o sistemas del sistema complejo que implementan la respectiva función o funciones. Por lo tanto, el validador de datos puede comprobar que las funciones a nivel de sistema complejo afectadas por los sistemas con fallos o por los sistemas con fallos de orden inferior se correlacionan con las funciones a nivel de sistema complejo implementadas por los respectivos sistemas con fallos.

En diversos casos, después de que los datos de fallo y los datos de diseño se hayan comunicado al almacenamiento 204, 206 respectivo, cualquiera de ellos o los dos pueden ser modificados por ejemplo por un operador. En estos casos modificación puede significar cualquier cambio a los datos de varios diferentes incluyendo, por ejemplo, una adición, un borrado, una revisión o similar. En estos casos, el validador 202 de datos puede estar configurado para validar los datos de fallo o de diseño modificados y cualquier otro dato del almacenamiento respectivo que puedan ser afectados por los datos de fallo o de diseño modificados.

En un ejemplo, se puede efectuar una modificación de los datos de diseño mediante una solicitud de cambio (CR) u otro mecanismo similar. Una CR puede afectar a uno o más sistemas del sistema complejo, y puede afectar a una o más áreas incluyendo interfaces lógicas entre sistemas (por ejemplo, interfaces lógicas nuevas/borradas/revisadas)

y/o mensajes de alerta (por ejemplo, asociaciones nuevas/borradas/revisadas entre alertas y sistemas). De forma adicional o alternativa, por ejemplo, una CR puede afectar a la ubicación zonal de un sistema por ejemplo en el caso de que el sistema se mueva entre zonas. En eventos como este o similares, una CR puede incluir información acerca de las interfaces y del sistema implicados en el cambio (el lado del diseño), uno cualquiera o más de los cuales puede estar relacionado con datos de fallo de uno o más casos de fallo. Por lo tanto, el validador 202 de datos puede estar configurado para identificar características comunes entre interfaces afectadas y/o entre sistemas dentro del mecanismo de cambio y para relacionarlas con el caso o los casos de fallo apropiados. Si se encuentra una relación, ésta puede ser señalada con una bandera para su evaluación en cuanto a si un cambio en el análisis de fallos puede estar justificado.

Se hace ahora referencia a la Figura 3, la cual ilustra un sistema 300 de presentación de datos de acuerdo con una realización de ejemplo. Como se ha indicado anteriormente, el sistema 300 de presentación de datos puede ser un ejemplo del sistemas 104 de presentación de datos del sistema 100 de análisis de fallos de la Figura 1. El sistema de presentación de datos puede estar configurado de manera general para generar una presentación de datos de análisis de fallos que incluya datos de fallo y/o datos de diseño. Estos datos pueden ser o incluir, por ejemplo, datos procedentes del sistema 102 de recogida de datos, o más concretamente en un ejemplo, del sistema 200 de recogida de datos de la Figura 2.

Como se muestra en la Figura 3, el sistema 300 de presentación de datos puede incluir una interfaz de solicitud o similar configurada para recibir una solicitud de datos de análisis de fallos. En un ejemplo, la interfaz de solicitud puede ser parte de un motor 302 de presentaciones, de un generador de presentaciones o similar configurado para generar una presentación de los datos de análisis de fallos solicitados. Los datos de análisis de fallos pueden incluir datos de fallo y/o datos de diseño, los cuales se pueden almacenar en un respectivo almacenamiento 304, 306, el cual en un ejemplo puede corresponder al respectivo almacenamiento 204, 206 mostrado en la Figura 2.

El motor 302 de presentaciones puede estar configurado para seleccionar un modelo de presentación de entre una pluralidad de modelos de presentaciones para seleccionar y organizar los datos de análisis de fallos solicitados. El motor de presentaciones puede estar configurado para seleccionar el modelo de presentación de cualquier manera de varias diferentes. En un ejemplo, el motor de presentaciones puede estar configurado para seleccionar el modelo de presentación de acuerdo con la solicitud de datos de análisis de fallo, la cual puede indicar o reflejar un modelo de presentación concreto. Los modelos de presentación pueden incluir cualquier tipo de presentación de varios de ellos diferentes para la organización de datos de análisis de fallos. Como se ha indicado anteriormente y se explica con mayor detalle más adelante, ejemplos de modelos de presentación apropiados incluyen un modelo de presentación de efectos en cascada, un modelo de presentación de cabina de vuelo, un modelo de presentación del perfil de vuelo, un modelo de presentación de impactos funcionales, un modelo de presentación de planificación de ensayos o similares. Otros ejemplos pueden incluir combinaciones de uno o más de los anteriores modelos de presentación. Los modelos de presentación se pueden mantener en un respectivo almacenamiento, tal como por ejemplo almacenamiento en fichero, almacenamiento en base de datos, almacenamiento en la nube o similar, y se pueden formatear y almacenar de cualquier manera de varias diferentes de acuerdo con el almacenamiento respectivo.

El motor 302 de presentaciones puede estar configurado para recuperar del respectivo almacenamiento 304, 306 los datos de análisis de fallos solicitados para el modelo de presentación seleccionado. El motor de presentaciones puede estar configurado para generar una presentación de los datos de análisis de fallos solicitados, los cuales se pueden organizar de acuerdo con el modelo de presentación seleccionado. El motor de presentaciones puede estar entonces configurado para comunicar la presentación, por ejemplo a una GUI en la cual se puede visualizar una presentación, o una impresora para generar una impresión de la presentación.

La presentación generada por el motor 302 de presentaciones puede ser generada de forma dinámica de acuerdo con un modelo de presentación seleccionado, de tal manera que cambiando el modelo de presentación seleccionado se pueda realizar una presentación diferente de los datos de análisis de fallos. En un ejemplo, el motor de presentaciones puede por lo tanto estar además configurado para recibir una solicitud para una organización diferente de datos de análisis de fallo. En este ejemplo, el motor de presentaciones puede estar configurado para seleccionar un modelo de presentación diferente de entre la pluralidad de modelos de presentación en respuesta a la solicitud. El motor de presentaciones puede entonces estar configurado para generar una presentación diferente de los datos de análisis de fallos recuperados. Esto puede incluir el que el motor de presentaciones esté configurado para reorganizar datos de análisis de fallos de acuerdo con el modelo de presentación diferente seleccionado.

Como se ha indicado anteriormente, los modelos de presentación pueden incluir cualquier tipo de presentación de varios diferentes para organizar datos de análisis de fallos. Se hará ahora referencia a las Figuras 9-13, las cuales ilustran de forma esquemática ejemplos de modelos de presentación apropiados. Como se muestra, estos ejemplos incluyen una presentación de efectos en cascada, una presentación de cabina de vuelo, una presentación del perfil de vuelo, una presentación de impactos funcionales, una presentación de planificación de ensayos o similar.

La Figura 9 ilustra un modelo 900 de presentación de efectos en cascada de acuerdo con una realización de ejemplo. El modelo de presentación de efectos en cascada proporciona de manera general una representación

gráfica de efectos de fallo en cascada incluyendo uno o más efectos directos, y en diferentes casos, uno o más efectos indirectos. Como se ha explicado anteriormente, un efecto directo puede ser cualquier efecto primario (o de origen) que se produzca directamente como resultado de un fallo a nivel de sistema de origen. Un efecto indirecto puede ser cualquier efecto secundario (o de segundo orden), un efecto terciario (o de tercer orden), un efecto cuaternario (o de cuarto orden) y así sucesivamente que se produzca indirectamente como resultado de un fallo a nivel de sistema de origen, y directamente de un efecto directo o de otro efecto indirecto. Este modelo de presentación puede ser de particular interés para entender las razones detrás de los efectos y los impactos a través de sistemas del sistema complejo. Este modelo de presentación puede ser útil para varios implicados diferentes del sistema complejo tales como ingenieros de sistemas, representantes autorizados (ARs), ingenieros de seguridad, expertos en la materia del sistema individual (SMEs), pilotos o similares.

Como se muestra en la Figura 9, en el modelo 900 de presentación de efectos en cascada para un caso de fallo, cada sistema del sistema complejo puede ser representado como un nodo 902 y puede incluir datos 904 de fallo respectivos tales como uno o más mensajes de alerta (por ejemplo, mensajes EICAS), nivel de riesgo a nivel de sistema y/o descripción del efecto adicional (señalándose sólo un nodo y mostrándose sus respectivos datos de fallo en la Figura 9). El modelo de presentación de efectos en cascada también puede ilustrar conexiones 906 (señalándose sólo una conexión) entre los nodos 902, las cuales pueden ilustrar cómo un fallo de un sistema del sistema complejo puede producir como resultado, de forma directa o indirecta, un fallo de uno o más sistemas del sistema complejo. En un ejemplo, se pueden presentar estas conexiones para ilustrar efectos en cascada de un fallo de sistema. A este respecto, el modelo de presentación de efectos en cascada puede identificar un sistema con fallos de origen, y que puede experimentar uno o más efectos directos del fallo. A su vez, el sistema con fallos de origen puede estar conectado de manera directa o indirecta a uno o más sistemas con fallos de orden inferior que pueden experimentar uno o más efectos indirectos respectivos. Por ejemplo, el sistema con fallos de origen puede estar directamente conectado a uno o más sistemas con fallos secundarios que pueden experimentar respectivos uno o más efectos secundarios. A su vez, el sistema o sistemas con fallos secundarios respectivos pueden experimentar uno o más respectivos efectos terciarios. Para el sistema complejo, esto puede ocurrir para n órdenes de sistemas extraídos del sistema con fallos de origen.

En un ejemplo, los nodos 902 del modelo 900 de presentación de efectos en cascada se pueden organizar por el orden de sus efectos. El sistema con fallos de origen se puede organizar de acuerdo a que experimente o no efectos 908 directos. Este sistema con fallos de origen puede estar conectado entonces a uno o más sistemas con fallos secundarios organizados de acuerdo a que experimente o no los efectos 910 secundarios, y los cuales pueden estar conectados a uno o más sistemas con fallos terciarios organizados de acuerdo a que experimente o no los efectos 914 terciarios. Se debería entender que aunque el modelo de presentación de efectos en cascada de la Figura 9 parece indicar al menos dos órdenes de efectos resultantes de un fallo de origen, menos de dos órdenes de efectos pueden resultar de un fallo de origen (incluyendo un fallo de origen sólo con efectos directos).

