SISTEMAS Y MÉTODOS DE EXPLOSIÓN COMERCIAL

APLICACIONES RELACIONADAS

[0001] La presente solicitud de patente está relacionada con la solicitud de patente australiana n.º 2023901892, titulada "Sistemas y métodos de granallado comercial", presentada el 15 de junio de 2023 a nombre de Orica International Pte Ltd, cuya memoria descriptiva, tal como se presentó, se incorpora al presente documento en su totalidad por referencia. La presente solicitud de patente también está relacionada con la solicitud de patente singapurense n.º 10202301672W, titulada "Control de acceso para máquinas de granallado electrónico", presentada el 13 de junio de 2023 a nombre de Orica International Pte Ltd, cuya memoria descriptiva, tal como se presentó, se incorpora al presente documento en su totalidad por referencia.

CAMPO TÉCNICO

[0002] Aspectos de la presente divulgación se refieren a sistemas y métodos que proporcionan voladuras comerciales con detonadores/iniciadores controlados a distancia, incluyendo dispositivos de voladura electrónica inalámbrica (WEB) y sistemas de voladura electrónica (EBS) en barrenos de voladura (que pueden extenderse en cualquier dirección, incluyendo vertical, vertical y transversal) de una o más voladuras. Dichas voladuras comerciales pueden utilizarse en operaciones de minería a cielo abierto, minería subterránea, canteras, demolición y/o estudios sísmicos.

[0003] Aspectos de la presente divulgación también se refieren a sistemas y métodos que proporcionan seguridad y control de acceso en operaciones de voladuras comerciales con sistemas electrónicos de voladura controlados a distancia con detonadores/iniciadores, incluyendo la prevención de la operación no autorizada de dichos sistemas. Dichos sistemas electrónicos de voladura pueden incluir sistemas inalámbricos de voladura electrónica (WEB) con dispositivos WEB y sistemas cableados de voladura electrónica (EBS) con dispositivos EBS.

ANTECEDENTES

[0004] comerciales se pueden utilizar en operaciones de minería a cielo abierto, operaciones de minería subterránea, operaciones de canteras, operaciones de demolición y/o estudios sísmicos.

[0005] Algunos sistemas y métodos de voladura comerciales utilizan al menos un sistema de voladura electrónico (EBS), por ejemplo, el i-kon (TM) de ORICA LTD, que incluye muchos dispositivos EBS de fondo de pozo (por ejemplo, detonadores i-kon) en los pozos de voladura y conectados por cables a un detonador remoto (también conocido como "máquina de voladura remota"), por ejemplo, DETONADOR 3000 (TM) de ORICA, que a su vez es controlado por un controlador (también conocido como "controlador de voladura", "estación de control" o "estación de comando central") que registra y controla el detonador remoto (o quizás muchos detonadores remotos) para iniciar una voladura de acuerdo con un plan de voladura predefinido.

[0006] Otros sistemas y métodos de voladura comerciales utilizan sistemas de voladura electrónica inalámbrica (WEB), por ejemplo, el sistema WebGen™ de ORICA LTD, que incluye muchos dispositivos WEB de fondo de pozo (por ejemplo, cebadores WebGen) en los barrenos de voladura y están configurados para recibir señales de comunicación de inducción magnética (MI) a través de la tierra (TTE), donde "tierra" significa roca/mineral/tallo/etc., desde una antena de transmisión MI (por ejemplo, una de las antenas WebGen de ORICA). Dicha comunicación TTE a menudo es prácticamente solo en una dirección, proporcionando así solo comunicación unidireccional o "enlace descendente" desde el equipo fuera del pozo, incluidas las antenas de transmisión fuera del pozo. En este contexto, la comunicación "TTE" se refiere a señales de comunicación inalámbrica que transportan información a través de materiales geológicos sustancialmente no conductores sin usar cables, y por lo tanto, el término "tierra" en este contexto puede incluir material en el que están enterrados los dispositivos, incluyendo tierra, roca, suelo, suelo, material de tallo, material explosivo a granel, hormigón y/o ladrillo, dependiendo del tipo de operación.

