(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 021 011**

(51) Int. CI.:

G06F 21/57 (2013.01)
H04L 9/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **30.09.2021 PCT/EP2021/076985**

(87) Fecha y número de publicación internacional: **07.04.2022 WO22069657**

(96) Fecha de presentación y número de la solicitud europea: **30.09.2021 E 21786841 (3)**

(97) Fecha y número de publicación de la concesión europea: **01.01.2025 EP 4200734**

(54) Título: **Procedimiento para la operación de una red y producto de programación informática**

(30) Prioridad:

30.09.2020 DE 102020212405

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
26.05.2025

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.00%)
Werner-von-Siemens-Straße 1
80333 München, DE

(72) Inventor/es:

HOLST, FLORIAN y
WALTER, MARCEL

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Procedimiento para la operación de una red y producto de programación informática

La invención se refiere a un procedimiento para la operación de una red con al menos un punto final con al menos un recurso de red o para administrar al menos un recurso de red, así como a un producto de programación informática.

Las redes de empresas y plantas de producción están expuestas regularmente a numerosos ataques de terceros. Por lo tanto, garantizar la seguridad informática es de gran importancia. En el estado de la técnica se conocen los documentos US 8 874 685 B1, US 9 762 582 B1, US 2007/143851 A1, US 2016/373478 A1 y US 2014/046645 A1.

Por lo tanto, el objetivo de la invención es crear un procedimiento para operar una red que pueda ejecutarse de forma segura y que tenga una opción de automatización.

El procedimiento de la invención es un procedimiento según la reivindicación 1 para operar una red con al menos un punto final con al menos un recurso de red o administrar al menos un recurso de red. El procedimiento de la invención comprende los siguientes pasos:

- Definir un conjunto de reglas con al menos una regla para el al menos un punto final,
- Observar la conformidad del al menos un punto final con el conjunto de reglas,
- Asignar una puntuación en función de la conformidad y
- Determinar al menos una medida en función de la puntuación.

Idealmente, el procedimiento de la invención es un procedimiento implementado por ordenador.

Mediante el procedimiento de la invención, la red puede ser operada de manera ventajosa de acuerdo con los requisitos de seguridad informática. Convenientemente, el conjunto de reglas incluye reglas de seguridad informática, de modo que el procedimiento de la invención permite asegurar fácilmente las redes, por ejemplo, en empresas o plantas de fabricación.

Preferiblemente, en el procedimiento de la invención, la al menos una medida comprende una limitación de privilegios del punto final en la red en función de la puntuación. De este modo, la administración de los recursos de la red puede limitarse a un subconjunto de privilegios menos críticos para la seguridad.

En los procedimientos según la invención, la al menos una medida comprende preferiblemente la interrupción del funcionamiento de la red. En el caso extremo de que no sea posible continuar con el funcionamiento de la red, se puede considerar la interrupción del funcionamiento de la red.

En el procedimiento según la invención, el al menos un punto final se forma preferiblemente con al menos un recurso de red y/o al menos un hardware administrador, preferiblemente un ordenador cliente y/o un hardware de autenticación, y/o al menos una interfaz de hardware, preferiblemente una cuenta de usuario. Ventajosamente, el ordenador cliente o el hardware de autenticación, como una tarjeta de identificación de la empresa legible electrónicamente, puede estar vinculado a una cuenta de administrador, de modo que solo un administrador pueda conectarse al punto final.

En un desarrollo avanzado ventajoso del procedimiento de la invención, el recurso de red, que es al menos uno, está formado por un hardware, en particular un servidor, y/o por un software, en particular un sistema operativo y/o un programa de aplicación, para su aplicación por medio de la red.

En un desarrollo avanzado ventajoso del procedimiento de la invención, el punto final forma una interfaz de administrador.

En el procedimiento según la invención, el conjunto de reglas establece preferiblemente la regularidad de una actualización del software y/o de un software en el hardware.

En un desarrollo avanzado ventajoso del procedimiento según la invención, la medida comprende una limitación de privilegios administrativos y/o una modificación de la conexión del punto final a la red, por ejemplo, una desconexión del punto final de la red, y/o una formación para un administrador que se conecte al punto final.