La Figura 10 ilustra un modelo 1000 de presentación de cabina de vuelo de acuerdo con una realización de ejemplo. El modelo de presentación de cabina de vuelo proporciona de manera general una representación gráfica de efectos de fallo en cascada que pueden ser experimentados por uno o más sistemas de cabina de vuelo. El modelo de presentación de cabina de vuelo puede ser de particular interés para entender cómo puede aparecer un fallo concreto a la tripulación de una aeronave u otro sistema complejo similar. Esta información puede ser útil para implicados tales como ingenieros de sistemas, ARs, ingenieros de seguridad, PYMEs de sistemas, pilotos y similares.

Como se muestra en la Figura 10, el modelo 1000 de presentación de cabina de vuelo puede incluir una representación esquemática de una cabina de vuelo 1002 en la cual varios de sus diferentes sistemas se pueden ilustrar mediante respectivas representaciones 1004 esquemáticas (algunas de las cuales, pero no todas ellas, se señalan en la Figura 10). En un ejemplo, la cabina de vuelo y sus sistemas se pueden representar de forma esquemática de una manera que refleja la colocación de los sistemas (o más en concreto, en un ejemplo, de sus controles) que pueden ser visibles para la tripulación de la cabina de vuelo. En un ejemplo, esta representación esquemática se puede generar a partir de datos de diseño para la cabina de vuelo.

A continuación, para un caso de fallo, el modelo 1000 de presentación de cabina de vuelo puede identificar uno o más sistemas con fallos incluidos sistemas con fallos de origen o sistemas con fallos de orden inferior, y pueden hacerlo directamente sobre sus representaciones 1004 esquemáticas respectivas. En un ejemplo, el modelo de presentación de cabina de vuelo puede resaltar mediante texto, de forma gráfica o de otra manera las representaciones esquemáticas de uno o más sistemas con fallos. En un ejemplo adicional, el modelo de presentación de cabina de vuelo puede resaltar uno o más sistemas con fallos de una manera que refleje datos de fallo adicionales tales como los estados funcionales de los sistemas con fallos. Como se muestra en la Figura 10, por ejemplo, el modelo de presentación de cabina de vuelo puede resaltar representaciones 1006 de sistemas con fallos que tengan un estado “degradado”, y señalar con una cruz representaciones 1008 de sistemas con fallos que tengan un estado “con fallos”.

Además de lo anterior, el modelo 1000 de presentación de cabina de vuelo puede incluir datos de fallo adicionales para sistemas con fallos en la cabina de vuelo. En un ejemplo, estos datos de fallo adicionales pueden incluir para al

menos algunos de los sistemas con fallos, uno o más mensajes 1010 de alerta y/o acciones compensatorias que pueden haber sido generadas o adoptadas en respuesta a un fallo. De forma adicional o alternativa, por ejemplo, los datos de fallo adicionales pueden incluir nivel de riesgo a nivel de sistema y/o descripción de efecto adicional para al menos algunos de los sistemas con fallos.

La Figura 11 ilustra un modelo 1100 de presentación del perfil de vuelo de acuerdo con una realización de ejemplo. El modelo de presentación del perfil de vuelo proporciona de manera general una representación gráfica de efectos de fallo en cascada sobre un perfil de vuelo teórico. Este modelo de presentación puede ser diferente a las otras presentaciones “planas” en que proporciona una vista por tiempos/por fases del vuelo de un caso de fallo. No todos los fallos de sistema se producen al mismo tiempo. En los fallos en cascada pueden existir retrasos. Por ejemplo, la pérdida de refrigeración puede conducir a fallos en sistemas que pueden estar degradados o tener fallos por encima de una cierta temperatura, pero puede llevar tiempo que la temperatura del sistema, una vez enfriado, aumente por encima de la respectiva temperatura. Esta información puede ser útil para implicados tales como ingenieros de sistemas, ARs, ingenieros de seguridad, PYMEs de sistemas, pilotos o similares.

Como se muestra en la Figura 11, el modelo 1100 de presentación del perfil de vuelo puede incluir una representación gráfica de un perfil 1102 de vuelo para un vuelo de la aeronave, el cual en un ejemplo puede parecer similar a un gráfico lineal de altitud de la aeronave frente al tiempo. El modelo de presentación del perfil de vuelo puede incluir entonces un cronograma de uno o más casos de fallo que se producen durante el vuelo, y puede hacerlo sobre el perfil de vuelo. En un ejemplo, el modelo de presentación del perfil de vuelo puede incluir datos de fallo tales como una identificación de uno o más fallos 1104 de origen o fallos de orden inferior, y/o una o más descripciones 1106 de efecto adicional, mensajes 1108 de alerta y/o acciones 1110 compensatorias (algunas de las cuales, pero no todas, están señaladas en la Figura 11).

Al menos algunos de los datos de fallo del modelo 1100 de presentación del perfil de vuelo pueden estar asociados al tiempo (a través de una fase de vuelo identificada). Por lo tanto, el modelo de presentación del perfil de vuelo puede incluir conexiones 1112 entre datos de fallo y tiempos sobre el perfil de vuelo (que se muestran para un ejemplo como una conexión con forma de flecha) (señalándose algunas de las conexiones, pero no todas). Por ejemplo, un fallo 1104 de origen o de orden inferior puede estar asociado al instante en el que se produjo el fallo, y efectos 1106 adicionales de un fallo pueden estar asociados al instante en el que se experimentaron esos efectos. En otro ejemplo, un mensaje 1108 de alerta puede estar asociado con el instante en el que un sistema generó el respectivo mensaje, y una acción 1110 compensatoria puede estar asociada al instante en el que la tripulación adoptó la respectiva acción. En un ejemplo, el modelo de presentación del perfil de vuelo puede además indicar un retraso 1114 temporal entre un fallo y datos de fallo que se pueden generar o adoptar en respuesta al fallo.

La Figura 12 ilustra un modelo 1200 de presentación de impactos funcionales de acuerdo con una realización de ejemplo. Por lo general el modelo de presentación de impactos funcionales proporciona una representación tabular que resume efectos a nivel de sistema individual y sus impactos sobre las funciones a nivel de sistema complejo. Este modelo de presentación puede ser único con respecto a los otros modelos de presentación porque proporciona a los ingenieros una forma de evaluar el efecto global de las degradaciones de cada función a nivel de sistema complejo. Esta información puede ser útil para implicados tales como ingenieros de sistemas, ARs, ingenieros de seguridad, PYMEs de sistemas, pilotos o similares.

Como se muestra en la Figura 12, el modelo 1200 de presentación de impactos funcionales puede incluir una tabla que tenga una o más filas (o registros) 1202 para uno o más casos de fallo respectivos, y una o más columnas (o campos) 1204 que especifican información relativa al caso o casos de fallo respectivos. Para cada caso de fallo dentro de una fila, las columnas pueden identificar un fallo y/o uno o más efectos o fallos de orden inferior provocados por ese fallo, y pueden identificar o resumir funciones a nivel de sistema complejo afectadas por el respectivo fallo y/o fallos de orden inferior. En un ejemplo, para cada caso de fallo, una de las columnas puede proporcionar además un resumen del efecto combinado de cada degradación de función a nivel de sistema complejo y de su efecto sobre la seguridad a nivel del sistema complejo global.

La Figura 13 ilustra un modelo 1300 de presentación de planificación de ensayos de acuerdo con una realización de ejemplo. Por lo general el modelo de presentación de planificación de ensayos proporciona una representación tabular que resume planes o procedimientos de ensayo para uno o más casos de fallo y datos de fallo asociados a los respectivos casos de fallo. A este respecto, un equipo de ensayos puede realizar muchos análisis de fallos durante los ensayos del sistema complejo. El modelo de presentación de planificación de ensayos de las realizaciones de ejemplo se puede utilizar para generar presentaciones de planificación de ensayos directamente a partir de datos de fallo, y puede incluir datos de fallo incluidos en otros modelos de presentación. Esto puede facilitar que el equipo de ensayos conteste a cualquier pregunta acerca de un fallo si ésta surge durante los ensayos. Por ejemplo, se pueden ver preguntas acerca de relaciones entre fallos a partir de datos de fallo en los efectos en cascada, o preguntas acerca de cuándo se pueden producir los fallos durante el funcionamiento del sistema complejo pueden ser respondidas por medio de presentaciones de perfil de vuelo.

Como se muestra en la Figura 13, el modelo 1300 de presentación de planificación de ensayos puede incluir una tabla que tenga una o más filas (o registros) 1302 para uno o más respectivos casos de fallo que se quieren

ensayar, y una o más columnas (o campos) 1304 que especifiquen información referente al caso o casos de fallo respectivos. Como se muestra, por ejemplo, las columnas pueden identificar un caso de fallo, y datos de fallo y procedimientos de ensayo para el caso de fallo. Para cada caso de fallo dentro de una fila, las columnas pueden identificar un fallo y/o uno o más efectos o fallos de orden inferior provocados por él, y puede identificar o resumir datos de fallo y procedimientos de ensayo para el caso de fallo. En un ejemplo, para cada caso de fallo, una de las columnas puede además proporcionar otra información miscelánea que puede ser útil para un equipo de ensayos.

De acuerdo con realizaciones de ejemplo de la presente invención, el sistema 100 de análisis de fallos y sus subsistemas incluidos el sistema 102 de recogida de datos y el sistema 104 de presentación de datos se pueden implementar por diferentes medios. De manera similar, los ejemplos de un sistema 200 de recogida de datos y sistema 300 de presentación de datos, incluyendo cada uno de sus elementos respectivos, pueden ser implementados por diferentes medios de acuerdo con realizaciones de ejemplo. Medios para implementar los sistemas, subsistemas y sus respectivos elementos pueden incluir hardware, solo o bajo la dirección de una o más instrucciones de código de programa informático, instrucciones de programa o instrucciones de código de programa informático ejecutables procedentes de un medio de almacenamiento informático.

En un ejemplo, se pueden proporcionar uno o más aparatos que están configurados para funcionar como, o implementar, los sistemas, subsistemas y respectivos elementos mostrados y descritos en este documento. En ejemplos que implican a más de un aparato, los respectivos aparatos pueden estar conectados, o en comunicación, entre sí de varias maneras diferentes, como por ejemplo de forma directa o indirecta por medio de una red por cable o inalámbrica o similar.