[0007] Anteriormente, los sistemas EBS o WEB se seleccionaban en función de los tipos de voladuras que se utilizaban (por ejemplo, detención), el material que se iba a voladura y/o el tipo de operación de voladura (incluido, por ejemplo, la accesibilidad segura al área de voladura

antes de la misma); sin embargo, algunos tipos de operaciones estaban limitados por tener que utilizar solo uno o solo el otro sistema/método.

[0008] Además, para garantizar la seguridad en algunos sistemas de voladuras remotas anteriores, como los EBS, se han requerido dos llaves físicas para iniciar una voladura con éxito: una llave remota y una llave de disparo. Al iniciar un detonador remoto (también conocido como "máquina de voladura electrónica remota"), el detonador remoto creaba una llave física remota individual con detalles del detonador remoto, como los registradores conectados, el número de detonadores, los números de serie de los dispositivos conectados, su número de identificación y una clave digital aleatoria generada por el detonador remoto. Un operador humano llevaba la llave física remota a un controlador del sistema de voladuras (también conocido como "detonador controlador", "estación de control", "detonador de control" o "estación de comando central"). para registrar el detonador remoto, p. ej., véase la patente estadounidense n.º de serie 6851369 (“Control de acceso para máquinas de voladura electrónicas”, 8 de febrero de 2005, de Orica Explosives Technology Pty Ltd, con los inventores Dirk Hummel y Olaf Cramer). Solo se tuvo en cuenta un detonador remoto registrado para la siguiente secuencia de voladura. La clave digital aleatoria del dongle remoto se utilizó para cifrar la información transmitida entre el controlador del sistema de voladura y el detonador remoto. Después de la inicialización del detonador remoto a través del controlador del sistema de voladura, se requirió el dongle de disparo en el controlador del sistema de voladura para habilitar la activación del voltaje de disparo en los detonadors remotos. El dongle de disparo permitió la activación del voltaje de disparo y almacenó los comandos DETONAR finales, por lo tanto, solo si el dongle de disparo se insertó en un puerto de comunicación del controlador (p. ej., su puerto de 7 pines o un puerto USB) el operador pudo avanzar en la secuencia de voladura. Tras pulsar las teclas de disparo en el controlador del sistema de detonación, este leía los comandos de disparo del adaptador de disparo. Estos comandos eran necesarios para activar los detonadores conectados al volador remoto.

[0009] Sin embargo, en aplicaciones donde se requiere una gran cantidad de máquinas de voladura remotas o dinamitadores remotos, por ejemplo, más de 100 máquinas de voladura remotas, llevar llaves físicas o claves de autorización de cada máquina de voladura remota al controlador puede ser demasiado lento/dificultoso dentro de los límites de tiempo relevantes, en particular cuando hay un cambio en los planes de voladura, por ejemplo, cuando las

máquinas de voladura remotas están bajo tierra y el controlador del sistema de voladura está en la superficie (por lo tanto, no bajo tierra) y a cierta distancia, por ejemplo, se accede mediante un ascensor lento, al tiempo que se garantiza que los dinamitadores remotos estén registrados de forma segura y confiable en el controlador del sistema de voladura. Por ejemplo, en la minería subterránea, pueden estar conectados más detonadores listos para la voladura de los que finalmente se requieren (dependiendo de los efectos de las explosiones anteriores), y puede ser indeseable/peligroso llevar llaves físicas o claves de autorización de cada dinamitador remoto de vuelta al controlador del sistema de voladura cuando hay un cambio en el plan de voladura.

[0010] Se desea abordar o mejorar una o más desventajas o limitaciones asociadas con la técnica anterior, o al menos proporcionar una alternativa útil.

