(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 947 581**

(51) Int. CI.:

G06F 30/00 (2010.01)
G06F 111/02 (2010.01)
G06F 111/08 (2010.01)
G06F 111/10 (2010.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.12.2018 PCT/FR2018/053454**

(87) Fecha y número de publicación internacional: **27.06.2019 WO19122747**

(96) Fecha de presentación y número de la solicitud europea: **20.12.2018 E 18842541 (7)**

(97) Fecha y número de publicación de la concesión europea: **07.06.2023 EP 3729302**

(54) Título: **Procedimiento y sistema de asistencia para la resolución de problemas de un sistema complejo**

(30) Prioridad:

22.12.2017 FR 1762945

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.08.2023

(73) Titular/es:

AIRBUS DEFENCE AND SPACE SAS (100.0%)
31 rue des Cosmonautes ZI du Palays
31402 Toulouse Cedex 4, FR

(72) Inventor/es:

MARTY, JEAN-LUC;
CANU, DAVID y
ARNOLD, ALEXANDRE

(74) Agente/Representante:

VEIGA SERRANO, Mikel

DESCRIPCIÓN

Procedimiento y sistema de asistencia para la resolución de problemas de un sistema complejo

Sector de la técnica

La presente invención se refiere al campo de la resolución de problemas en componentes de sistemas complejos. Más concretamente, se refiere a un procedimiento y un sistema de asistencia para la resolución de problemas de un sistema complejo.

Estado de la técnica

Un sistema complejo comprende generalmente una pluralidad de elementos unidos entre sí por numerosas interconexiones. Estos elementos pueden ser, por ejemplo, componentes mecánicos, electrónicos y/o componentes de software. Tales sistemas complejos existen en una gran variedad de ámbitos, como, por ejemplo, la industria, la automoción, el ferrocarril y la aviación. Estos sistemas complejos pueden plantear problemas a un operario de mantenimiento a la hora de localizar un fallo observado, por ejemplo, por un usuario de tal sistema, es decir, a la hora de determinar el componente o los componentes defectuosos causantes del fallo.

Estos sistemas complejos suelen contar con pruebas de diagnóstico o de buen funcionamiento diseñadas para detectar y localizar fallos. Algunas pruebas se basan en la técnica del árbol de fallos, que utiliza una descomposición arborescente del sistema complejo. Esta técnica se utiliza para determinar las combinaciones mínimas de sucesos que conducen a la pérdida de la función principal del sistema complejo, tal como una avería o un accidente.

La técnica del árbol de fallos permite evaluar la probabilidad de que se produzca el suceso temido, a partir de las combinaciones de sucesos elementales que pueden producirlo. De este modo, conociendo las probabilidades de estos sucesos elementales, es posible deducir la probabilidad del suceso temido y el impacto en esa probabilidad de una reducción (o aumento) de una u otra de las probabilidades de los sucesos elementales. Las probabilidades de los sucesos elementales se utilizan entonces para identificar el componente o los componentes defectuosos del sistema complejo que son la causa del fallo.

Es habitual que en un sistema complejo, un fallo tenga múltiples o diferentes causas potenciales. A menudo, estas causas potenciales no pueden someterse a prueba automáticamente. En este caso, debe enviarse a un operario de mantenimiento y un procedimiento de asistencia para la resolución de problemas (“troubleshooting” según el término en inglés) debe implementarse (véase, por ejemplo, el documento US 2017/312614 A1).

Hasta la fecha, este procedimiento de asistencia para la resolución de problemas en un sistema complejo mediante probabilidades elementales a partir de un árbol de fallos no es satisfactorio. De hecho, no hay nada que permita a un operario de mantenimiento aislar un fallo concreto que deba someterse a prueba de entre todos los fallos previstos. En este caso, el operario de mantenimiento puede tener que dedicar más tiempo del necesario a la resolución de problemas del sistema complejo, retrasando de este modo su retorno a un estado de funcionamiento normal del sistema complejo.

Objeto de la invención

Por tanto, la presente invención pretende superar tales desventajas proporcionando un procedimiento y un sistema de asistencia para la resolución de problemas de un sistema complejo.

Un primer objeto de la invención se refiere a un procedimiento de asistencia de diagnóstico para identificar un componente defectuoso que no está bajo supervisión automática de un sistema complejo que comprende una pluralidad de componentes mecánicos, eléctricos, electrónicos y/o de software conectados entre sí, estando cada uno de una parte de los componentes bajo supervisión automática, asociado a uno o más sensores de fallo, no estando una parte de los componentes bajo supervisión automática, comprendiendo el procedimiento, implementado por un procesador:

- recibir un fichero que contenga una modelización de la totalidad o de una parte del sistema complejo mediante un árbol de fallos que defina la totalidad o una parte de las combinaciones de sucesos que causan un suceso pico asociado a un fallo en el sistema complejo, comprendiendo el árbol de fallos una pluralidad de sucesos intermedios y una pluralidad de sucesos de base,

- asignar un valor de probabilidad de ocurrencia a priori a cada uno de los sucesos de base del árbol de fallos, con el fin de generar un árbol de fallos aumentado,

- asignar información de fallo a cada uno de los sucesos de base y a cada uno de los sucesos intermedios del árbol de fallos aumentado que estén asociados a un componente supervisado automáticamente, recibiéndose la información de fallo a partir de los sensores de fallos y describiendo una observación del estado operativo del

componente asociado al suceso del árbol de fallos aumentado,

- calcular un valor de probabilidad de ocurrencia a posteriori para cada uno de los sucesos del árbol de fallos aumentado, a partir de valores de probabilidad de ocurrencia a priori asignados y de información de fallos asignada,

- asignar un coste de resolución de problemas a cada uno de los sucesos del árbol de fallos aumentado que están asociados a un componente que no está bajo supervisión automática y del que pueden resolverse los problemas, definiendo el coste de resolución de problemas el tiempo necesario para resolver los problemas de dicho componente,

- modelizar, mediante un proceso de decisión de Markov, PDM, a partir del árbol de fallos aumentado, de una o varias evoluciones posibles del sistema complejo, en respuesta a al menos una acción de resolución de problemas por parte del operario de mantenimiento, de al menos un componente, correspondiendo la acción de resolución de problemas a un procedimiento de identificación del fallo o de la confirmación del buen funcionamiento del componente,

- determinar una secuencia óptima de acciones de resolución de problemas para el sistema complejo, según una política de decisión que minimice la expectativa de la suma de los costes de resolución de problemas y que se determine mediante la aplicación de un algoritmo de resolución de PDM.

En el procedimiento, la etapa de calcular un valor de probabilidad de ocurrencia a posteriori puede comprender las etapas de:

- construir una red bayesiana a partir del árbol de fallos aumentado, estando la red bayesiana diseñada para realizar predicciones sobre las relaciones entre los sucesos del árbol de fallos aumentado a partir de la información de fallos y valores de probabilidad a priori, etc.

- calcular el valor de probabilidad a partir de la red bayesiana.