En el último caso mencionado del desarrollo avanzado mencionado, resulta conveniente asignar la puntuación en al menos dos categorías y adaptar la formación, preferiblemente mediante módulos, en función de la puntuación en las categorías, preferiblemente en función de la ocupación de las categorías y/o del peso absoluto y/o relativo de las categorías.

De manera adecuada, en un desarrollo avanzado de la invención, un administrador no será admitido en la red hasta que haya recibido la formación.

Preferiblemente, en el procedimiento de la invención, la puntuación se asigna o se mantiene en función de una formación, preferiblemente repetida, y/o de una verificación, preferiblemente repetida.

El producto de programa informático según la invención de la reivindicación 11 está diseñado para su aplicación en el procedimiento según la invención tal como se ha descrito anteriormente. El producto de programa informático según la invención está diseñado para almacenar un conjunto de reglas con al menos una regla para el al menos un punto final, para recibir datos de observación sobre la conformidad del al menos un punto final con el conjunto de reglas, así como para asignar una puntuación en función de la conformidad.

A continuación, la invención se explica con más detalle mediante un ejemplo de realización representado en el dibujo. La única figura de dibujo 1 muestra una red empresarial con recursos de red que se administran mediante la red empresarial, esquemáticamente en sección transversal.

La red 10 mostrada en la Fig. 1 es una red empresarial y tiene ordenadores conectados entre sí. Algunos de los ordenadores de la red 10 forman servidores 30 distribuidos para recursos de red. Otros de los ordenadores de la red 10 están configurados como ordenadores cliente 50 para la administración de los servidores 30. Tanto los servidores 30 como los ordenadores cliente 50 constituyen puntos finales de la red 10, que introducen contenidos o servicios en la red 10 como servidores 30 o proporcionan una interfaz a un administrador para tareas administrativas como ordenadores cliente 50. En el ejemplo de ejecución representado, la red 10 está diseñada como una red en la nube. En esta red en la nube, los servidores 30 no existen como ordenadores separados, aislados entre sí en cuanto a su hardware respectivo, sino que los servidores 30 existen como servidores lógicos 30 en el sentido de una base de datos distribuida almacenada en una multitud de ordenadores de la red 10. En otros ejemplos de ejecución no representados explícitamente, la red 10 también puede estar configurada como cualquier otra red convencional, por ejemplo, una red jerárquica 10, en la que los servidores 30 están presentes como servidores de hardware separados y físicamente independientes.

Los servidores 30 están configurados para ejecutar un software de coordinación de proyectos por medio de la red 10. Mediante el software de coordinación de proyectos los usuarios pueden introducir hitos del proyecto en el sistema y coordinarlos entre sí en cuanto a su consecución, de modo que un usuario obtenga una visión general rápida del estado de un proyecto, así como del cumplimiento de sus obligaciones en cuanto a los hitos del proyecto.

La red contiene además un servidor central 60 de gestión de derechos que concede o deniega derechos de acceso a los recursos de la red.

La red 10 también tiene una unidad de observación 70 que vigila el estado de seguridad de la red 10. La unidad de observación 70 comprueba periódicamente o de forma continua el estado de actualización de los sistemas operativos de los servidores 30, por ejemplo, el estado de actualización de los sistemas Linux de los servidores 30. En esto, la unidad de observación 70 compara la actualización del sistema operativo respectivo con una actualización objetivo del sistema operativo, que corresponde, por ejemplo, a una recomendación de un mantenedor de repositorios de una distribución del sistema Linux. Si, por ejemplo, no se han armonizado los parches actuales del sistema Linux, se calcula una puntuación que se asigna al servidor 30 respectivo en función del período durante el cual no se ha actualizado el sistema Linux a pesar de que hubiera sido posible hacerlo, así como en función del número y la criticidad de los parches, que se deriva de una clasificación realizada por los desarrolladores o por los mantenedores del repositorio. Por ejemplo, la puntuación contiene una suma de una magnitud proporcional al período de tiempo mencionado anteriormente (por ejemplo, una indicación del período de tiempo en horas con un factor de proporcionalidad) y una magnitud que suma una medida (por ejemplo, un valor de "5" para "altamente crítico", un valor de "3" para "crítico" y un valor de "1" para "recomendado") para la criticidad de seguridad de cada parche que haya faltado a pesar de estar disponible. De esta manera, a cada servidor 30 se le asigna una puntuación para la seguridad del sistema operativo, que es tanto más alta cuanto más o más graves sean las vulnerabilidades de seguridad del respectivo servidor 30.