[0011] La referencia en esta especificación a cualquier publicación previa (o información derivada de ella), o a cualquier asunto que se conozca, no es, y no debe tomarse como, un reconocimiento o admisión o cualquier forma de sugerencia de que la publicación previa (o información derivada de ella) o el asunto conocido forma parte del conocimiento general común en el campo de esfuerzo al que se refiere esta especificación.

SUMARIO

[0012] De acuerdo con la presente invención, se proporciona un sistema de voladura comercial que incluye:

un controlador central configurado para enviar instrucciones de comando de voladura para dos o más dispositivos electrónicos de voladura, en donde los dos o más dispositivos electrónicos de voladura incluyen al menos un dispositivo electrónico de voladura inalámbrico (WEB) y al menos un dispositivo de sistema electrónico de voladura cableado (EBS);

al menos un detonador remoto conectable al controlador central y configurado para recibir las instrucciones de comando de voladura para el dispositivo EBS, y configurado para enviar al menos un comando de voladura correspondiente al dispositivo EBS a través de cables; y

al menos un sistema de antena conectable al controlador central y configurado para recibir las instrucciones de comando de voladura para el dispositivo WEB, y configurado para enviar al menos un comando de voladura correspondiente al dispositivo WEB a través de señales de inducción magnética (MI),

en donde el detonador remoto está configurado para enviar uno o más mensajes de protocolo de enlace al controlador indicando que el dispositivo EBS está programado para el blast para que el controlador sincronice el envío de un comando DETONAR para el dispositivo EBS con el envío de un comando DETONAR para el dispositivo WEB.

[0013] En una o más realizaciones, el controlador central está configurado para proporcionar una máquina de estado WEB y una máquina de estado EBS, y para sincronizar la máquina de estado WEB con la máquina de estado EBS basándose en los mensajes de protocolo de enlace.

[0014] En una o más realizaciones, el controlador central está configurado para enviar una instrucción de comando MI DETONAR y una instrucción de comando EBS DETONAR separadas por un intervalo predeterminado.

[0015] En una o más realizaciones, al menos uno de los detonadores remotos y el sistema de antena son físicamente un dispositivo combinado y el intervalo predeterminado es utilizado por el dispositivo combinado para enviar la instrucción de comando MI DETONAR y la instrucción de comando EBS DETONAR.

[0016] En una o más realizaciones, el controlador central está configurado para recibir una o más de las siguientes opciones: una confirmación de autorización de baliza, un dispositivo de voladura y una clave de archivo de voladura para enviar las instrucciones del comando de voladura.

[0017] En una o más realizaciones, el controlador central y el sistema de antena están conectados mediante una interfaz de datos bidireccional para proporcionar mensajes de protocolo de enlace al controlador desde el sistema de antena.

[0018] De acuerdo con la presente invención, se proporciona un sistema de voladura comercial que incluye:

un controlador central configurado para enviar instrucciones de comando de voladura a dos o más dispositivos electrónicos de voladura en una voladura de acuerdo con un plan de voladura, en donde los dos o más dispositivos electrónicos de voladura incluyen al menos un dispositivo electrónico de voladura inalámbrico (WEB) y al menos un dispositivo de sistema electrónico de voladura cableado (EBS);

al menos un detonador remoto conectable al controlador central y configurado para recibir las instrucciones de comando de voladura para el dispositivo EBS, y configurado para enviar al menos un comando de voladura al dispositivo EBS a través de cables basados en las instrucciones de comando de voladura;

al menos un sistema de antena conectable al controlador central y configurado para recibir las instrucciones del comando de voladura para el dispositivo WEB, y configurado para enviar al menos un comando de voladura al dispositivo WEB a través de señales de inducción magnética (MI) basadas en las instrucciones del comando de voladura; y

al menos un dispositivo de sincronización MI configurado para recibir el comando de voladura a través de las señales MI, y conectable al o a cada detonador remoto para enviar señales de sincronización que representan el comando de voladura para que el dispositivo WEB sincronice el disparo del dispositivo EBS y el dispositivo WEB.