Además, los nodos de la red bayesiana representan entidades correspondientes del sistema complejo, estando los arcos entre los nodos asociados con distribuciones de probabilidad condicional que representan probabilidades de sucesos asociados con algunas de las entidades del sistema complejo que están asociadas con sucesos asociados con otras entidades del sistema complejo.

En el procedimiento, la etapa de asignar un coste de resolución de problemas puede comprender la etapa de,

- obtener el coste de resolución de problemas a partir de una función de coste dependiente de al menos un término correspondiente al tiempo necesario para la resolución de problemas del componente y un término correspondiente a la dificultad de acceso físico para la resolución de problemas de dicho componente.

En el procedimiento, la etapa de modelización mediante PDM puede comprender la etapa de definición de PDM de horizonte finito según un cuadruplo {S,A,T,R} en el que,

- S es un conjunto que define los estados en los que puede encontrarse el sistema complejo en un momento t a partir de un estado inicial del sistema complejo,

- A es un conjunto que de fine acciones de resolución de problemas que pueden realizarse en función del estado del sistema complejo y que influyen en la evolución del estado actual del sistema complejo,

- T es una función de transición que define el conjunto de probabilidades de transición entre dos estados del sistema complejo en los estados t y t + 1, en respuesta a las acciones de resolución de problemas del conjunto A,

- R es una función de recompensa que define el conjunto de costes de resolución de problemas asociados a las acciones de resolución de problemas del conjunto A.

Además, cuando T define el conjunto de probabilidades de fallo, se alcanza un estado terminal de PDM cuando al menos una probabilidad de fallo de un suceso de base es igual a 1.

Además, cuando T define el conjunto de probabilidades de fallo, se alcanza un estado terminal de PDM cuando el conjunto de probabilidades de fallo es igual a 0.

Por último, cuando T define el conjunto de probabilidades de fallo, se alcanza un estado terminal de PDM cuando todos los nodos del sistema complejo que pueden ser sometidos a resolución de problemas tienen una probabilidad de fallo igual a 0 o 1.

Un segundo objeto de la invención se refiere a un producto de programa informático que comprende instrucciones

que, cuando son ejecutadas por un procesador, hacen que dicho procesador implemente un procedimiento según el primer objeto de la invención.

Un tercer objeto de la invención se refiere a un sistema de asistencia de diagnóstico para identificar un componente que no se encuentra bajo supervisión automática defectuoso de un sistema complejo que comprende una pluralidad de componentes mecánicos, eléctricos, electrónicos y/o de software conectados entre sí, estando cada uno de una parte de los componentes bajo supervisión automática, asociado con uno o más sensores de fallo, no estando una parte de los componentes bajo supervisión automática, comprendiendo el sistema un servidor de asistencia de diagnóstico y un dispositivo electrónico previstos para acceder a una red de comunicaciones:

- el servidor de asistencia al diagnóstico comprende un primer procesador configurado para implementar un procedimiento según el primer objeto de la invención, a partir de un fichero que contiene una modelización de la totalidad o parte del sistema complejo mediante un árbol de fallos que define la totalidad o parte de las combinaciones de sucesos causantes de un suceso pico asociado a un fallo en el sistema complejo, comprendiendo el árbol de fallos una pluralidad de sucesos intermedios y una pluralidad de sucesos de base,

- el dispositivo electrónico portátil comprende un segundo procesador acoplado a un dispositivo de entrada de usuario y a un dispositivo de visualización, en el que el segundo procesador está configurado para,

  - recibir la totalidad o parte de la secuencia óptima de acciones de resolución de problemas del sistema complejo a través de la red de comunicaciones,

  - visualizar en el dispositivo de visualización una imagen representativa de la acción actual de resolución de problemas que va a realizarse, a partir de la secuencia óptima de acciones de resolución de problemas del sistema complejo,

  - detectar una señal de entrada procedente del dispositivo de entrada de usuario que sea representativa de una entrada de usuario durante la visualización de la imagen representativa de la acción actual de resolución de problemas que va a realizarse,

  - en respuesta a una entrada de usuario indicativa de la detección de un fallo o de la confirmación del buen funcionamiento del componente asociado a la acción actual de resolución de problemas que va a realizarse, visualizar en el dispositivo de visualización una imagen representativa de la siguiente acción de resolución de problemas que va a realizarse, a partir de la secuencia óptima de acciones de resolución de problemas del sistema complejo.

En el sistema:

- el segundo procesador del dispositivo electrónico portátil está configurado además para enviar la entrada de usuario al primer procesador del servidor de asistencia a la resolución de problemas,

- en respuesta a la recepción de la entrada de usuario, el primer procesador está configurado además para,

- determinar la siguiente acción de resolución de problemas de la secuencia óptima de acciones de resolución de problemas del sistema complejo, y

- enviar la siguiente acción de resolución de problemas de la secuencia óptima de acciones de resolución de problemas del sistema al segundo procesador del dispositivo electrónico portátil.

Además, el dispositivo de entrada de usuario puede estar comprendido en el dispositivo de visualización.

Descripción de las figuras

Otras características y ventajas de la invención se comprenderán mejor al leer la siguiente descripción y con referencia a los dibujos adjuntos, proporcionados a título ilustrativo y en modo alguno limitativos.

La figura 1 representa un sistema de asistencia para la resolución de problemas de un sistema complejo según la invención.

La figura 2 representa un procedimiento de asistencia para la resolución de problemas de un sistema complejo según la invención.

La figura 3 representa un árbol de fallos.

La figura 4 representa un proceso de decisión de Markov.

Por motivos de claridad, los elementos representados no están dibujados a escala uno con respecto a otro, a menos que se indique lo contrario.

Descripción detallada de la invención

En el contexto de la descripción, por “sistema complejo” se entiende un sistema (o aparato, o incluso objeto) formado por un gran número de entidades eléctricas, electrónicas, de software, mecánicas y sus combinaciones que están conectadas entre sí. Por ejemplo, y de manera no limitativa, puede tratarse de un vehículo automóvil, una aeronave, una central nuclear, un sistema de satélites o cualquier sistema informático. Además, se asume que el sistema complejo se modela mediante un árbol de fallos que define la totalidad o parte de las combinaciones de sucesos que causan un suceso pico asociado a un fallo del sistema complejo. En este contexto, el árbol de fallos comprende una pluralidad de sucesos intermedios y una pluralidad de sucesos de base.

El principio general de la invención se basa en el hecho de que los procedimientos de resolución de problemas (“troubleshooting” según el término en inglés) se llevan a cabo en entidades no supervisadas de un sistema complejo. La no supervisión significa que un operario de mantenimiento de un sistema complejo no dispone de ninguna información sobre el estado de funcionamiento de las entidades que van a someterse a resolución de problemas. Esto hace que sea muy difícil hacer frente rápidamente a las consecuencias de un fallo y garantizar la mantenibilidad del sistema complejo. La mantenibilidad se define generalmente como la capacidad de un activo para mantenerse o restaurarse en un estado en el que pueda realizar una función requerida. Esto se consigue cuando el mantenimiento se lleva a cabo en condiciones dadas, utilizando procedimientos y medios prescritos.