También se asigna una puntuación similar al software de coordinación de proyectos en función de los parches o actualizaciones disponibles para este.

La suma de la puntuación del software de coordinación de proyectos y de la puntuación del sistema operativo constituye una puntuación total para el servidor 30, que se asigna al servidor 30 como certificado. Si la puntuación total supera un primer umbral crítico, esta puntuación total o la información sobre la superación de este primer umbral se transmite al servidor de gestión de derechos 60 que, al superar el primer umbral, inicia una medida para aumentar la seguridad de la red 10. La medida puede consistir, por ejemplo, en un funcionamiento restringido del servidor 30 en modo de emergencia o, en caso de que se supere significativamente el valor umbral, por ejemplo, en un factor del 50 %, en la desconexión del servidor 30 o de la red 10.

Además, esta puntuación total no se asigna únicamente al servidor 30. Más bien, la puntuación total también se asigna al administrador respectivo (no se muestra explícitamente en el dibujo), que es responsable de actualizar el servidor 30 y el software de coordinación del proyecto. Esta asignación se realiza o bien a un ordenador cliente 50 del administrador respectivo o, en caso de un posible cambio de los ordenadores cliente 50 del administrador respectivo a una cuenta de administrador, al acceso privilegiado del administrador a la red 10.

La asignación de una puntuación total al servidor 30, así como la atribución de un valor de puntuación a la cuenta de administrador, se realiza en el ejemplo de ejecución mostrado mediante una cuenta de puntuación asignada de forma unívoca al servidor 30 y a la cuenta de administrador. Las cuentas de puntuación del servidor 30 y de los administradores se mantienen en el servidor de gestión de derechos 60.

En el ejemplo de ejecución mostrado, la asignación se realiza a una cuenta de administrador que, en el ejemplo de ejecución mostrado, está asignada de forma unívoca a un administrador concreto. A la cuenta de administrador solo se le atribuyen los valores de puntuación que corresponden al software del que es responsable el administrador de la cuenta de administrador, es decir, aquellos para los que el administrador de la cuenta de administrador asume realmente tareas de actualización.

La gestión de derechos se describe en la figura 2:

Para poder ser admitido como administrador de un servidor 30 de la red 10, un administrador debe completar una formación en ciberseguridad (CYTR) que informa sobre un conjunto de reglas administrativas de seguridad vinculantes para la red 10. Las normas relevantes para la seguridad comprenden, entre otras cosas, los requisitos para la instalación oportuna y tan completa como posible de parches. Si el administrador completa la formación en ciberseguridad CYTR, se le otorgará un certificado de administrador ISDL. Sobre la base del certificado de administrador ISDL, se añade a la cuenta de administrador una firma criptográfica, como firma de administrador, que lo autoriza como administrador del servidor 30.

Al mismo tiempo, el propio servidor 30 debe cumplir también los requisitos de seguridad, que se resumen en una configuración nominal del sistema SYSOPC, lo que significa que todo el software instalado en el servidor 30 debe estar actualizado, en este caso el sistema operativo y el software de coordinación de proyectos. Tras comprobar que la configuración del servidor 30 cumple con la configuración nominal del sistema SYSOPC, se le concede al servidor 30 una autorización de servidor ISLP para la red 10. Debido a la autorización del servidor ISLP para la red 10, al servidor 30 se le otorga otra firma criptográfica en forma de firma de servidor, que identifica al servidor 30 como al menos inicialmente suficiente para la configuración nominal del sistema SYSOPC. Mediante la firma del servidor, el servidor 30 es autorizado a integrarse en la red 10.