[0019] En una o más realizaciones, el dispositivo de sincronización MI está configurado para realizar una o más de las siguientes acciones:

al recibir una secuencia MI, enviar en respuesta una señal de relación señal-ruido (SNR) MI para el detonador remoto y/o el controlador central;

al recibir un comando MI SINCRONIZACIÓN, enviar en respuesta una instrucción de comando de preparación para disparar para el detonador remoto, en donde el comando de preparación para disparar se envía al detonador remoto en un momento predeterminado después de la recepción del comando MI SINCRONIZAR; y

al recibir un comando MI DETONAR, envíe en respuesta una instrucción de comando DETONAR para que el detonador remoto dispare el dispositivo EBS.

[0020] En una o más realizaciones, el detonador remoto está configurado para enviar mensajes de protocolo de enlace al controlador indicando que el dispositivo EBS está programado para el detonador para que el controlador sincronice el envío de un comando de DETONACIÓN para el dispositivo EBS con el envío de un comando de DETONACIÓN para el dispositivo WEB.

[0021] En una o más realizaciones, el controlador central está configurado para proporcionar una máquina de estado WEB y una máquina de estado EBS, y para sincronizar la máquina de estado WEB con la máquina de estado EBS basándose en los mensajes de protocolo de enlace.

[0022] En una o más realizaciones, el controlador central está configurado para recibir una o más de las siguientes opciones: una confirmación de autorización de baliza, un dispositivo de voladura y una clave de archivo de voladura para enviar las instrucciones del comando de voladura.

[0023] En una o más realizaciones, el dispositivo de sincronización MI incluye un magnetómetro configurado para generar una salida electrónica/eléctrica que representa el comando de voladura recibido.

[0024] En una o más realizaciones, el magnetómetro incluye al menos una antena MI y un receptor correspondiente.

[0025] En una o más realizaciones, el dispositivo de sincronización MI incluye una interfaz de comunicación para la conexión al detonador remoto.

[0026] En una o más realizaciones, el sistema incluye además:

un dispositivo físico de registro remoto configurado para conectarse comunicativamente al controlador central y al menos a un detonador remoto y/o al menos a un sistema de antena (cada uno denominado en adelante una "unidad remota"),

en donde el controlador central está configurado para proporcionar un par de claves de cifrado asimétricas pública-privada con una clave pública y una clave privada, y para escribir la clave pública en el dispositivo de registro remoto cuando el dispositivo de registro remoto está conectado comunicativamente al controlador,

en donde cada uno de los al menos un detonador remoto y/o el al menos un sistema de antena está configurado para leer la clave pública del dispositivo de registro remoto cuando el dispositivo de registro remoto está conectado comunicativamente al detonador remoto o sistema de antena correspondiente,

en donde el controlador central y cada uno del al menos un detonador remoto y/o el al menos un sistema de antena están configurados para comunicarse entre sí a través de una red de datos utilizando el par de claves.

[0027] En una o más realizaciones, cada detonador remoto y/o cada sistema de antena está configurado para proporcionar una clave de cifrado de protocolo de enlace que es única/cuasi única para cada detonador remoto y/o cada sistema de antena, y para cifrar y enviar la clave de cifrado de protocolo de enlace al controlador central utilizando la clave pública y la red de datos.

[0028] En una o más realizaciones, el controlador central está configurado para proporcionar una clave de cifrado de comunicaciones que es única/cuasi única para cada detonador remoto y/o cada sistema de antena, y para cifrar y enviar la clave de cifrado de comunicaciones en un segundo mensaje de protocolo de enlace a cada detonador remoto y/o cada sistema de antena utilizando la clave de protocolo de enlace y la red de datos.

[0029] En una o más realizaciones, el controlador central y cada uno del al menos un detonador remoto y/o el al menos un sistema de antena están configurados para comunicarse entre sí utilizando la clave de cifrado de comunicaciones y la red de datos.