De este modo, un operario de mantenimiento se ve a menudo obligado a someter a prueba las entidades posiblemente defectuosas del sistema complejo una a una en un orden arbitrario. En este proceso, el operario de mantenimiento observa entonces periódicamente un sistema dinámico complejo que, en el momento de la observación, se ve influido por una decisión. Esta decisión se toma a partir de un conjunto de acciones posibles, es decir, el conjunto de entidades que pueden someterse a prueba en un estado determinado del sistema complejo. En otras palabras, la evolución del sistema complejo es el resultado de la interacción, a lo largo del tiempo, de leyes de transición aleatorias del sistema complejo y de la elección de una secuencia de acciones realizadas por el operario de mantenimiento.

Los inventores han identificado que un procedimiento de resolución de problemas de este tipo puede modelarse mediante un proceso de decisión de Markov (“Markov Decisión Process” según el término en inglés). De hecho, los procesos de decisión de Markov son un enfoque de optimización utilizado para resolver problemas de toma de decisiones secuenciales, en cada paso temporal, en un entorno incierto, lo que corresponde al problema identificado por los inventores. Los procesos de decisión de Markov permiten calcular una política que indica la acción que debe realizarse en función del estado del sistema. Según la invención, se propone combinar la técnica del árbol de fallos con un proceso de decisión de Markov. El objetivo de esto es determinar de manera óptima la secuencia de acciones de resolución de problemas necesarias para hacer frente rápidamente a las consecuencias de un fallo y garantizar la mantenibilidad del sistema complejo.

La figura 1 ilustra un sistema 100 para la resolución de problemas en un sistema complejo (no representado). El sistema 100 comprende un servidor 110 de asistencia para la resolución de problemas y un dispositivo 120 electrónico portátil, ambos dispuestos para acceder a una red 130 de comunicaciones. En una realización particular, el sistema 100 comprende una pluralidad de servidores 110 de asistencia para la resolución de problemas y/o una pluralidad de dispositivos 120 electrónicos portátiles. En una realización, el dispositivo 120 electrónico no es portátil. En otra realización, el servidor 110 de asistencia para la resolución de problemas y el dispositivo 120 electrónico están comprendidos en el mismo equipo informático.

El servidor 110 de asistencia para la resolución de problemas comprende un primer procesador 111 configurado para ejecutar, al menos parcialmente, un procedimiento de asistencia para la resolución de problemas de un sistema complejo. El procedimiento se describirá a continuación con referencia a la figura 2. Por el momento, basta con señalar que el procedimiento según la invención es capaz de determinar una secuencia óptima de acciones de resolución de problemas para el sistema complejo.

El dispositivo 120 electrónico portátil comprende un segundo procesador 121 acoplado a un dispositivo 122 de entrada de usuario y un dispositivo 123 de visualización. En una realización particular, el dispositivo 122 de entrada de usuario está comprendido en el dispositivo 123 de visualización. En un ejemplo de esta realización, el dispositivo 123 de visualización es una pantalla que comprende un panel táctil en la totalidad o parte de una superficie de visualización de la pantalla.

En el ejemplo de la figura 1, el segundo procesador 121 está configurado para recibir la totalidad o parte de la secuencia óptima de acciones de resolución de problemas del sistema complejo a través de la red 130 de comunicaciones. Tal como se señaló anteriormente, el primer procesador 111 del servidor 110 de asistencia para la resolución de problemas determina la secuencia óptima de acciones de resolución de problemas del sistema complejo. Además, el segundo procesador 121 está configurado para visualizar en el dispositivo 123 de

visualización una imagen representativa de la acción actual de resolución de problemas que va a realizarse, por un operario de mantenimiento, a partir de la secuencia óptima de acciones de resolución de problemas del sistema complejo. En un ejemplo, la imagen representativa de la acción actual de resolución de problemas que va a realizarse contiene texto y/o símbolos que se refieren a la acción actual de resolución de problemas que va a realizarse.

El segundo procesador 121 también está configurado para detectar una señal de entrada procedente del dispositivo 121 de entrada de usuario que es representativa de una entrada de usuario durante la visualización de la imagen representativa de la acción actual de resolución de problemas que va a realizarse. En respuesta a una entrada de usuario que es indicativa de la detección, por parte de un operario de mantenimiento del sistema complejo, de un fallo o de la confirmación del funcionamiento correcto de la entidad asociada con la acción actual de resolución de problemas que va a realizarse, el segundo procesador 121 está configurado para visualizar en el dispositivo 123 de visualización una imagen representativa de la siguiente acción de resolución de problemas que va a realizarse, a partir de la secuencia óptima de acciones de resolución de problemas del sistema complejo.

El sistema 100 según la invención tiene como efecto que el operario de mantenimiento de un sistema complejo ya no esté obligado a someter a prueba las entidades potencialmente defectuosas del sistema complejo en un orden arbitrario. En efecto, según la invención, una primera acción de resolución de problemas que va a realizarse en el sistema complejo se determina primero a nivel del servidor 110 de asistencia para la resolución de problemas. A continuación, se visualiza en el dispositivo 120 electrónico portátil la siguiente acción de resolución de problemas que va a realizarse por el operario de mantenimiento en función del resultado observado tras la acción de resolución de problemas anterior de la entidad actual por parte del operario de mantenimiento. Por último, el conjunto de acciones de resolución de problemas se incluye en la secuencia óptima de acciones de resolución de problemas del sistema complejo.

En una realización particular del sistema 100, el segundo procesador 121 del dispositivo 120 electrónico portátil está configurado además para enviar la entrada de usuario al primer procesador 111 del servidor 110 de asistencia para la resolución de problemas a través de la red 130 de comunicaciones. A partir de entonces, en respuesta a la recepción de la entrada de usuario, el primer procesador 111 está configurado además para determinar la siguiente acción de resolución de problemas de la secuencia óptima de acciones de resolución de problemas del sistema complejo al segundo procesador del dispositivo electrónico portátil.

Esta implementación particular tiene como efecto reducir el número de cálculos necesarios para determinar la secuencia óptima de acciones de resolución de problemas que deben realizarse. De hecho, en esta implementación, los cálculos se realizan a medida que el operario de mantenimiento del sistema complejo realiza la resolución de problemas.

La figura 2 ilustra un procedimiento 200 de asistencia para la resolución de problemas de un sistema complejo según la invención, tal como se ha mencionado anteriormente.

Tal como se ha indicado anteriormente, se considera que el sistema complejo se modela mediante un árbol de fallos que define la totalidad o parte de las combinaciones de sucesos que causan un suceso pico asociado a un fallo del sistema complejo. En este contexto, el árbol de fallos comprende una pluralidad de sucesos intermedios y una pluralidad de sucesos de base. En la invención, los sucesos de base del árbol de fallos aumentado se consideran independientes.

La figura 3 ilustra un ejemplo de árbol 300 de fallos. Los símbolos utilizados para representar un árbol de fallos están normalizados, tal como propone la norma NF EN 61025 “Análisis de árbol de fallos” (para la versión en inglés, IEC 61025 “Fault tree analysis”). Un árbol de fallos puede representarse en forma de fichero, tal como propone, por ejemplo, la organización Open PSA Initiative (en inglés “Open Probabilistic Safety Assessment Initiative”; https://openpsa.github.io. En el ejemplo del formato Open PSA, se trata de un fichero de lenguaje extensible de marcas (“XML” según sus siglas en inglés).