En el ejemplo de ejecución mostrado, un administrador se registra en la red 10 para administrar un servidor 30 de la siguiente manera:

En primer lugar, UACREQ se autentica como administrador ante la red 10 de la forma habitual. Para ello, utiliza su cuenta de administrador para enviar un identificador único a la red 10. El servidor de gestión de derechos 60 comprueba si el administrador dispone de un certificado de administrador mediante la firma de administrador asignada al identificador. Si es así, se determina una cuenta de administrador basándose en la firma del administrador y se identifica la cuenta de puntuación asignada a esta cuenta de administrador. Se comprueba si el valor de puntuación registrado en la cuenta de puntuación supera el primer umbral. Si el valor de puntuación está por debajo del primer umbral, el administrador continúa con el inicio de sesión en la red 10. Si el valor de la puntuación está por encima del primer valor umbral, el administrador es rechazado por la red 10.

A continuación, el administrador selecciona un servidor 30 en el que se ejecuta el software de coordinación de proyectos y que él administra. El servidor 30 comprueba si el administrador ha sido registrado previamente en UREGSYS para administrar el servidor 30. Si no es así, el servidor 30 rechaza al administrador. Si el administrador está registrado para administrar el servidor 30, se continúa con el inicio de sesión del administrador.

Por último, el servidor de gestión de derechos 60 comprueba, basándose en la firma del servidor 30, si este cumple actualmente con la configuración nominal del sistema SYSOPC. Si es así, el administrador recibe permiso OPALL para administrar el servidor 30. Si, por el contrario, el servidor 30 no cumple actualmente la configuración nominal de sistema SYSOPC, se revoca el permiso de servidor ISLP.

En el ejemplo de ejecución mostrado, la autorización de servidor ISLP del servidor 30 y el certificado de administrador ISDL para administrar el servidor 30 no solo se validan para la autorización inicial de los administradores y el servidor 30 a la red 10. Más bien, el mantenimiento del certificado de administrador ISDL depende del valor de puntuación de la cuenta de puntuación de la cuenta de administrador perteneciente al administrador, y la autorización del servidor ISLP depende del valor de puntuación de la cuenta de puntuación del servidor 30. Así, la unidad de observación 70 comprueba periódica o continuamente el estado de actualización de los sistemas operativos de los servidores 30. Si el valor de puntuación de la cuenta de puntuación de la cuenta de administrador perteneciente al administrador supera el primer umbral, el servidor

de gestión de derechos 60 excluye al administrador de la administración del servidor 30. Además, el servidor 30 también se desconecta de la red 10. En otros ejemplos de ejecución no mostrados explícitamente, el administrador no queda excluido de la administración posterior del servidor 30, sino que se envía un mensaje correspondiente a un responsable de seguridad de la red 10, que indica el correspondiente rebasamiento del primer valor umbral. Además, el servidor 30 no se desconecta de la red 10, sino que se envía un mensaje al responsable de seguridad de la red 10 para que pueda examinar la situación más detenidamente.

Si un administrador de un servidor 30 de una red 10 supera la cuenta de puntuación que se le ha asignado, el servidor de gestión de derechos 60 puede imponerle una formación, tras la cual se le volverá a conceder el certificado de administrador ISDL. En particular, el valor de la puntuación puede determinarse en varias dimensiones, por ejemplo, respectivamente en relación con el software del servidor 30 que haya sido configurado por este, por ejemplo, con el software de coordinación de proyectos y con un sistema operativo del servidor 30. Si, al superar el primer umbral del valor de puntuación de la cuenta de puntuación asignada al administrador a través de la cuenta de administrador, se determina que el rebosamiento se debe en gran medida a una actualización defectuosa del sistema operativo del servidor 30, luego la formación puede prever automáticamente una mayor ponderación de los contenidos relacionados con el sistema operativo del servidor 30. Para ello, los valores de puntuación se registran convenientemente en las dimensiones, es decir, en las categorías, para las que se dispone de contenidos de formación modularizados. En el ejemplo de ejecución mostrado, los contenidos de formación están modularizados en 5 a 10 categorías, que se incluyen en una formación para administradores cuando las categorías tienen asignadas inscripciones al superarse el valor de puntuación. Las categorías a las que no se les ha asignado un valor de puntuación distinto de cero, o bien no se tienen en cuenta en absoluto al ponderar la formación, o bien se tienen en cuenta con un contenido estándar que difiere del contenido de la formación complementaria, que se incluye en la formación para el administrador cuando la categoría tiene asignado un valor de puntuación distinto de cero. En el ejemplo de ejecución mostrado, los módulos de la formación se combinan automáticamente mediante un software del servidor de gestión de derechos 60.