[0030] En una o más realizaciones, el controlador central está configurado para proporcionar una clave de cifrado de transmisión que no es única/cuasi única para cada detonador remoto o sistema de antena, y para enviar la clave de cifrado de transmisión a cada detonador remoto y/o cada sistema de antena que utiliza la red de datos.

[0031] En una o más realizaciones, el controlador central está configurado para cifrar y enviar instrucciones de comando de explosión. a cada detonador remoto y/o a cada sistema de antena utilizando la clave de cifrado de transmisión y la red de datos.

[0032] En una o más realizaciones:

El controlador central tiene una interfaz de comunicaciones segura,

cada detonador remoto y/o cada sistema de antena tiene una interfaz de comunicaciones seguras correspondiente a la interfaz de comunicaciones seguras del controlador central,

el controlador central está configurado para proporcionar un par de claves de cifrado asimétricas pública-privada con una clave pública y una clave privada, y para escribir la clave pública individualmente en cada detonador remoto y/o cada sistema de antena cuando cada detonador remoto y/o cada sistema de antena están conectados respectivamente a través de las interfaces de comunicaciones seguras,

cada detonador remoto y/o cada sistema de antena configurado para leer la clave pública del controlador central cuando se conecta a través de las interfaces de comunicaciones seguras, y

El controlador central y cada uno de los al menos un detonador remoto y/o el al menos un sistema de antena están configurados para comunicarse entre sí a través de una red de datos utilizando el par de claves.

[0033] En una o más realizaciones, cada detonador remoto y/o cada sistema de antena está configurado para proporcionar una clave de cifrado de protocolo de enlace que es única/cuasi única para cada detonador remoto y/o cada sistema de antena, y para cifrar y enviar la clave de cifrado de protocolo de enlace al controlador central utilizando la clave pública y la red de datos.

[0034] En una o más realizaciones, el controlador central está configurado para proporcionar una clave de cifrado de comunicaciones que es única/cuasi única para cada detonador remoto y/o cada sistema de antena, y para cifrar y enviar la clave de cifrado de comunicaciones en un segundo mensaje de protocolo de enlace a cada detonador remoto y/o cada sistema de antena utilizando la clave de protocolo de enlace y la red de datos.

[0035] En una o más realizaciones, el controlador central y cada detonador remoto y/o cada sistema de antena están configurados para comunicarse entre sí utilizando la clave de cifrado de comunicaciones y la red de datos.

[0036] En una o más realizaciones, el controlador central está configurado para proporcionar una clave de cifrado de transmisión que no es única/cuasi única para cada detonador remoto y/o cada sistema de antena, y para enviar la clave de cifrado de transmisión a cada detonador remoto y/o cada sistema de antena utilizando la red de datos.

[0037] En una o más realizaciones, el controlador central está configurado para cifrar y enviar instrucciones de comando de explosión. a cada detonador remoto y/o a cada sistema de antena utilizando la clave de cifrado de transmisión y la red de datos.

[0038] De acuerdo con la presente invención, se proporciona un método de granallado comercial que incluye:

enviar instrucciones de comando de voladura para dos o más dispositivos electrónicos de voladura, en donde los dos o más dispositivos electrónicos de voladura incluyen al menos un dispositivo electrónico de voladura inalámbrico (WEB) y al menos un dispositivo de sistema electrónico de voladura cableado (EBS);

recibir las instrucciones de comando de voladura para el dispositivo EBS y enviar al menos un comando de voladura correspondiente al dispositivo EBS a través de cables;

recibir las instrucciones de comando de voladura para el dispositivo WEB, y configurado para enviar al menos un comando de voladura correspondiente al dispositivo WEB a través de señales de inducción magnética (MI);

enviando uno o más mensajes de protocolo de enlace indicando que el dispositivo EBS está programado; y

sincronizar el envío de un comando DETONAR para el dispositivo EBS con el envío de un comando DETONAR para el dispositivo WEB.