De este modo, en el ejemplo de la figura 3, un árbol de fallos tal como el árbol 300 de fallos puede contener un suceso 310 pico, sucesos 320 intermedios, sucesos 330 de base, conectores 340 OU y conectores 350 ET. Los sucesos 310, 320 están representados por rectángulos dentro de los cuales aparecen las etiquetas de estos sucesos. El suceso 310 pico y los sucesos 320 intermedios pueden descomponerse en una combinación, de modo que debajo de la casilla que los representa aparece el símbolo del conector 340, 350 que une los sucesos cuya combinación es necesaria y suficiente para causarla. Los sucesos 330 de base o condiciones 360 no se descomponen, de modo que inmediatamente debajo de la casilla que los representa hay un símbolo particular: un círculo para los sucesos de base y un pentágono (en forma de casa) para las condiciones. El símbolo del triángulo 370 puede utilizarse para saltar de una página a otra. Por ejemplo, el símbolo del triángulo 370 se coloca debajo de un suceso intermedio cuya descomposición comienza en otra página, en donde este suceso aparece en primer lugar. El símbolo del conector 340 OU se diferencia del símbolo del conector 350 ET porque su base cóncava sobresale hacia arriba, mientras que el otro tiene una base recta y horizontal. Por supuesto, otros elementos no mencionados en este caso también pueden formar parte del árbol 300 de fallos, en función de la norma utilizada.

Volviendo al proceso 200 de la figura 2, en la etapa 210, se asigna un valor de probabilidad de ocurrencia a priori a cada uno de los sucesos de base del árbol de fallos, con el fin de generar un árbol de fallos aumentado. Por ejemplo, con el formato Open PSA, esto puede implicar la creación de un nuevo atributo XML en el fichero que describe el árbol de fallos.

Se conoce que el valor de probabilidad de ocurrencia a priori de un fallo se asimila a su frecuencia de ocurrencia futura estimada en el sistema complejo. El valor de probabilidad de ocurrencia a priori suele ser diferente de la frecuencia histórica y puede desviarse, para un sistema complejo dado, de la probabilidad de ocurrencia media evaluada en un conjunto de sistemas complejos similares. Dicho de otro modo, la probabilidad de ocurrencia puede considerarse como la probabilidad de que se haya producido un fallo entre un primer momento (por ejemplo, la puesta en servicio del sistema complejo o la última renovación completa del sistema complejo) y un segundo momento, conocido como momento de la misión, correspondiente a la etapa 210.

En una implementación particular de la etapa 210, el valor de probabilidad de ocurrencia a priori se obtiene a partir de una función de distribución que caracteriza la ley de probabilidad de fallo específica de cada suceso de base del árbol de fallos.

En un ejemplo, la ley probabilidad de fallo para un suceso de base dado es una ley exponencial, por lo que su función de distribución se describe mediante la siguiente fórmula:

$$Q(t) = \begin{cases} 1 - e^{-\lambda t} & \lambda \geq 0 \\ 0 & \lambda < 0 \end{cases} \quad (1),$$

en donde t representa el momento y λ es el parámetro de intensidad de la ley exponencial que representa una tasa de fallos. En este ejemplo, t puede inicializarse en el momento de misión, tal como se ha mencionado anteriormente.

En otro ejemplo, la ley de probabilidad de fallo es una ley estadística seleccionada de un grupo que consiste en la ley exponencial, la ley normal, la ley lognormal, la ley Weibull, la ley Gamma y combinaciones de las mismas.

En una implementación particular de la etapa 210, el valor de probabilidad de ocurrencia a priori puede estimarse o actualizarse a partir de datos observados en el mundo físico (por ejemplo, retroalimentación) por el operario de mantenimiento.

Posteriormente, en la etapa 220, se asigna información sobre fallos a cada uno de los sucesos de base y a cada uno de los sucesos intermedios del árbol de fallos aumentado que están asociados a una entidad bajo supervisión automática. Tal como se ha mencionado anteriormente, esto puede implicar la creación de un nuevo atributo XML en el fichero que describe el árbol de fallos aumentado. En la invención, una entidad está “bajo supervisión automática” cuando existe un medio para observar el estado operativo de esta entidad. El medio de observación del estado operativo de la entidad puede ser un medio humano (por ejemplo, los ojos del operario de mantenimiento) o un medio automático (por ejemplo, un dispositivo electrónico de supervisión). Según la invención, se considera que la información sobre fallos describe una observación del estado operativo de la entidad asociada al suceso del árbol de fallos aumentado.

En un ejemplo, la información de fallo es binaria. En este ejemplo, un primer estado binario indica que el suceso intermedio en cuestión ha fallado, mientras que un segundo estado binario indica que el suceso intermedio en cuestión funciona normalmente.

En una implementación particular de la etapa 220, la información de fallo se recibe desde uno o más sensores de fallo asociados con una o más entidades.

A continuación, en la etapa 230, se calcula un valor de probabilidad de ocurrencia a posteriori para cada uno de los sucesos del árbol de fallos aumentado, a partir de los valores de probabilidad de ocurrencia a priori asignados y de información de fallos asignada. Para ello, puede utilizarse la teoría de la probabilidad. Además, para tener en consideración el hecho de que una entidad bajo supervisión automática esté fallando o no, también deberá determinarse la probabilidad condicional de un suceso que conozca que otro suceso se haya realizado o no.

En una implementación particular de la etapa 230, se construye una red bayesiana a partir del árbol de fallos aumentado y se calcula el valor de probabilidad a partir de la red bayesiana.

En efecto, se conoce que un árbol de fallos cuyos sucesos de base están asociados a probabilidades simples es un caso particular de red bayesiana (véase a este respecto, por ejemplo, M. Bouissou, 2008, “Gestion de la complexité dans les études quantitatives de sûreté de fonctionnement de systèmes”, Eyrolles; M. Bouissou, 2000. “Deux méthodes originales pour calculer les performances d’un système possédant des états de fonctionnement dégradé”. Congreso 12 sobre fiabilidad y mantenibilidad, Montpellier, 2000; A. Bobbio, L. Portinale, M. Minichino, E.

Ciancamerla, 2001. “Improving the analysis of dependable systems by mapping fault trees into Bayesian networks”. Reliability Engineering & System Safety. Volumen 71, número 3, marzo de 2001, páginas 249-260).

En esta implementación particular, la red bayesiana pretende realizar predicciones sobre las relaciones entre los sucesos del árbol de fallos aumentado a partir de la información sobre los fallos y los valores de probabilidad a priori. Para ello, los nodos de la red bayesiana representan entidades correspondientes del sistema complejo. Además, los arcos entre los nodos están asociados a distribuciones de probabilidad condicionales que representan probabilidades de sucesos asociados a ciertas entidades del sistema complejo que están asociadas a sucesos asociados a otras entidades del sistema complejo.