De forma general, un aparato de las realizaciones de ejemplo de la presente descripción puede comprender, puede incluir, o puede estar implementado en uno o más dispositivos electrónicos fijos o portátiles. Ejemplos de dispositivos electrónicos apropiados incluyen un teléfono inteligente, una tableta, un ordenador portátil, un ordenador de sobremesa, una estación de trabajo, un ordenador servidor o similar. El aparato puede incluir uno o más de cada uno de varios componentes tales como, por ejemplo, un procesador (por ejemplo, una unidad de procesamiento) conectado a una memoria (por ejemplo, un dispositivo de almacenamiento).

El procesador es de forma general cualquier dispositivo hardware que es capaz de procesar información tal como, por ejemplo, datos, código de programa informático, instrucciones o similares (en ocasiones denominados de manera general “programas informáticos”, por ejemplo, software, soporte lógico inalterable –*firmware*-, etc.), y/u otra información electrónica apropiada. Más en concreto, por ejemplo, el procesador puede estar configurado para ejecutar programas informáticos, los cuales pueden estar almacenados dentro del procesador o almacenados en la memoria (del mismo aparato o de otro). El procesador puede ser varios procesadores, un núcleo con múltiples procesadores o algún otro tipo de procesador, dependiendo de la implementación concreta. Además, el procesador se puede implementar utilizando varios sistemas procesadores heterogéneos, en los cuales existe un procesador principal con uno o más procesadores secundarios en un único chip. Como otro ejemplo ilustrativo, el procesador puede ser un sistema simétrico de múltiples procesadores que contiene múltiples procesadores del mismo tipo. En otro ejemplo adicional, el procesador puede estar implementado como, o puede incluir, uno o más circuitos integrados de aplicación específica (ASICs), matrices de puertas programables in-situ (FPGAs) o similares. De esta forma, aunque el procesador puede ser capaz de ejecutar un programa informático para realizar una o más funciones, el procesador de diversos ejemplos puede ser capaz de realizar una o más funciones sin la ayuda de un programa informático.

La memoria es de forma general cualquier soporte físico que es capaz de almacenar información tal como, por ejemplo, datos, programas informáticos y/u otra información apropiada de modo temporal y/o de modo permanente. La memoria puede incluir memoria volátil y/o permanente, y puede ser fija o extraíble. Ejemplos de memorias apropiadas incluyen memoria de acceso aleatorio (RAM), memoria de sólo lectura (ROM), un disco duro, una memoria flash, una memoria USB, un disquete informático extraíble, un disco óptico, una cinta magnética o alguna combinación de los anteriores. Los discos ópticos pueden incluir memorias de sólo lectura en disco compacto (CD-ROM), discos compactos regrabables (CD-R/W), DVDs o similares. En diferentes casos, a la memoria se le puede denominar medio de almacenamiento informático, el cual, como dispositivo no transitorio capaz de almacenar información, puede ser distinguible de medios de transmisión informáticos tales como señales electrónicas transitorias capaces de transportar información desde un lugar a otro. Al medio informático descrito en este documento se le puede denominar de forma general medio de almacenamiento informático o medio de transmisión informático.

Además de la memoria, el procesador también puede estar conectado a una o más interfaces para mostrar, transmitir y/o recibir información. Las interfaces pueden incluir una interfaz de comunicaciones (por ejemplo, una unidad de comunicación) y/o una o más interfaces de usuario. La interfaz de comunicaciones puede estar configurada para transmitir y/o recibir información, por ejemplo a y/o desde otro(s) aparato(s), red(es) o similares. La interfaz de comunicaciones puede estar configurada para transmitir y/o recibir información mediante enlaces de comunicaciones físicos (por cable) y/o inalámbricos. Ejemplos de interfaces de comunicación apropiados incluyen un controlador de interfaz de red (NIC), un NIC inalámbrico (WNIC) o similares.

Las interfaces de usuario pueden incluir una pantalla y/o una o más interfaces de entrada de usuario (por ejemplo, una unidad de entrada/salida). La pantalla puede estar configurada para presentar o mostrar información a un usuario, incluyendo ejemplos apropiados de dicha pantalla una pantalla de cristal líquido (LCD), una pantalla LED, una pantalla de plasma (PDP) o similar. Las interfaces de entrada de usuario pueden ser por cable o inalámbricas, y pueden estar configuradas para recibir información que un usuario introduce en el aparato, por ejemplo para su procesamiento, almacenamiento y/o visualización. Ejemplos apropiados de interfaces de entrada de usuario incluyen un micrófono, un dispositivo de captura de imagen o de video, un teclado o teclado numérico, una palanca de control, una superficie sensible al tacto (independiente de una pantalla táctil o integrada en ella), un sensor biométrico o similares. Las interfaces de usuario pueden además incluir una o más interfaces para comunicación con periféricos tales como impresoras, escáneres o similares.

Como se ha indicado anteriormente, instrucciones de código de programa pueden estar almacenadas en memoria, y pueden ser ejecutadas por un procesador, para implementar funciones de los sistemas, subsistemas y sus elementos respectivos descritos en este documento. Como se apreciará, desde un medio de almacenamiento informático se puede cargar cualquier instrucción de código de programa en un ordenador u otro aparato programable para producir una máquina concreta, de tal manera que la máquina concreta se convierte en un medio para implementar las funciones especificadas en este documento. Estas instrucciones de código de programa también pueden estar almacenadas en un medio de almacenamiento informático que puede controlar un ordenador, un procesador u otro aparato programable para que funcione de una manera concreta para, de ese modo, generar una máquina concreta o un artículo de fabricación concreto. Las instrucciones almacenadas en el medio de almacenamiento informático pueden producir un artículo de fabricación, convirtiéndose el artículo de fabricación en un medio para implementar las funciones descritas en este documento. Las instrucciones de código de programa pueden ser recuperadas de un medio de almacenamiento informático y cargadas en un ordenador, procesador u otro aparato programable para configurar el ordenador, procesador u otro aparato programable para ejecutar operaciones que deben ser realizadas sobre o por el ordenador, procesador u otro aparato programable.

La recuperación, carga y ejecución de las instrucciones de código de programa se puede realizar secuencialmente de tal manera que una instrucción primero se recupere, luego se cargue y después se ejecute en un instante. En algunas realizaciones de ejemplo, la recuperación, carga y/o ejecución se pueden realizar en paralelo de tal manera que se recuperen, se carguen y/o se ejecuten múltiples instrucciones juntas. La ejecución de las instrucciones de código de programa puede producir un proceso implementado por ordenador tal que las instrucciones ejecutadas por el ordenador, procesador u otro aparato programable proporcionen operaciones para implementar las funciones descritas en este documento.

La ejecución de instrucciones por un procesador, o el almacenamiento de instrucciones en un medio de almacenamiento informático, soporta combinaciones de operaciones para realizar las funciones especificadas. Se entenderá también que una o más funciones, y combinaciones de funciones, pueden ser implementadas mediante sistemas informáticos basados en hardware de propósito especial y/o procesadores que realizan las funciones especificadas, o combinaciones de hardware de propósito especial e instrucciones de código de programa.

A una persona con experiencia en la técnica a la cual pertenece esta descripción se le ocurrirán muchas modificaciones y otras realizaciones de la invención descrita en este documento que tengan el beneficio de las enseñanzas presentadas en las descripciones anteriores y en los dibujos asociados. Por lo tanto, se debe entender que la invención no debe estar limitada a las realizaciones específicas descritas y que se pretende que las modificaciones y otras realizaciones estén incluidas dentro del alcance de las reivindicaciones adjuntas. Además, aunque las descripciones anteriores y los dibujos asociados describen realizaciones de ejemplo en el contexto de ciertas combinaciones de ejemplo de elementos y/o de funciones, se debería observar que realizaciones alternativas pueden proporcionar diferentes combinaciones de elementos y/o de funciones sin alejarse del alcance de las reivindicaciones adjuntas. A este respecto, por ejemplo, también se contemplan combinaciones de elementos y/o de funciones diferentes a los descritos anteriormente de forma explícita, como pueden ser los que se describen en algunas de las reivindicaciones adjuntas. Aunque en este documento se emplean términos específicos, se utilizan sólo en un sentido genérico y descriptivo y no con fines limitativos.

REIVINDICACIONES

1. Un sistema (100) para integrar datos (904) de fallo para diferentes presentaciones de análisis de fallos, comprendiendo el sistema:

un validador (202) de datos configurado para recibir y validar datos (904) de análisis de fallos para un sistema complejo que incluye una pluralidad de sistemas (902), **caracterizado por** los siguientes rasgos:

los datos (904) de análisis de fallos incluyen datos (904) de fallos y datos de diseño, identificando los datos (904) de fallos a uno o más sistemas con fallos de la pluralidad de sistemas (902), y describiendo los datos de diseño al sistema complejo y a los posibles fallos de al menos algunos de sus sistemas (902), y
el que el validador (202) de datos esté configurado para validar los datos (904) de análisis de fallos incluye que esté configurado para realizar una o más comprobaciones de consistencia entre los datos (904) de fallos y los datos de diseño para integrar de ese modo los datos (904) de fallos para una pluralidad de diferentes presentaciones de análisis de fallos; y

un motor (302) de presentaciones acoplado al validador (202) de datos y configurado para generar de manera selectiva uno cualquiera o más de la pluralidad de diferentes presentaciones de los datos (904) de análisis de fallo, siendo compartidos al menos algunos de los datos (904) de análisis de fallos validados entre al menos algunos de los diferentes presentaciones.

2. El sistema de la reivindicación 1, en el cual los sistemas con fallos incluyen un sistema con fallos directamente afectado por un fallo de origen, y cualquier sistema con fallos de orden inferior indirectamente afectado por el fallo de origen,
en el cual los datos de diseño incluyen información de la interfaz lógica que describe relaciones (906) lógicas entre los sistemas del sistema complejo, y
en el cual el que el validador (202) de datos esté configurado para realizar una o más comprobaciones de consistencia incluye que esté configurado para realizar una o más comprobaciones de consistencia de la interfaz lógica utilizando datos (904) de fallos e información de interfaz lógica, incluyendo la comprobación de consistencia de la interfaz lógica una comprobación de que el sistema con fallos está relacionado de manera lógica (906) con los sistemas con fallos de orden inferior, o de que los sistemas relacionados de manera lógica (906) con el sistema con fallos son los sistemas con fallos de orden inferior.