[0039] En una o más realizaciones, el método incluye sincronizar una máquina de estado WEB con una máquina de estado EBS basándose en los mensajes de protocolo de enlace.

[0040] En una o más realizaciones, el método incluye el envío de una instrucción de comando MI DETONAR y una instrucción de comando EBS DETONAR separadas por un intervalo predeterminado (o el "retardo de DETONACIÓN MI predeterminado").

[0041] En una o más realizaciones, el método incluye enviar la instrucción de comando MI DETONAR y la instrucción de comando EBS DETONAR desde un dispositivo unitario.

[0042] En una o más realizaciones, el método incluye recibir una o más de una confirmación de autorización de baliza, un dispositivo de voladura y una clave de archivo de voladura para enviar las instrucciones del comando de voladura.

[0043] En una o más realizaciones, el método incluye el envío de mensajes de protocolo de enlace en respuesta a las instrucciones de comando de explosión para el dispositivo WEB.

[0044] De acuerdo con la presente invención, se proporciona un método de granallado comercial que incluye:

enviar instrucciones de comando de voladura a dos o más dispositivos electrónicos de voladura en una voladura de acuerdo con un plan de voladura, en donde los dos o más dispositivos electrónicos de voladura incluyen al menos un dispositivo electrónico de voladura inalámbrico (WEB) y al menos un dispositivo de sistema electrónico de voladura cableado (EBS);

recibir las instrucciones de comando de voladura para el dispositivo EBS;

enviar al menos un comando de voladura al dispositivo EBS a través de cables según las instrucciones del comando de voladura;

recibir las instrucciones del comando de explosión para el dispositivo WEB;

enviando al menos un comando de voladura al dispositivo WEB a través de señales de inducción magnética (MI) basadas en las instrucciones del comando de voladura;

recibir la orden de voladura a través de las señales MI; y

enviando señales de sincronización basadas en el comando de explosión recibido a través de las señales MI para sincronizar el disparo del dispositivo EBS y el dispositivo WEB.

[0045] En una o más realizaciones, el método incluye uno o más de los siguientes:

enviar una señal de relación señal-ruido (SNR) MI después de recibir una secuencia MI;

enviar un comando de preparación para disparar en un momento predeterminado después de recibir un comando MI SINCRONIZAR; y

enviando un comando DETONAR al dispositivo EBS después de recibir un comando MI DETONAR.

[0046] En una o más realizaciones, el método incluye el envío de mensajes de protocolo de enlace que indican que el dispositivo EBS está programado para la explosión a fin de sincronizar el envío de un comando de DETONACIÓN para el dispositivo EBS con el envío de un comando de DETONACIÓN para el dispositivo WEB.

[0047] En una o más realizaciones, el método incluye sincronizar una máquina de estado WEB con una máquina de estado EBS basándose en los mensajes de protocolo de enlace.

[0048] En una o más realizaciones, el método incluye recibir una o más de una confirmación de autorización de baliza, un dispositivo de voladura y una clave de archivo de voladura para enviar las instrucciones del comando de voladura.

[0049] En una o más realizaciones, el método incluye generar una salida electrónica/eléctrica que representa el comando de voladura recibido a través de las señales MI.

[0050] En una o más realizaciones, el método incluye generar la salida electrónica/eléctrica utilizando al menos una antena MI y un receptor correspondiente.

[0051] En una o más realizaciones, el método incluye enviar las señales de sincronización a través de una interfaz de comunicación a un detonador remoto.

[0052] En una o más realizaciones, el método incluye:

el controlador central del sistema de detonación electrónica que proporciona un par de claves de cifrado asimétrico público-privado con una clave pública y una clave privada;

el controlador central se conecta comunicativamente a un dispositivo de registro remoto físico para escribir la clave pública en el dispositivo de registro remoto;

cada detonador remoto y/o cada sistema de antena se conecta comunicativamente por separado al dispositivo de registro remoto para leer por separado la clave pública; y

cada detonador remoto y/o cada sistema de antena que se comunica con el controlador central a través de una red de datos utilizando la clave pública.