En la etapa 240, se asigna un coste de resolución de problemas a cada uno de los sucesos del árbol de fallos aumentado que están asociados a una entidad que no está bajo supervisión automática y que puede someterse a resolución de problemas. En la invención, se dice que una entidad puede “someterse a resolución de problemas” si el operario de mantenimiento puede acceder a la misma para determinar si la entidad ha fallado o no. Según la invención, se considera que el coste de resolución de problemas define la dificultad para que el operario de mantenimiento identifique el fallo de la entidad asociada con el suceso en el árbol de fallos aumentado. En otras palabras, el coste de resolución de problemas es una pérdida relacionada con la dificultad de determinar si una entidad ha fallado. Por ejemplo, el coste de resolución de problemas puede utilizarse para definir la dificultad de acceso físico del operario de mantenimiento a la entidad posiblemente averiada.

En la invención, se considera que, tras una acción de resolución de problemas de una entidad por parte del operario de mantenimiento, la posible evolución del sistema complejo irá acompañada de efectos económicos medibles. De este modo, se ha elegido definir el coste de resolución de problemas como criterio económico que permite comparar los efectos medidos, con el fin de elegir las acciones que controlen la resolución de problemas del sistema complejo de manera óptima. El coste de resolución de problemas permite, por tanto, medir el efecto económico de una acción de resolución de problemas dada en un estado dado del sistema complejo. El problema resuelto de este modo por la invención consiste en determinar una secuencia de acciones de resolución de problemas que va a realizarse para minimizar el efecto económico total esperado, conociendo la distribución de probabilidad del estado inicial del sistema complejo.

En una implementación particular de la etapa 240, se obtiene el coste de resolución de problemas a partir de una función de coste dependiente de al menos un término que corresponde a una medición o estimación de la dificultad de identificar el fallo por el operario de mantenimiento de la entidad. Por ejemplo, la función de coste se elige de un grupo que consiste en una función lineal a trozos, una función exponencial y sus combinaciones. Además, por ejemplo, el término de la función de coste se elige de un grupo que consiste en el tiempo necesario para la resolución de problemas de la unidad, el número de personas necesarias para la resolución de problemas de la entidad, el coste monetario necesario para la resolución de problemas de la entidad, la dificultad de acceso para la resolución de problemas de la entidad y sus combinaciones.

En la etapa 250, se modela mediante un proceso de decisión de Markov, a partir del árbol de fallos aumentado, una o varias evoluciones posibles del sistema complejo, en respuesta a al menos una acción de resolución de problemas por el operario de mantenimiento, de al menos una entidad. Según la invención, se considera que la acción de resolución de problemas corresponde a un procedimiento para identificar el fallo o confirmar el buen funcionamiento de la entidad.

Como recordatorio, un proceso de decisión de Markov es un proceso de control estocástico discreto. En cada etapa, el proceso se encuentra en un determinado estado s, y un agente elige una acción a. La probabilidad de que el proceso alcance el estado s’ viene determinada por la acción elegida. Más concretamente, se describe mediante la función de transición de estados T(s,a,s’). Por tanto, el estado s’ depende del estado actual s y de la acción a seleccionada por el decisor. Sin embargo, para una s y una a, el estado siguiente es independiente de los estados y acciones anteriores. Se dice entonces que el proceso cumple la propiedad de Markov. Por último, cuando el proceso pasa del estado s al s’, el agente obtiene una recompensa positiva o negativa R(s,a,s’).

En una implementación particular de la etapa 250, se define el proceso de decisión de Markov en un horizonte finito según un cuadruplo {S,A,T,R} en el que,

- S es un conjunto que define los estados en los que puede encontrarse el sistema complejo en un momento t, a partir de un estado inicial del sistema complejo,

- A es un conjunto que define las acciones de resolución de problemas que pueden realizarse en función del estado del sistema complejo y que influyen en la evolución del estado actual del sistema complejo,

- T es una función de transición que define el conjunto de probabilidades de transición entre dos estados del sistema complejo en los estados t y t + 1, en respuesta a las acciones de resolución de problemas del conjunto A. En una implementación de la invención, T(s,a,s’) corresponde a la probabilidad de pasar al estado s’, cuando la acción a se realiza en el estado s y se considera que la entidad asociada a la acción a ha fallado. De este modo, en esta

implementación, T(s,a,s') es una probabilidad de fallo,

- R es una función de recompensa que define el conjunto de costes de resolución de problemas asociados a las acciones de resolución de problemas del conjunto A. En la invención, la recompensa es negativa y, por tanto, corresponde a un coste. De este modo, R(s,a,s') es el coste percibido tras realizar la acción a en el estado s que conduce al sistema al estado s'.

La figura 4 ilustra un proceso 400 de decisión de Markov que modela la evolución de un sistema complejo durante la resolución de problemas, según la dinámica de Markov. El ejemplo de proceso 400 de decisión de Markov se describirá ahora según el formalismo mencionado anteriormente.

El conjunto S del proceso 400 de decisión de Markov se define según la fórmula siguiente:

$$S = \{ S0, S1, S2, S3, S4, S5, S6, S7, S8, S9, S10, S11, S12 \} \quad (2),$$

en donde el estado S0 representa el estado inicial del sistema complejo en el momento t = 0. En una implementación particular, t se inicializa en el momento en que comienza la resolución de problemas del sistema complejo. En el ejemplo de la figura 4, los estados S1 y S2 pueden alcanzarse, partiendo del estado S0, bajo la influencia de la acción a3.

El conjunto A del proceso 400 de decisión de Markov se define según la fórmula siguiente

$$A = \{ a1, a2, a3, a4 \} \quad (3),$$

en donde los índices 1, 2, 3 y 4 se refieren a una entidad del sistema complejo. De este modo, la acción a1 corresponde a la acción de resolución de problemas asociada a la entidad 1 del sistema complejo. En el ejemplo de la figura 4, en un estado dado del conjunto S, una acción de resolución de problemas que haya concluido que la entidad en cuestión funciona correctamente se representa mediante un círculo que comprende el texto "OK". Por otra parte, una acción de resolución de problemas que ha concluido que la entidad en cuestión ha fallado se representa mediante un círculo que comprende el texto "KO". Por último, una acción de resolución de problemas que aún no se ha llevado a cabo se representa mediante un círculo que comprende un signo de interrogación. De este modo, en la figura 4, el estado S0 describe la siguiente situación:

- se considera que la entidad 1 funciona correctamente,

- se considera que la entidad 2 presenta fallos, y

- las entidades 3 y 4 aún no se han sometido a prueba.

El conjunto T del proceso 400 de decisión de Markov se define según la fórmula siguiente

$$T = \{ p1, p2, p3, p4, p5, p6, p7, p8, p9, p10, p11, p12 \} \quad (4).$$

En la invención, una probabilidad p de la función T de transición corresponde a la probabilidad de que la entidad sometida a prueba falle.