3. El sistema de cualquiera de las reivindicaciones 1 ó 2, en el cual los datos (904) de fallo incluyen uno o más mensajes (1010) de alerta generados en respuesta a fallos respectivos de los sistemas con fallos, y los datos de diseño incluyen una colección de mensajes (1010) de alerta asociados a diversos sistemas del sistema complejo, y
en el cual el que el validador (202) de datos esté configurado para realizar una o más comprobaciones de consistencia incluye que esté configurado para realizar una o más comprobaciones de consistencia de las alertas utilizando los mensajes (1010) de alerta generados y la colección de mensajes (1010) de alerta, incluyendo la comprobación de consistencia de las alertas una comprobación de que los uno o más mensajes (1010) de alerta generados para los sistemas con fallos se correlacionan con los mensajes (1010) de alerta asociados a los respectivos sistemas con fallos de la colección de mensajes (1010) de alerta.

4. El sistema de cualquiera de las reivindicaciones 1-3, en el cual los datos de diseño incluyen uno o más diagramas (1004) esquemáticos que describen relaciones físicas entre el sistema complejo y sus sistemas (902), siendo el sistema complejo divisible en una pluralidad de zonas físicamente diferenciadas, y
en el cual el que el validador (202) de datos esté configurado para realizar una o más comprobaciones de consistencia incluye que esté configurado para realizar una comprobación de consistencia de la ubicación utilizando los datos (904) de fallo y uno o más diagramas (1004) esquemáticos, incluyendo la comprobación de consistencia de la ubicación una comprobación de que los sistemas con fallos están situados físicamente en la misma zona del sistema complejo.

5. El sistema de cualquiera de las reivindicaciones 1-4, en el cual los datos (904) de fallo incluyen niveles de riesgo para respectivos fallos de los sistemas con fallos, y los datos de diseño incluyen una colección de niveles de riesgo asociados a diversos sistemas (902) del sistema complejo, y
en el cual el que el validador (202) de datos esté configurado para realizar una o más comprobaciones de consistencia incluye que esté configurado para realizar una comprobación de consistencia de la evaluación de riesgos utilizando los niveles de riesgo para respectivos fallos de los sistemas con fallos y la colección de mensajes (1010) de alerta, incluyendo la comprobación de consistencia de la evaluación de riesgos una comprobación de que los niveles de riesgo para los respectivos fallos de los sistemas con fallos se correlacionan con niveles de riesgo asociados a los respectivos sistemas con fallos de la colección de niveles de riesgo.

6. El sistema de cualquiera de las reivindicaciones 1-5, en el cual los sistemas del sistema complejo incluyen uno o más sistemas eléctricos, los sistemas con fallos incluyen uno o más sistemas eléctricos con fallos, y los datos (904) de fallo identifican estados de potencia de los uno o más sistemas eléctricos con fallos,

en el cual los datos de diseño incluyen datos de carga eléctrica que describen los estados de potencia de uno o más sistemas eléctricos con fallos para diversos estados de funcionamiento del sistema complejo, y
en el cual el que el validador (202) de datos esté configurado para realizar una o más comprobaciones de consistencia incluye que esté configurado para realizar una comprobación de consistencia de la carga eléctrica utilizando los datos (904) de fallo y datos de carga eléctrica, incluyendo la comprobación de consistencia de la carga eléctrica una comprobación de que los estados de potencia de los uno o más sistemas eléctricos con fallos se correlacionan con los datos de carga eléctrica.

7. El sistema de cualquiera de las reivindicaciones 1-4, en el cual los datos (904) de fallo incluyen una lista de una o más funciones a nivel de sistema complejo afectadas por los sistemas con fallos,
en el cual los datos de diseño incluyen una lista de una o más funciones a nivel de sistema complejo y de sistemas del sistema complejo que implementan las respectivas funciones, y
en el cual el que el validador (202) de datos esté configurado para realizar una o más comprobaciones de consistencia incluye que esté configurado para realizar una comprobación de consistencia de los impactos funcionales incluyendo una comprobación de que los datos (904) de fallo que incluyen a las funciones a nivel de sistema complejo afectadas por los sistemas con fallos se correlacionan con los datos de diseño que incluyen a las funciones a nivel de sistema complejo implementadas por los respectivos sistemas con fallos.

8. Un método de integración de datos (904) de fallo para diferentes presentaciones de análisis de fallos, comprendiendo el método:

recibir datos de análisis de fallos para un sistema complejo que incluye una pluralidad de sistemas (902), incluyendo los datos (904) de análisis de fallos datos (904) de fallos que identifican a uno o más sistemas con fallos de la pluralidad de sistemas (902); **caracterizado por** los siguientes pasos:

validar los datos de análisis de fallos para integrar de ese modo los datos (904) de fallos para una pluralidad de diferentes presentaciones (1004) de análisis de fallos; y
generar de manera selectiva uno cualquiera o más de la pluralidad de diferentes presentaciones (1004) de los datos de análisis de fallo, siendo compartidos al menos algunos de los datos (904) de análisis de fallos validados entre al menos algunos de los diferentes presentaciones (1004).

9. El método de la reivindicación 8, en el cual los datos (904) de análisis de fallos incluyen además datos de diseño que describen al sistema complejo y a posibles fallos de al menos algunos de sus sistemas (902), y
en el cual la validación de los datos de análisis de fallos incluye la realización de una o más comprobaciones de consistencia entre los datos (904) de fallo y los datos de diseño.

10. El método de la reivindicación 9, en el cual los sistemas con fallos incluyen un sistema con fallos afectado directamente por un fallo de origen, y cualquier sistema con fallos de orden inferior afectado indirectamente por el fallo de origen,
en el cual los datos de diseño incluyen información de la interfaz lógica que describe relaciones (906) lógicas entre los sistemas (902) del sistema complejo, y
en el cual la realización de las una o más comprobaciones de consistencia incluye la realización de una comprobación de consistencia de la interfaz lógica utilizando los datos (904) de fallo y la información de interfaz lógica, incluyendo la comprobación de consistencia de la interfaz lógica una comprobación de que el sistema con fallos está relacionado de manera lógica con los sistemas con fallos de orden inferior, o de que los sistemas (906) relacionados de manera lógica con los sistemas con fallos son los sistemas con fallos de orden inferior.

11. El método de cualquiera de las reivindicaciones 9 ó 10, en el cual los datos (904) de fallo incluyen uno o más mensajes (1010) de alerta generados en respuesta a respectivos fallos de los sistemas con fallos, y los datos de diseño incluyen una colección de mensajes (1010) de alerta asociados a diversos sistemas (906) del sistema complejo, y
en el cual la realización de las una o más comprobaciones de consistencia incluye la realización de una comprobación de consistencia de las alertas utilizando los mensajes (1010) de alerta generados y la colección de mensajes (1010) de alerta, incluyendo la comprobación de consistencia de las alertas una comprobación de que los uno o más mensajes (1010) de alerta generados para el sistema con fallos se correlacionan con mensajes (1010) de alerta asociados a los respectivos sistemas con fallos de la colección de mensajes (1010) de alerta.

12. El método de cualquiera de las reivindicaciones 9-11, en el cual los datos de diseño incluyen uno o más diagramas (1004) esquemáticos que describen relaciones físicas entre el sistema complejo y sus sistemas, siendo el sistema complejo divisible en una pluralidad de zonas físicamente diferenciadas, y
en el cual la realización de las una o más comprobaciones de consistencia incluye la realización de una comprobación de consistencia de la ubicación utilizando los datos (904) de fallo y uno o más diagramas esquemáticos, incluyendo la comprobación de consistencia de la ubicación una comprobación de que los sistemas con fallos están situados físicamente en la misma zona del sistema complejo.

13. El método de cualquiera de las reivindicaciones 9-10, en el cual los datos (904) de fallo incluyen niveles de riesgo para los respectivos fallos de los sistemas con fallos, y los datos de diseño incluyen una colección de niveles de riesgo asociados a diversos sistemas del sistema complejo, y
en el cual la realización de las una o más comprobaciones de consistencia incluye la realización de una comprobación de consistencia de la evaluación de riesgos utilizando los niveles de riesgo para respectivos fallos de los sistemas con fallos y la colección de mensajes (1010) de alerta, incluyendo la comprobación de consistencia de la evaluación de riesgos una comprobación de que los niveles de riesgo para los respectivos fallos de los sistemas con fallos se correlacionan con niveles de riesgo asociados a los respectivos sistemas con fallos de la colección de niveles de riesgo.

14. El método de cualquiera de las reivindicaciones 9-13, en el cual los sistemas (902) del sistema complejo incluyen uno o más sistemas eléctricos, los sistemas con fallos incluyen uno o más sistemas eléctricos con fallos, y los datos (904) de fallo identifican estados de potencia de los uno o más sistemas eléctricos con fallos,
en el cual los datos de diseño incluyen datos de carga eléctrica que describen los estados de potencia de uno o más de los sistemas eléctricos con fallos para diversos estados de funcionamiento del sistema complejo, y
en el cual la realización de las una o más comprobaciones de consistencia incluye la realización de una comprobación de consistencia de la carga eléctrica utilizando los datos (904) de fallo y datos de carga eléctrica, incluyendo la comprobación de consistencia de la carga eléctrica una comprobación de que los estados de potencia de los uno o más sistemas eléctricos con fallos se correlacionan con los datos de carga eléctrica.

15. El método de cualquiera de las reivindicaciones 9-13, en el cual los datos (904) de fallo incluyen una lista de una o más funciones a nivel de sistema complejo afectadas por los sistemas con fallos,
en el cual los datos de diseño incluyen una lista de una o más funciones a nivel de sistema complejo y sistemas del sistema complejo que implementan las respectivas funciones, y
en el cual la realización de las una o más comprobaciones de consistencia incluye la realización de una comprobación de consistencia de los impactos funcionales incluyendo una comprobación de que los datos (904) de fallo que incluyen a las funciones a nivel de sistema complejo afectadas por los sistemas con fallos se correlacionan con los datos de diseño que incluyen a las funciones a nivel de sistema complejo implementadas por los respectivos sistemas con fallos.