REIVINDICACIONES

1. Procedimiento para operar una red (10) con al menos un punto final (50) que administra al menos un recurso de red (30), que comprende los pasos de

- establecer un conjunto de reglas con al menos una regla para el al menos un punto final (50),

- observar una conformidad del al menos un punto final (50) con el conjunto de reglas,

- asignar una puntuación en función de la conformidad y

- determinar al menos una medida en función de la puntuación,

- caracterizado porque el punto final (50) forma una interfaz de administrador y

- en el que el conjunto de reglas con la al menos una regla es un conjunto de reglas para administrar el al menos un recurso de red (30) a través del al menos un punto final (50) y

- el al menos un recurso de red (30) está separado físicamente del al menos un punto final (50) que administra este recurso de red y

- no solo el al menos un punto final (50) que administra el recurso de red (30) puede acceder a este recurso de red (30), sino que también pueden acceder uno o varios puntos finales adicionales de la red, y en el que

- el al menos un recurso de red (30) se forma con un hardware, en particular un servidor, y/o con un software, en particular un sistema operativo y/o un programa de aplicación para aplicación por medio de la red (10), y

- el conjunto de reglas establece la regularidad y/o oportunidad de una actualización del software y/o de un software en el hardware, y

- la puntuación depende de un período durante el cual se omite al menos una actualización y/o depende de un número y/o de una criticidad en relación con la seguridad informática de las actualizaciones omitidas.

2. Procedimiento según la reivindicación anterior, en el que la al menos una medida comprende una limitación de privilegios del punto final (50) en la red (10) en función de la puntuación.

3. Procedimiento según la reivindicación 2, en el que la limitación de privilegios es una limitación de los privilegios para la administración del recurso de red (30).

4. Procedimiento según una de las reivindicaciones anteriores, en el que la al menos una medida comprende una interrupción del funcionamiento de la red (10).

5. Procedimiento según una de las reivindicaciones anteriores, en el que el al menos un punto final (50) se forma respectivamente con al menos un recurso de red (30) y/o al menos un hardware de administrador, preferiblemente un ordenador cliente y/o un hardware de autenticación, y/o al menos una interfaz de hardware, preferiblemente una cuenta de usuario.

6. Procedimiento según una de las reivindicaciones anteriores, en el que la medida comprende una modificación o limitación de privilegios administrativos.

7. Procedimiento según una de las reivindicaciones anteriores, en el que la medida comprende una conexión o modificación de la conexión del punto final (50) a la red (10).

8. Procedimiento según una de las reivindicaciones anteriores, en el que la medida incluye una formación para un administrador que se conecta al punto final (50).

9. Procedimiento según una de las reivindicaciones anteriores, en el que la puntuación se asigna en al menos dos categorías y la formación, preferiblemente mediante módulos, se adapta en función de la puntuación en las categorías, preferiblemente en función de la ocupación de las categorías y/o del peso absoluto y/o relativo de las categorías y/o en el que un administrador es admitido en la red (10) solo después de una formación.

10. Procedimiento según una de las reivindicaciones anteriores, en el que la puntuación se otorga, mantiene o modifica en función de una formación, preferiblemente repetida, y/o de una verificación, preferiblemente repetida.

11. Producto de programa informático diseñado para ejecutar el procedimiento según una de las reivindicaciones anteriores, diseñado además para almacenar un conjunto de reglas con al menos una regla para el al menos un punto final (50), para recibir datos de observación sobre la conformidad del al menos un punto final (50) con el conjunto de reglas, así como para asignar una puntuación en función de la conformidad.