Gracias a la asignación de un valor de probabilidad de ocurrencia a priori a cada uno de los sucesos de base del árbol de fallos aumentado asociado al sistema complejo, es posible determinar las probabilidades pi. En efecto, estas probabilidades corresponden a probabilidades condicionales definidas según la fórmula siguiente:

$$T(s, a, s') = P(X_{t+1} = s' \mid X_t = s, A_t = a) \quad (5).$$

De este modo, en el ejemplo de la figura 4, la probabilidad p6 se obtiene calculando la probabilidad condicional de que la entidad 4 falle, sabiendo que el estado anterior es S2. En forma matemática, el cálculo puede formularse de la siguiente manera:

$$p6 = (X_{t+1} = S6 \mid X_t = S2, A_t = a4) = P(S6 \mid S2, a4) \quad (6)$$

Para este cálculo, puede utilizarse una red bayesiana como la mencionada anteriormente.

El conjunto R del proceso 400 de decisión de Markov se define según la siguiente fórmula R = {c1,c2} (6). En el ejemplo de la figura 4, c1 corresponde al coste asociado a la realización de la acción 3, y c2 corresponde al coste asociado a la realización de la acción 4.

En la etapa 260, se determina sucesivamente una secuencia óptima de acciones de resolución de problemas del

sistema complejo, según una política de decisión que minimiza la expectativa de la suma de los costes de resolución de problemas y que se determina aplicando un algoritmo de resolución del proceso de decisión de Markov. En la invención, la expectativa de un coste de recuperación de problemas asociado a una acción se define como el producto de la probabilidad de transición bajo la influencia de la acción y el coste de resolución de problemas asociado a esta acción. De este modo, la política de decisión obtenida mediante la resolución del proceso de decisión de Markov proporcionará la acción de resolución de problemas que debe realizarse en todos los estados del conjunto S observados sucesivamente tras los resultados de las acciones de resolución de problemas anteriores. Sin embargo, también está previsto utilizar algoritmos en los que la política de decisión obtenida mediante la resolución del proceso de decisión de Markov proporcionará el conjunto de acciones de resolución de problemas que deben tenerse en cuenta en todos los estados que teóricamente podría adoptar el conjunto S.

Mediante la resolución del proceso de decisión de Markov, se obtiene una política que indica la acción óptima que debe realizarse en cada estado del sistema complejo. Por tanto, con una única política, la secuencia de acciones finalmente elegida dependerá de la evolución real del proceso.

En un ejemplo, el algoritmo para resolver un proceso de decisión de Markov se elige de un grupo formado por iteración de valores (value iteration según el término en inglés), Q-Learning, SARSA, UCT, programación dinámica, iteración de políticas y aprendizaje por diferencia temporal.

En una primera implementación particular (no representada), se determina un estado terminal del proceso de decisión de Markov en el que ya no se realizan acciones. En otras palabras, en el estado terminal del proceso de decisión de Markov, el procedimiento 200 ya no proporciona al operario de mantenimiento ninguna acción que realizar. El efecto de esta implementación es fomentar un rápido retorno a un estado estable del sistema complejo.

En esta implementación particular, se tiene en consideración el caso en el que T define el conjunto de probabilidades de fallo, como se ha indicado anteriormente.

En este caso, se considera que se ha alcanzado un estado terminal del proceso de decisión de Markov cuando el estado actual del proceso de decisión de Markov satisface la(s) siguiente(s) condición(es), tomada(s) sola(s) o combinada(s):

- se identifica un suceso de base como defectuoso. Este será el caso, por ejemplo, cuando al menos una probabilidad de fallo de un suceso de base sea igual a 1;

- todos los sucesos de base se identifican como no defectuosos. Este será el caso, por ejemplo, cuando el conjunto de probabilidades de fallo sea igual a 0; y

- no puede realizarse ninguna acción de resolución de problemas. Este será el caso, por ejemplo, cuando todos los nodos que pueden someterse a resolución de problemas del sistema complejo tengan una probabilidad de fallo igual a 0 o 1.

REIVINDICACIONES

1. Procedimiento (200) de asistencia de diagnóstico de un sistema complejo que comprende una pluralidad de componentes mecánicos, eléctricos, electrónicos y/o de software conectados entre sí, estando cada uno de los componentes de una parte de los componentes bajo supervisión automática y asociado a uno o más sensores de fallo, no estando una parte de los componentes bajo supervisión automática, comprendiendo el procedimiento, implementado por un procesador:

- recibir un fichero que contiene una modelización de la totalidad o parte del sistema complejo mediante un árbol (300) de fallos que define la totalidad o parte de las combinaciones de sucesos causantes de un suceso (310) pico asociado a un fallo del sistema complejo, comprendiendo el árbol de fallos una pluralidad de sucesos (320) intermedios y una pluralidad de sucesos (330) de base,

- asignar (210) un valor de probabilidad de ocurrencia a priori a cada uno de los sucesos de base del árbol de fallos, con el fin de generar un árbol de fallos aumentado,

- asignar (220) información de fallo a cada uno de los sucesos de base y a cada uno de los sucesos intermedios del árbol de fallos aumentado que estén asociados a un componente bajo supervisión automática, recibiéndose la información de fallo a partir de los sensores de fallo y describiendo una observación del estado operativo del componente asociado al suceso del árbol de fallos aumentado,

- calcular (230) un valor de probabilidad de ocurrencia a posteriori, para cada uno de los sucesos del árbol de fallos aumentado, a partir de los valores de probabilidad de ocurrencia a priori asignados y de información de fallos asignada,

- asignar (240) un coste de resolución de problemas a cada uno de los sucesos del árbol de fallos aumentado que están asociados a un componente que no está bajo supervisión automática y que puede someterse a resolución de problemas, definiendo el coste de resolución de problemas el tiempo necesario para la resolución de problemas de dicho componente,

- modelar (250), mediante un proceso de decisión de Markov, PDM, a partir del árbol de fallos aumentado, una o varias evoluciones posibles del sistema complejo, en respuesta a al menos una acción de resolución de problemas por el operario de mantenimiento, de al menos un componente, correspondiendo la acción de resolución de problemas a un procedimiento de identificación de fallos o de confirmación del correcto funcionamiento del componente,

- determinar (260) una secuencia óptima de acciones de resolución de problemas del sistema complejo, según una política de decisión que minimiza la expectativa de la suma de los costes de resolución de problemas y que se determina aplicando un algoritmo de resolución de PDM.

2. Procedimiento según la reivindicación 1, en el que la etapa de calcular un valor de probabilidad de ocurrencia a posteriori comprende las etapas de:

- construir una red bayesiana a partir del árbol de fallos aumentado, proporcionándose la red bayesiana para realizar predicciones sobre las relaciones entre los sucesos del árbol de fallos aumentado a partir de la información sobre fallos y los valores de probabilidad a priori, y

- calcular el valor de probabilidad a partir de la red bayesiana.

3. Procedimiento según la reivindicación 2, en el que los nodos de la red bayesiana representan componentes correspondientes del sistema complejo, estando los arcos entre los nodos asociados con distribuciones de probabilidad condicional que representan probabilidades de sucesos asociados con algunos de los componentes del sistema complejo que están asociados con sucesos asociados con otros componentes del sistema complejo.