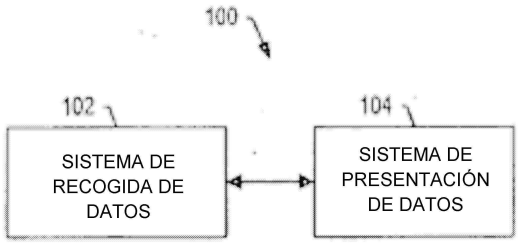

100
102
SISTEMA DE RECOGIDA DE DATOS
104
SISTEMA DE PRESENTACIÓN DE DATOS

FIG. 1

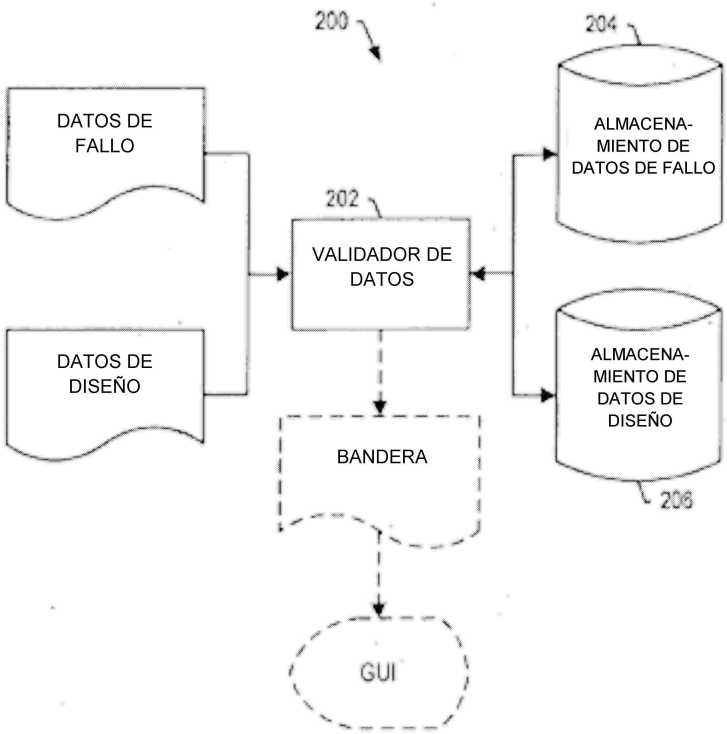

200
204
DATOS DE FALLO
ALMACENA-MIENTO DE DATOS DE FALLO
202
VALIDADOR DE DATOS
DATOS DE DISEÑO
ALMACENA-MIENTO DE DATOS DE DISEÑO
BANDERA
206
GUI

FIG. 2

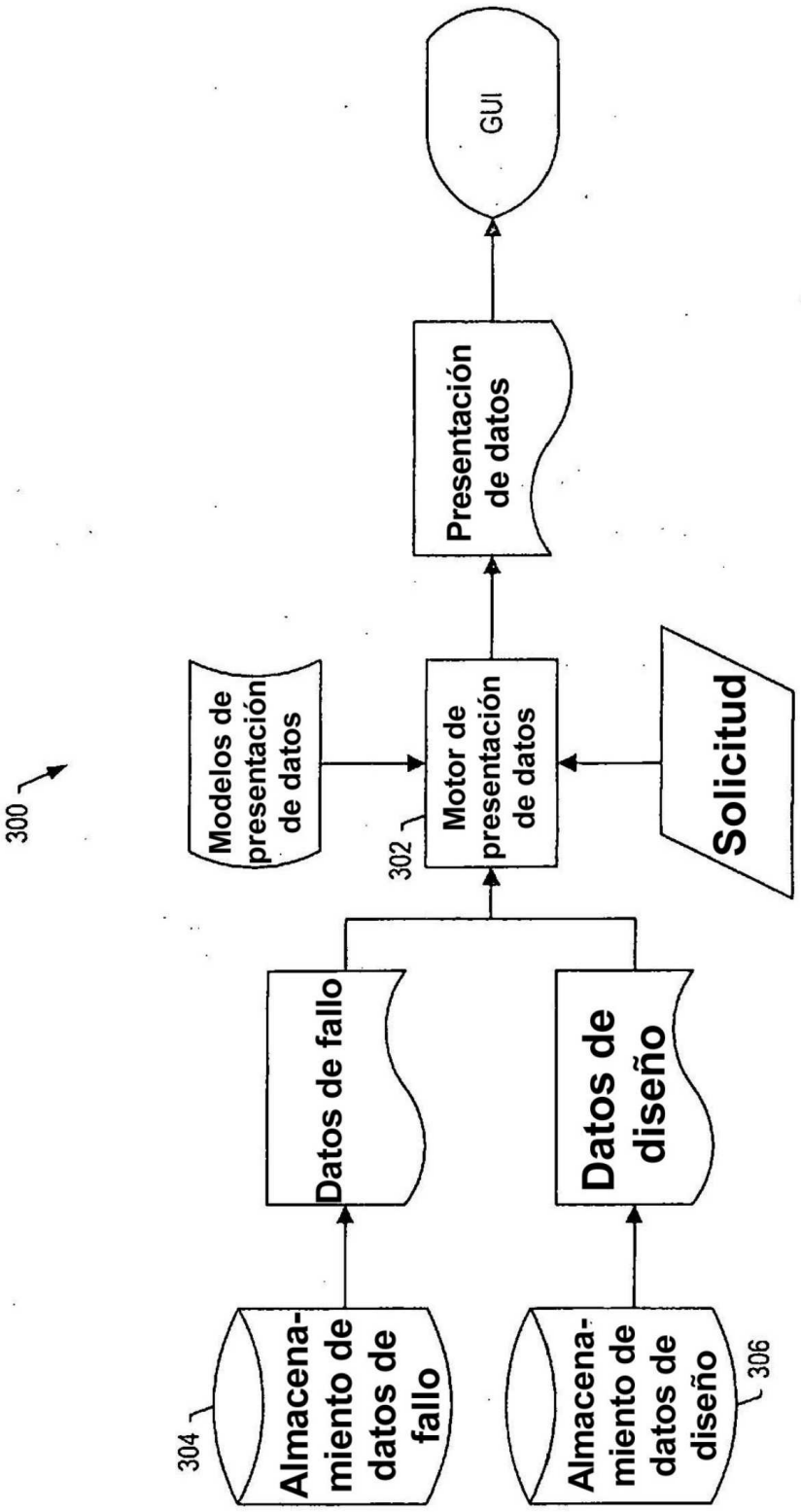

300
GUI
Presentación de datos
Modelos de presentación de datos
Motor de presentación de datos
302
Solicitud
Datos de fallo
Datos de diseño
Almacena-miento de datos de fallo
304
Almacena-miento de datos de diseño
306

FIG. 3

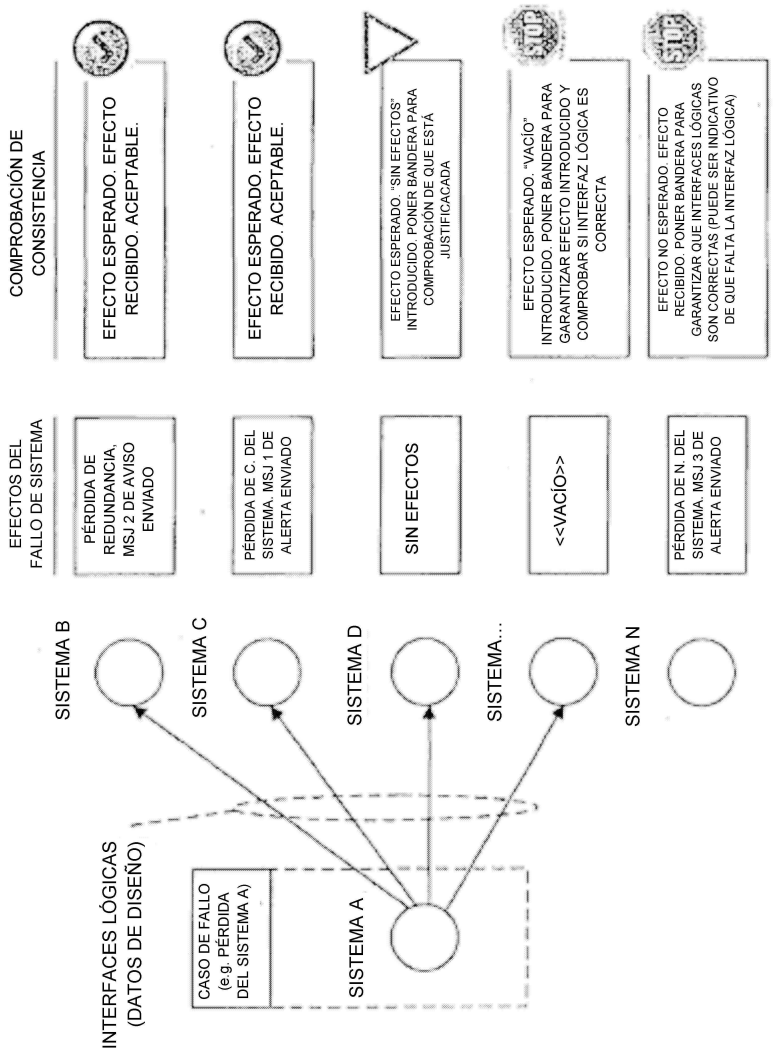

COMPROBACIÓN DE CONSISTENCIA
EFECTOS DEL FALLO DE SISTEMA
EFECTO ESPERADO. EFECTO RECIBIDO. ACEPTABLE.
EFECTO ESPERADO. EFECTO RECIBIDO. ACEPTABLE.
EFECTO ESPERADO. "SIN EFECTOS" INTRODUCIDO. PONER BANDERA PARA COMPROBACIÓN DE QUE ESTÁ JUSTIFICACADA
EFECTO ESPERADO. "VACÍO" INTRODUCIDO. PONER BANDERA PARA GARANTIZAR EFECTO INTRODUCIDO Y COMPROBAR SI INTERFAZ LÓGICA ES CORRECTA
EFECTO NO ESPERADO. EFECTO RECIBIDO. PONER BANDERA PARA GARANTIZAR QUE INTERFACES LÓGICAS SON CORRECTAS (PUEDE SER INDICATIVO DE QUE FALTA LA INTERFAZ LÓGICA)
PÉRDIDA DE REDUNDANCIA. MSJ 2 DE AVISO ENVIADO
PÉRDIDA DE C. DEL SISTEMA. MSJ 1 DE ALERTA ENVIADO
SIN EFECTOS
<<VACÍO>>
PÉRDIDA DE N. DEL SISTEMA. MSJ 3 DE ALERTA ENVIADO
SISTEMA B
SISTEMA C
SISTEMA D
SISTEMA...
SISTEMA N
INTERFACES LÓGICAS (DATOS DE DISEÑO)
CASO DE FALLO (e.g. PÉRDIDA DEL SISTEMA A)
SISTEMA A