DIBUJOS

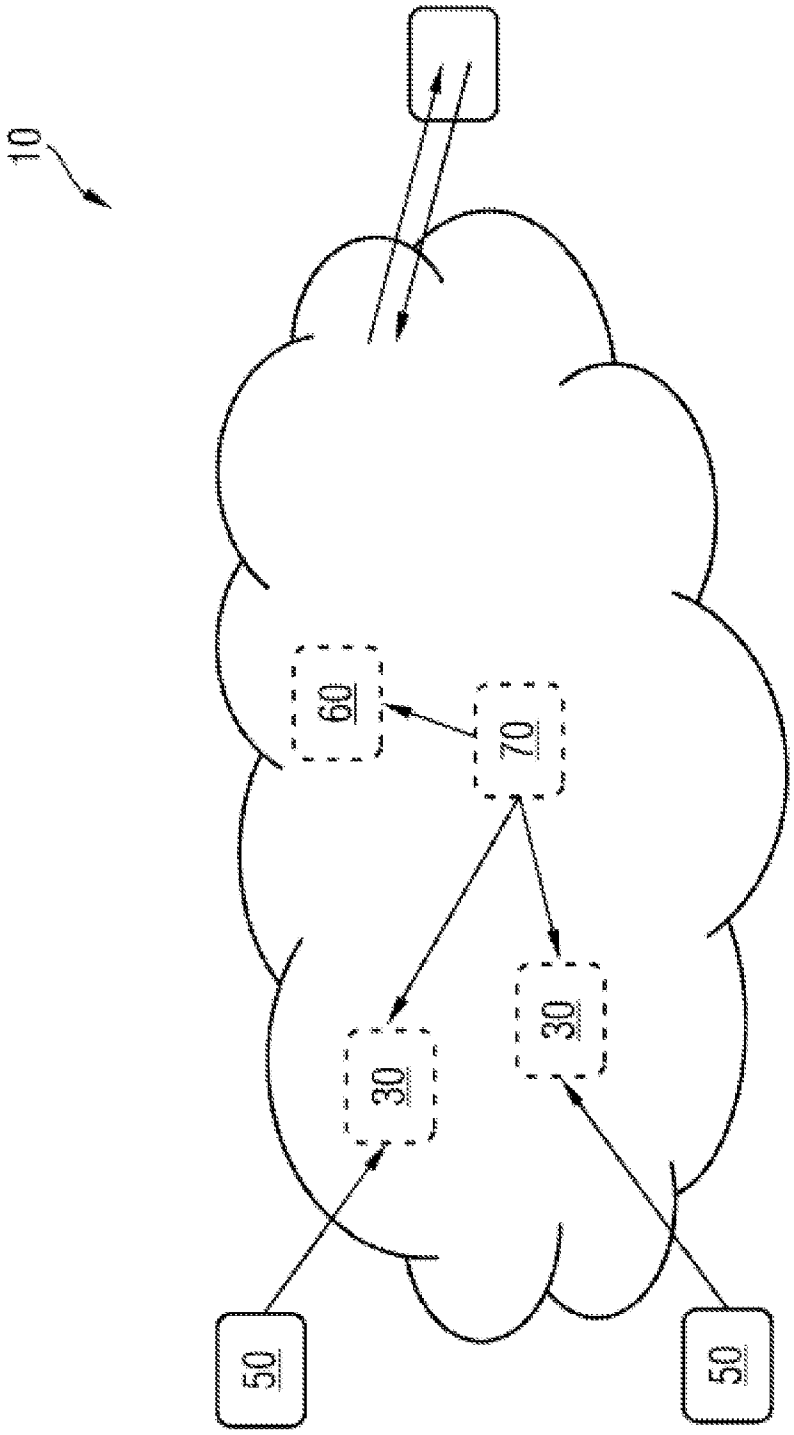
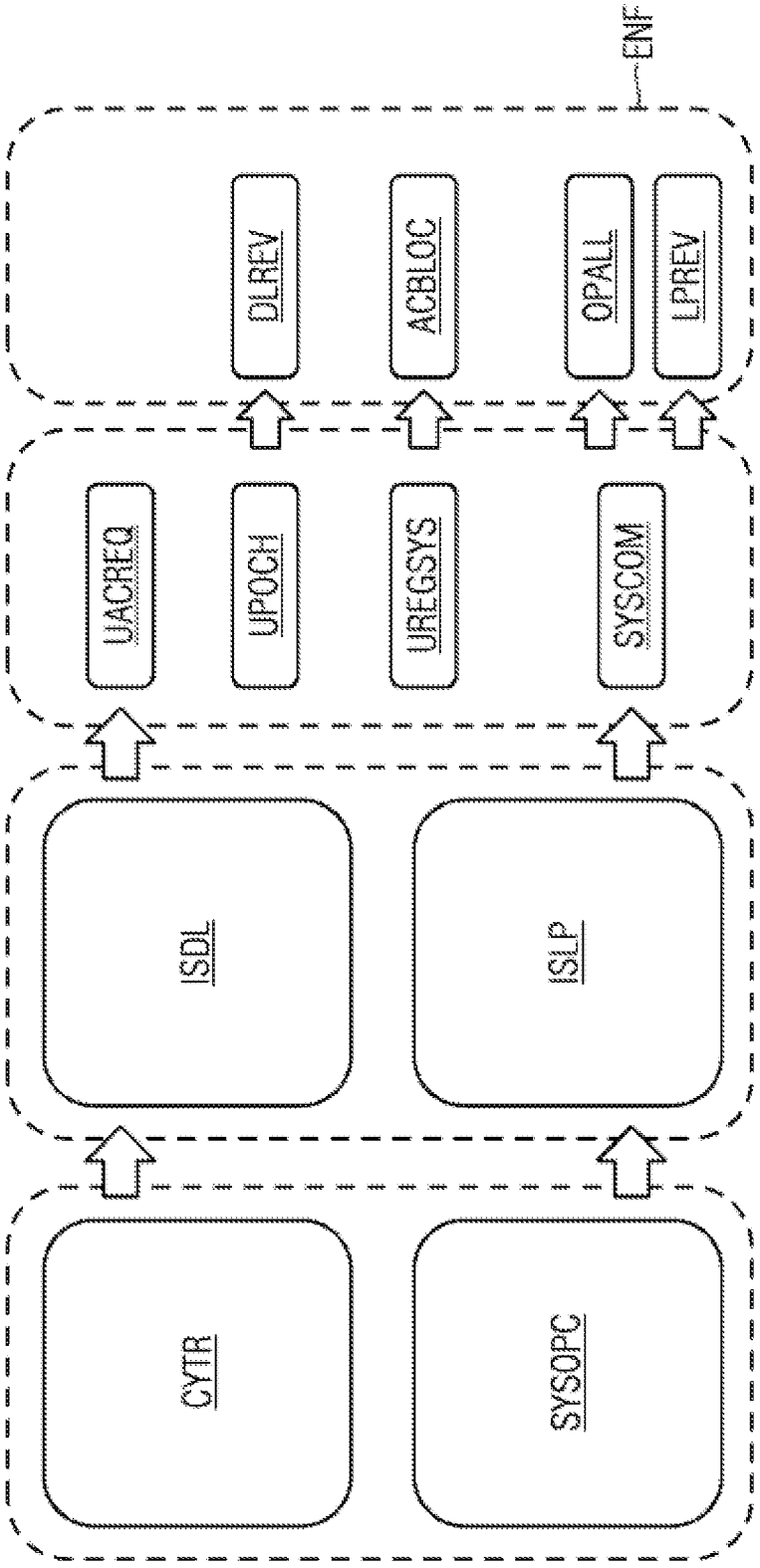


FIG 1

FIG 2


ENF
DLREV
ACBLOC
OPALL
LPREV
UACREQ
UPOCH
UREGSYS
SYSCOM
ISDL
ISLP
CYTR
SYSOPC