4. Procedimiento según las reivindicaciones anteriores, en el que la etapa de asignación de un coste de resolución de problemas comprende la etapa de obtención del coste de resolución de problemas a partir de una función de coste dependiente de al menos un término que corresponde al tiempo necesario para la resolución de problemas del componente y un término que corresponde a la dificultad de acceso físico para la resolución de problemas de dicho componente.

5. Procedimiento según las reivindicaciones anteriores, en el que la etapa de modelización mediante PDM comprende la etapa de definición de PDM de horizonte finito según un cuadruplo {S,A,T,R} en el que,

- S es un conjunto que define los estados en los que puede encontrarse el sistema complejo en un momento t, a partir de un estado inicial del sistema complejo,

- A es un conjunto que define las acciones de resolución de problemas que pueden realizarse en función del estado del sistema complejo y que influyen en la evolución del estado actual del sistema complejo,

- T es una función de transición que define el conjunto de probabilidades de transición entre dos estados del sistema complejo en los estados t y t + 1, en respuesta a las acciones de resolución de problemas del conjunto A,

- R es una función de recompensa que define el conjunto de costes de resolución de problemas asociados a las acciones de resolución de problemas del conjunto A.

6. Procedimiento según la reivindicación 5, en el que, cuando T define el conjunto de probabilidades de fallo, se alcanza un estado terminal de PDM cuando al menos una probabilidad de fallo de un suceso de base es igual a 1.

7. Procedimiento según la reivindicación 5, en el que, cuando T define el conjunto de probabilidades de fallo, se alcanza un estado terminal de PDM cuando el conjunto de probabilidades de fallo es igual a 0.

8. Procedimiento según la reivindicación 5 en el que, cuando T define el conjunto de probabilidades de fallo, se alcanza un estado terminal de PDM cuando todos los nodos que pueden someterse a resolución de problemas del sistema complejo tienen una probabilidad de fallo igual a 0 o 1.

9. Producto de programa informático que comprende instrucciones que, cuando son ejecutadas por un procesador, hacen que dicho procesador implemente un procedimiento según cualquiera de las reivindicaciones anteriores.

10. Sistema (100) de asistencia de diagnóstico de un sistema complejo que comprende una pluralidad de componentes mecánicos, eléctricos, electrónicos y/o informáticos conectados entre sí, estando cada uno de los componentes de una parte de los componentes bajo supervisión automática y asociado a uno o varios sensores de fallo, no estando una parte de los componentes bajo supervisión automática, comprendiendo el sistema un servidor (110) de asistencia de diagnóstico y un dispositivo (120) electrónico, ambos proporcionados para acceder a una red (130) de comunicaciones:

- el servidor de asistencia de diagnóstico comprende un primer procesador (111) configurado para implementar un procedimiento (200) según una cualquiera de las reivindicaciones 1 a 8, a partir de un fichero que contiene una modelización de la totalidad o parte del sistema complejo mediante un árbol (300) de fallos que define la totalidad o parte de las combinaciones de sucesos causantes de un suceso (310) pico asociado a un fallo del sistema complejo, comprendiendo el árbol de fallos una pluralidad de sucesos (320) intermedios y una pluralidad de sucesos (330) de base,

- el dispositivo electrónico portátil comprende un segundo procesador (121) acoplado a un dispositivo (122) de entrada de usuario y a un dispositivo (123) de visualización, en el que el segundo procesador está configurado para,

  - recibir la totalidad o parte de la secuencia óptima de acciones de resolución de problemas del sistema complejo a través de la red de comunicaciones,

  - visualizar en el dispositivo de visualización de una imagen representativa de la acción actual de resolución de problemas que va a realizarse, a partir de la secuencia óptima de acciones de resolución de problemas del sistema complejo,

  - detectar una señal de entrada procedente del dispositivo de entrada de usuario que es representativa de una entrada de usuario durante la visualización de la imagen representativa de la acción actual de resolución de problemas que va a realizarse,

  - en respuesta a una entrada de usuario que es indicativa de la detección de un fallo o de la confirmación del funcionamiento correcto del componente asociado a la acción actual de resolución de problemas que va a realizarse, visualizar en el dispositivo de visualización una imagen representativa de la siguiente acción de resolución de problemas que va a realizarse, a partir de la secuencia óptima de acciones de resolución de problemas del sistema complejo.

11. Sistema según la reivindicación 10, en el que,

- el segundo procesador del dispositivo electrónico portátil está configurado además para enviar la entrada de usuario al primer procesador del servidor de asistencia de diagnóstico,

- en respuesta a la recepción de la entrada de usuario, el primer procesador está configurado además para,

  - determinar la siguiente acción de resolución de problemas de la secuencia óptima de acciones de resolución de problemas del sistema complejo, y

- enviar la siguiente acción de solución de problemas de la secuencia óptima de acciones de resolución de problemas del sistema complejo al segundo procesador del dispositivo electrónico portátil.

12. Sistema según las reivindicaciones 10 u 11, en el que el dispositivo de entrada de usuario está comprendido en el dispositivo de visualización.