FIG. 4

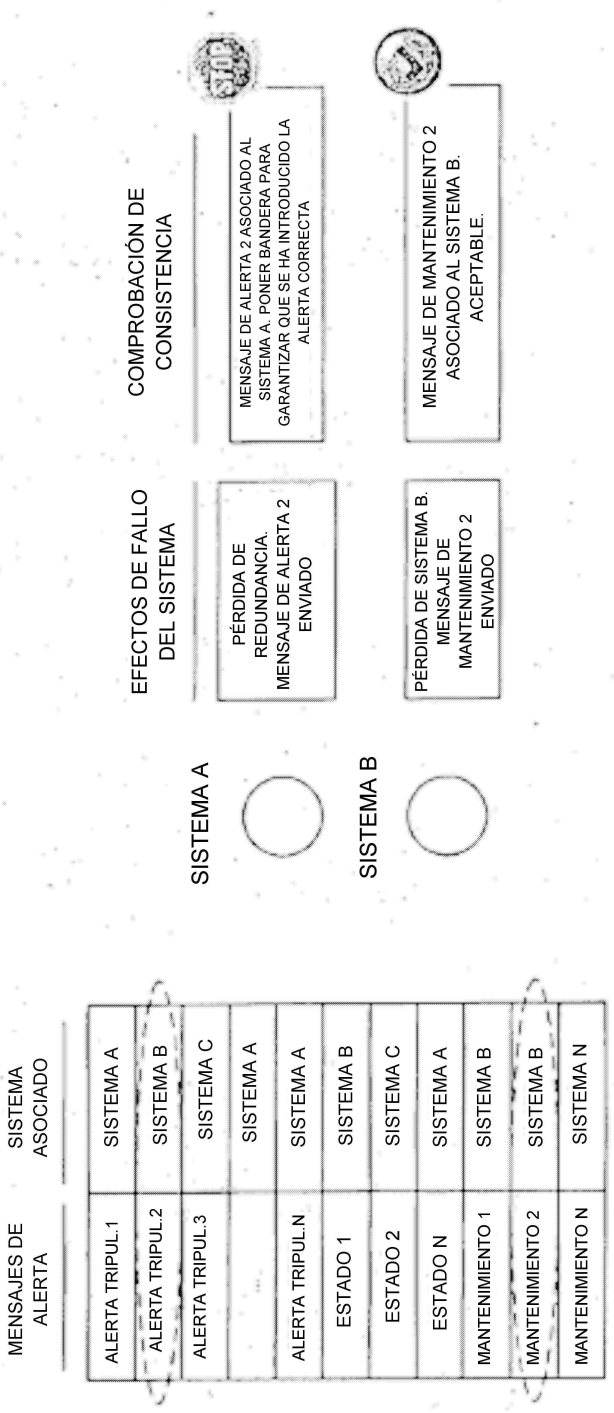

MENSAJES DE ALERTA
SISTEMA ASOCIADO
ALERTA TRIPUL.1
SISTEMA A
ALERTA TRIPUL.2
SISTEMA B
ALERTA TRIPUL.3
SISTEMA C
SISTEMA A
ALERTA TRIPUL.N
SISTEMA A
ESTADO 1
SISTEMA B
ESTADO 2
SISTEMA C
ESTADO N
SISTEMA A
MANTENIMIENTO 1
SISTEMA B
MANTENIMIENTO 2
SISTEMA B
MANTENIMIENTO N
SISTEMA N
EFECTOS DE FALLO DEL SISTEMA
COMPROBACIÓN DE CONSISTENCIA
SISTEMA A
PÉRDIDA DE REDUNDANCIA. MENSAJE DE ALERTA 2 ENVIADO
MENSAJE DE ALERTA 2 ASOCIADO AL SISTEMA A. PONER BANDERA PARA GARANTIZAR QUE SE HA INTRODUCIDO LA ALERTA CORRECTA
SISTEMA B
PÉRDIDA DE SISTEMA B. MENSAJE DE MANTENIMIENTO 2 ENVIADO
MENSAJE DE MANTENIMIENTO 2 ASOCIADO AL SISTEMA B. ACEPTABLE.

FIG. 5

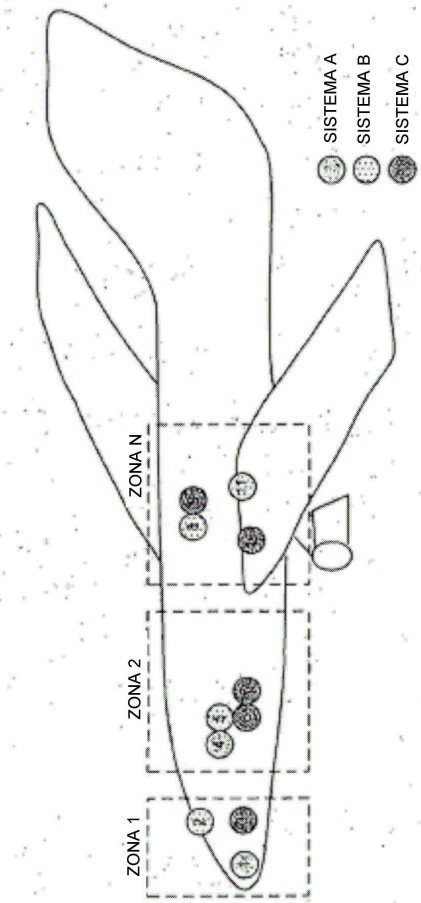

SISTEMA A
SISTEMA B
SISTEMA C
ZONA N
ZONA 2
ZONA 1

FIG. 6

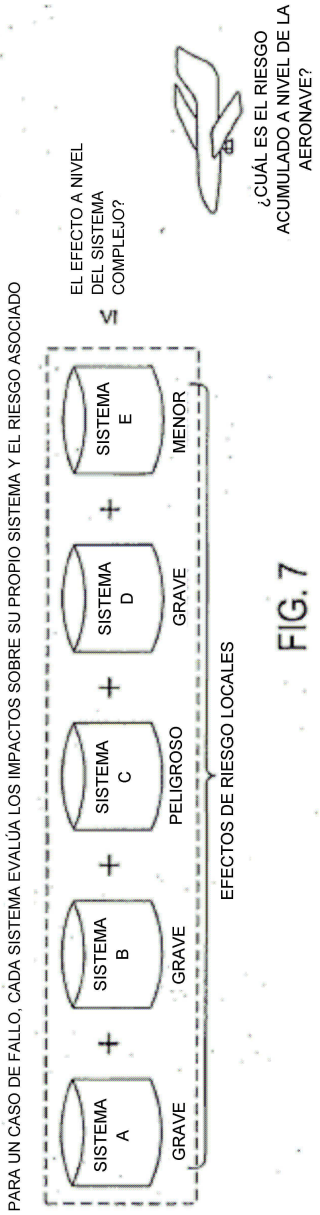

PARA UN CASO DE FALLO, CADA SISTEMA EVALÚA LOS IMPACTOS SOBRE SU PROPIO SISTEMA Y EL RIESGO ASOCIADO
SISTEMA A
GRAVE
+
SISTEMA B
GRAVE
+
SISTEMA C
PELIGROSO
+
SISTEMA D
GRAVE
+
SISTEMA E
MENOR
EFECTOS DE RIESGO LOCALES
EL EFECTO A NIVEL DEL SISTEMA COMPLEJO?
≤I
¿CUÁL ES EL RIESGO ACUMULADO A NIVEL DE LA AERONAVE?

FIG. 7

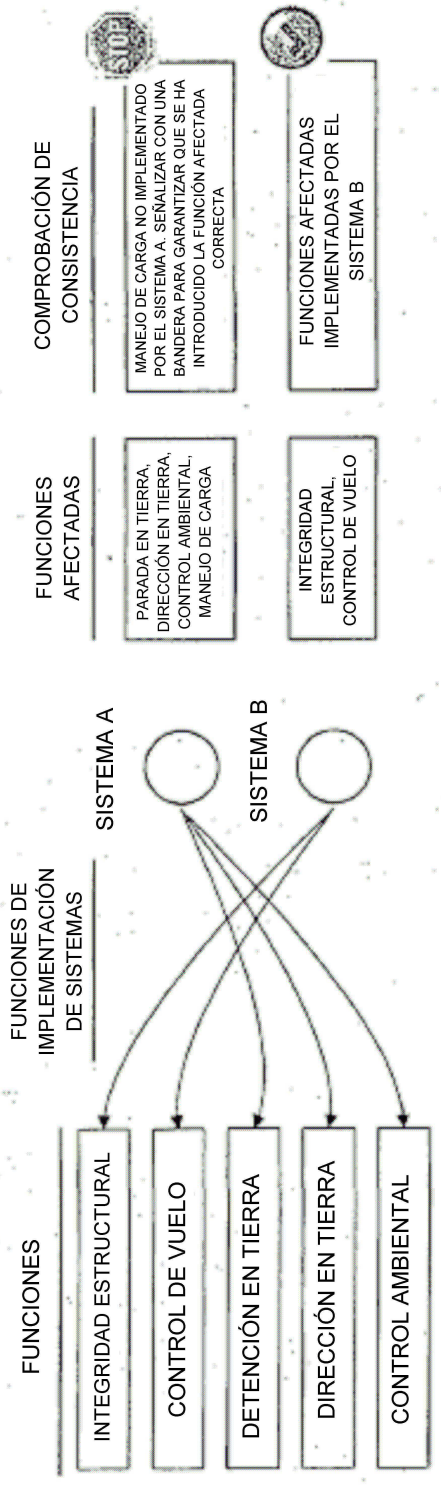

FUNCIONES
FUNCIONES DE IMPLEMENTACIÓN DE SISTEMAS
SISTEMA A
SISTEMA B
INTEGRIDAD ESTRUCTURAL
CONTROL DE VUELO
DETENCIÓN EN TIERRA
DIRECCIÓN EN TIERRA
CONTROL AMBIENTAL
FUNCIONES AFECTADAS
PARADA EN TIERRA, DIRECCIÓN EN TIERRA, CONTROL AMBIENTAL, MANEJO DE CARGA
INTEGRIDAD ESTRUCTURAL, CONTROL DE VUELO
COMPROBACIÓN DE CONSISTENCIA
STOP
MANEJO DE CARGA NO IMPLEMENTADO POR EL SISTEMA A. SEÑALIZAR CON UNA BANDERA PARA GARANTIZAR QUE SE HA INTRODUCIDO LA FUNCIÓN AFECTADA CORRECTA
FUNCIONES AFECTADAS IMPLEMENTADAS POR EL SISTEMA B

FIG. 8

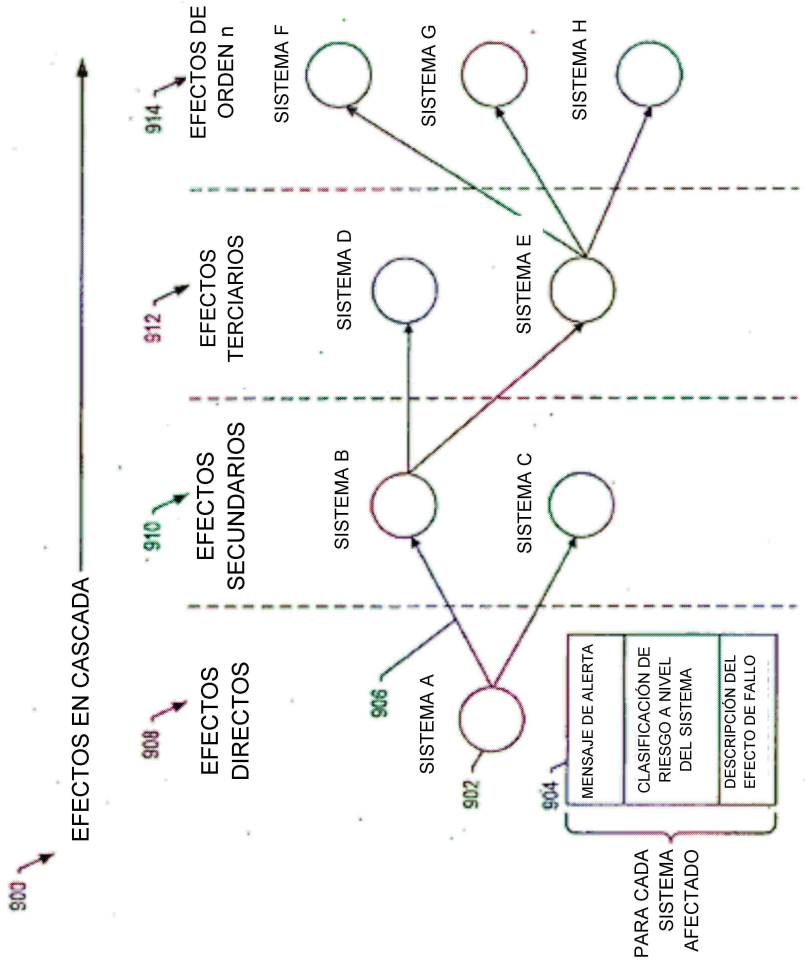

900
EFECTOS EN CASCADA
908
EFECTOS DIRECTOS
910
EFECTOS SECUNDARIOS
912
EFECTOS TERCIARIOS
914
EFECTOS DE ORDEN n
SISTEMA A
SISTEMA B
SISTEMA C
SISTEMA D
SISTEMA E
SISTEMA F
SISTEMA G
SISTEMA H
902
904
906
MENSAJE DE ALERTA
CLASIFICACIÓN DE RIESGO A NIVEL DEL SISTEMA
DESCRIPCIÓN DEL EFECTO DE FALLO
PARA CADA SISTEMA AFECTADO

FIG. 9

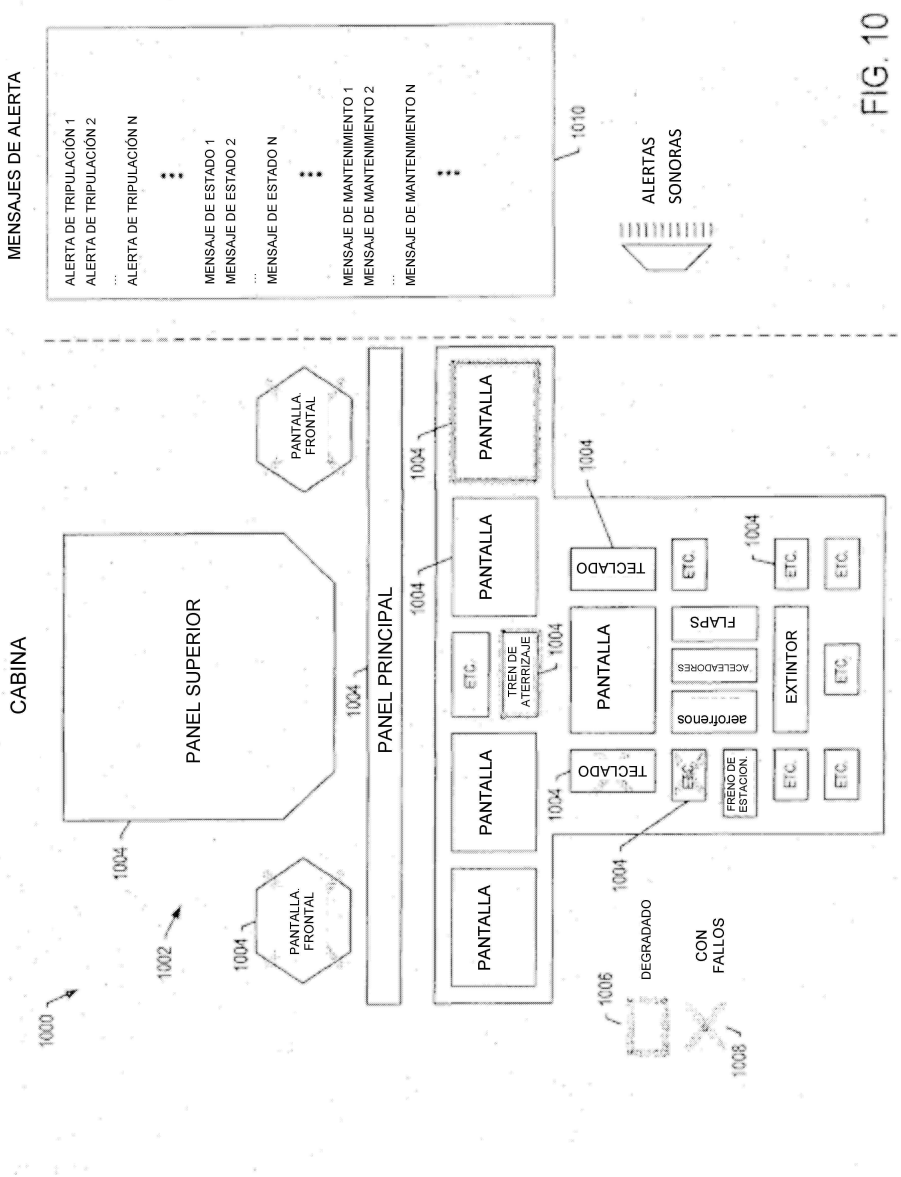

MENSAJES DE ALERTA
ALERTA DE TRIPULACIÓN 1
ALERTA DE TRIPULACIÓN 2
...
ALERTA DE TRIPULACIÓN N
MENSAJE DE ESTADO 1
MENSAJE DE ESTADO 2
...
MENSAJE DE ESTADO N
MENSAJE DE MANTENIMIENTO 1
MENSAJE DE MANTENIMIENTO 2
...
MENSAJE DE MANTENIMIENTO N
1010
ALERTAS SONORAS
CABINA
PANEL SUPERIOR
PANEL PRINCIPAL
PANTALLA FRONTAL
PANTALLA
TECLADO
ETC.
TREN DE ATERRIZAJE
FLAPS
ACELEADORES
aerofrenos
EXTINTOR
FRENO DE ESTACION
1000
1002
1004
1006
1008
DEGRADADO
CON FALLOS