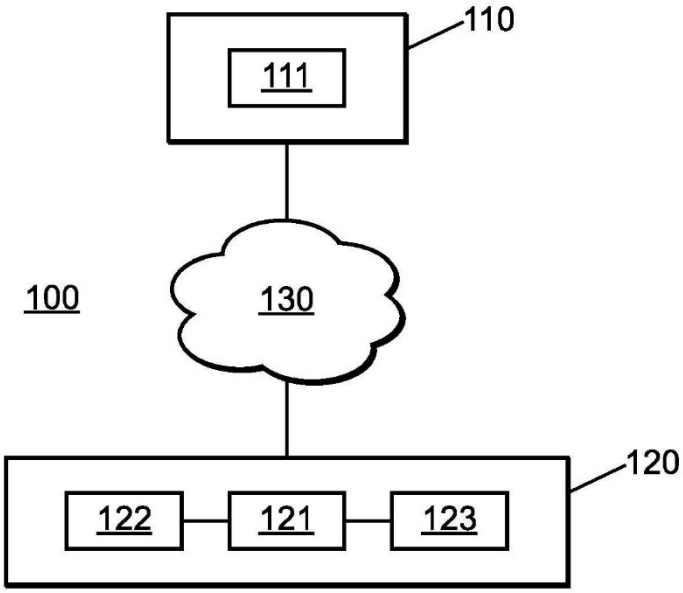

FIG. 1

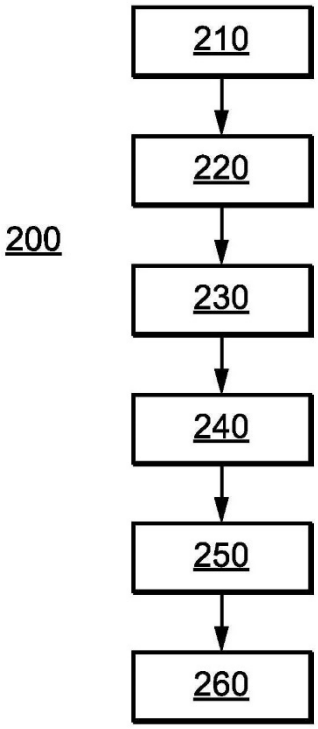

FIG. 2

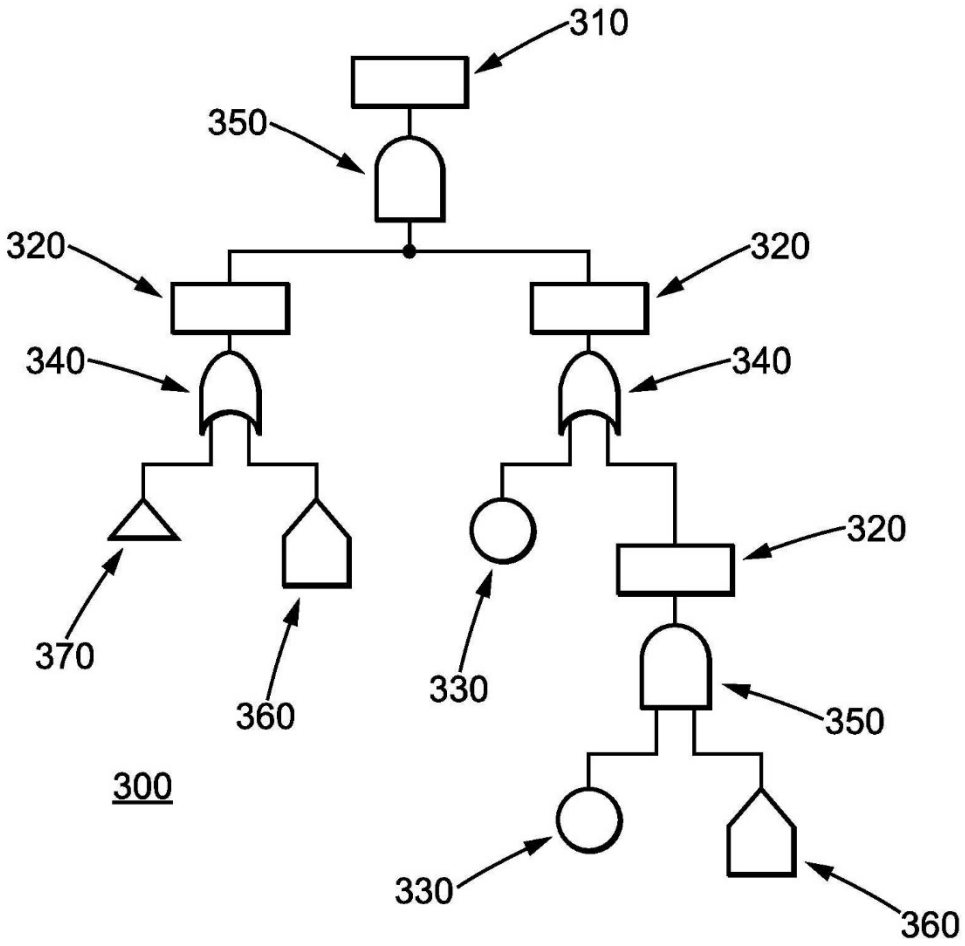

FIG. 3

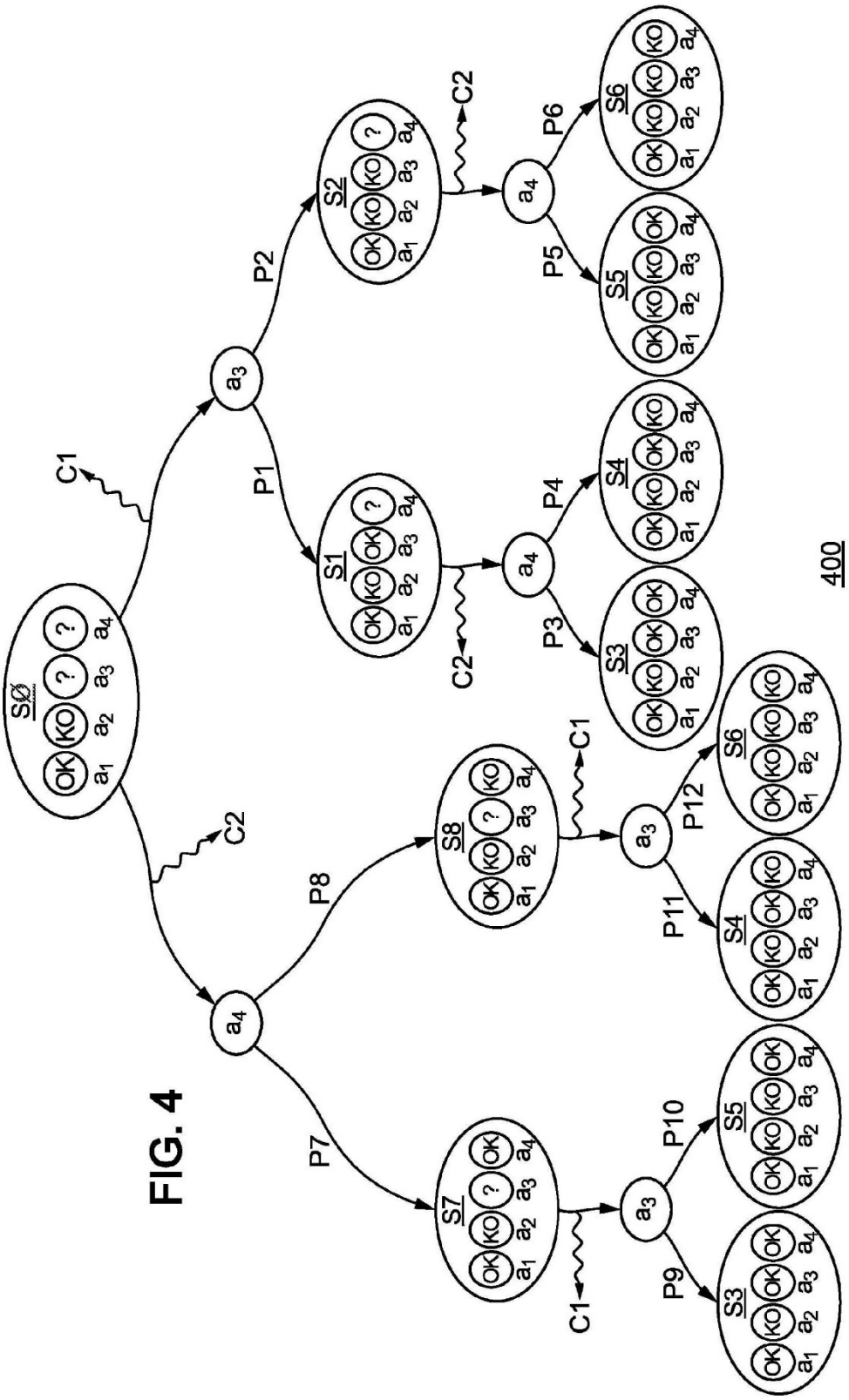
SØ
S1
S2
S3
S4
S5
S6
S7
S8
C1
C2
P1
P2
P3
P4
P5
P6
P7
P8
P9
P10
P11
P12
400

FIG. 4