FIG. 10

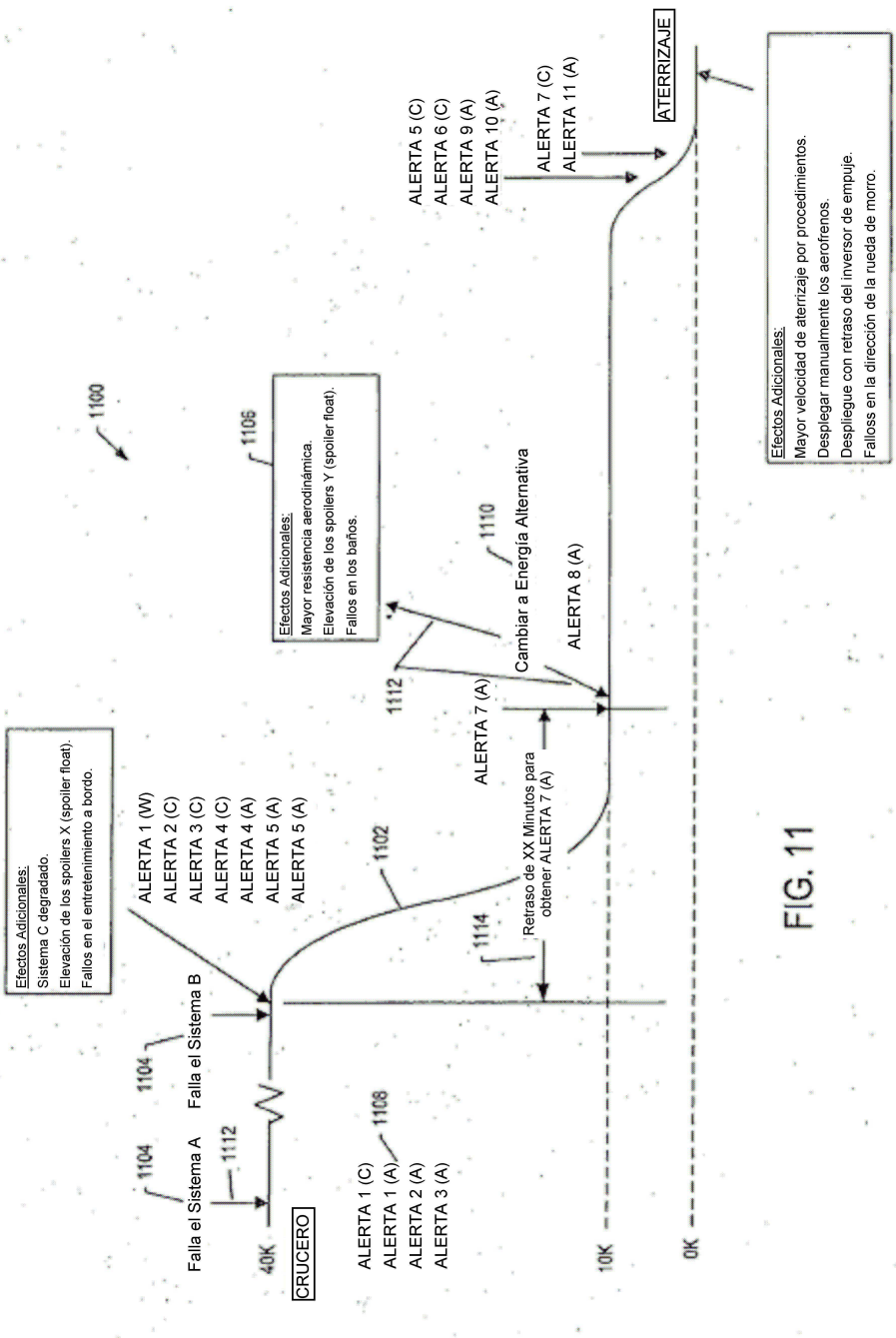
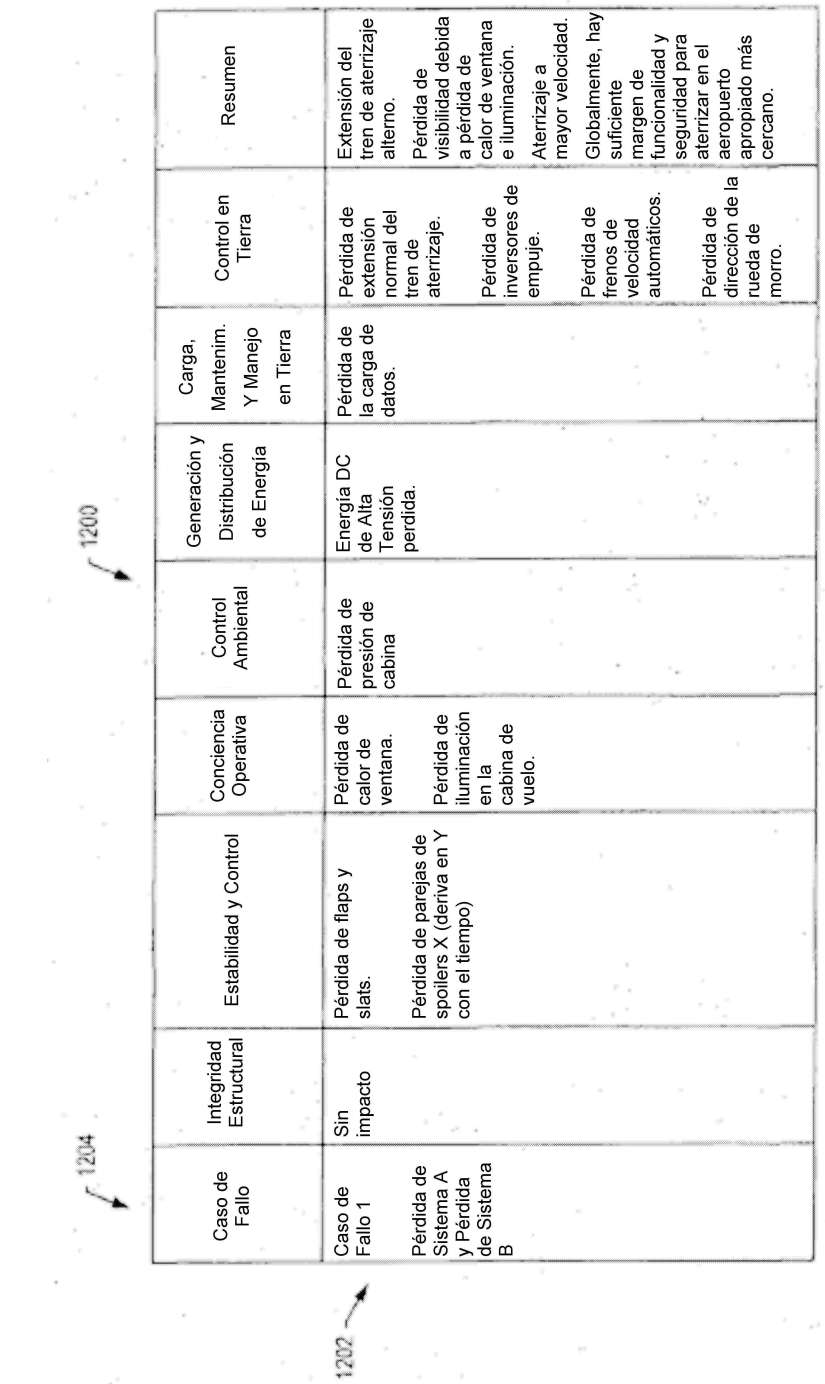

1100
1102
1104
1106
1108
1110
1112
1114
Efectos Adicionales:
Sistema C degradado.
Elevación de los spoilers X (spoiler float).
Fallos en el entretenimiento a bordo.
ALERTA 1 (W)
ALERTA 2 (C)
ALERTA 3 (C)
ALERTA 4 (C)
ALERTA 4 (A)
ALERTA 5 (A)
ALERTA 5 (A)
Falla el Sistema B
Falla el Sistema A
40K
CRUCERO
ALERTA 1 (C)
ALERTA 1 (A)
ALERTA 2 (A)
ALERTA 3 (A)
Efectos Adicionales:
Mayor resistencia aerodinámica.
Elevación de los spoilers Y (spoiler float).
Fallos en los baños.
Retraso de XX Minutos para obtener ALERTA 7 (A)
ALERTA 7 (A)
Cambiar a Energía Alternativa
ALERTA 8 (A)
ALERTA 5 (C)
ALERTA 6 (C)
ALERTA 9 (A)
ALERTA 10 (A)
ALERTA 7 (C)
ALERTA 11 (A)
ATERRIZAJE
10K
0K
Efectos Adicionales:
Mayor velocidad de aterrizaje por procedimientos.
Desplegar manualmente los aerofrenos.
Despliegue con retraso del inversor de empuje.
Falloss en la dirección de la rueda de morro.

FIG. 11



Caso de Fallo	Integridad Estructural	Estabilidad y Control	Conciencia Operativa	Control Ambiental	Generación y Distribución de Energía	Carga, Mantenim. Y Manejo en Tierra	Control en Tierra	Resumen
Caso de Fallo 1 Pérdida de Sistema A y Pérdida de Sistema B	Sin impacto	Pérdida de flaps y slats. Pérdida de parejas de spoilers X (deriva en Y con el tiempo)	Pérdida de calor de ventana. Pérdida de iluminación en la cabina de vuelo.	Pérdida de presión de cabina	Energía DC de Alta Tensión perdida.	Pérdida de la carga de datos.	Pérdida de extensión normal del tren de aterrizaje. Pérdida de inversores de empuje. Pérdida de frenos de velocidad automáticos. Pérdida de dirección de la rueda de morro.	Extensión del tren de aterrizaje alterno. Pérdida de visibilidad debida a pérdida de calor de ventana e iluminación. Aterrizaje a mayor velocidad. Globalmente, hay suficiente margen de funcionalidad y seguridad para aterrizar en el aeropuerto apropiado más cercano.

FIG. 12

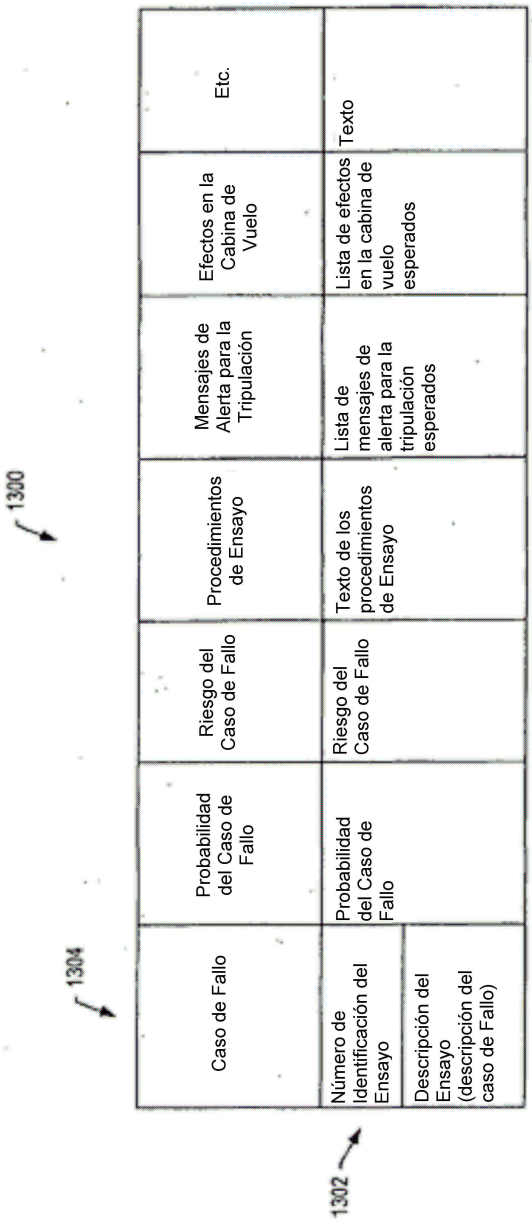

1300
1304
1302
Caso de Fallo
Número de Identificación del Ensayo
Descripción del Ensayo (descripción del caso de Fallo)
Probabilidad del Caso de Fallo
Probabilidad del Caso de Fallo
Riesgo del Caso de Fallo
Riesgo del Caso de Fallo
Procedimientos de Ensayo
Texto de los procedimientos de Ensayo
Mensajes de Alerta para la Tripulación
Lista de mensajes de alerta para la tripulación esperados
Efectos en la Cabina de Vuelo
Lista de efectos en la cabina de vuelo esperados
Etc.
Texto

FIG. 13