[0053] En una o más realizaciones, el método incluye que cada detonador remoto y/o cada sistema de antena proporcione una clave de cifrado de protocolo de enlace que sea única/cuasi única para cada detonador remoto y/o cada sistema de antena, y que encripte y envíe la clave de cifrado de protocolo de enlace al controlador central utilizando la clave pública y la red de datos.

[0054] En una o más realizaciones, el método incluye que el controlador central proporcione una clave de cifrado de comunicaciones que sea única/cuasi única para cada detonador remoto y/o cada sistema de antena, y que cifre y envíe la clave de cifrado de comunicaciones en un segundo mensaje de protocolo de enlace a cada detonador remoto y/o cada sistema de antena utilizando la clave de protocolo de enlace y la red de datos.

[0055] En una o más realizaciones, el método incluye el controlador central y cada detonador remoto y/o cada sistema de antena comunicándose entre sí utilizando la clave de cifrado de comunicaciones y la red de datos.

[0056] En una o más realizaciones, el método incluye que el controlador central proporcione una clave de cifrado de transmisión que no es única/cuasi única para cada detonador remoto y/o cada sistema de antena, y envíe la clave de cifrado de transmisión a cada detonador remoto y/o cada sistema de antena utilizando la red de datos.

[0057] En una o más realizaciones, el método incluye que el controlador central encripte y envíe instrucciones de comando de explosión. a cada detonador remoto y/o a cada sistema de antena utilizando la clave de cifrado de transmisión y la red de datos.

[0058] En una o más realizaciones, el método incluye:

el controlador central que proporciona un par de claves de cifrado asimétricas pública-privada con una clave pública y una clave privada;

el controlador central se conecta comunicativamente a cada detonador remoto y/o cada sistema de antena a través de las respectivas interfaces de comunicaciones seguras para proporcionar por separado la clave pública a cada detonador remoto y/o cada sistema de antena; y

cada detonador remoto y/o cada sistema de antena se comunica respectivamente con el controlador central a través de una red de datos utilizando la clave pública.

[0059] En una o más realizaciones, el método incluye que cada detonador remoto y/o cada sistema de antena proporcione una clave de cifrado de protocolo de enlace que sea única/cuasi única para cada detonador remoto y/o cada sistema de antena, y que encripte y envíe la clave de cifrado de protocolo de enlace al controlador central utilizando la clave pública y la red de datos.

[0060] En una o más realizaciones, el método incluye que el controlador central proporcione una clave de cifrado de comunicaciones que sea única/cuasi única para cada detonador remoto y/o cada sistema de antena, y que cifre y envíe la clave de cifrado de comunicaciones en un segundo mensaje de protocolo de enlace a cada detonador remoto y/o cada sistema de antena utilizando la clave de protocolo de enlace y la red de datos.

[0061] En una o más realizaciones, el método incluye el controlador central y cada detonador remoto y/o cada sistema de antena comunicándose entre sí utilizando la clave de cifrado de comunicaciones y la red de datos.

[0062] En una o más realizaciones, el método incluye que el controlador central proporcione una clave de cifrado de transmisión que no es única/cuasi única para cada detonador remoto

y/o cada sistema de antena, y envíe la clave de cifrado de transmisión a cada detonador remoto y/o cada sistema de antena utilizando la red de datos.

[0063] En una o más realizaciones, el método incluye que el controlador central encripte y envíe instrucciones de comando de explosión. a cada detonador remoto y/o a cada sistema de antena utilizando la clave de cifrado de transmisión y la red de datos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0064] A continuación se describen algunas realizaciones de la presente invención, a modo de ejemplo no limitativo únicamente, con referencia a los dibujos adjuntos, en los que:

a. La FIG. 1 es un diagrama esquemático de un sistema de voladura dual (también denominado “sistema de voladura concurrente”) descrito en este documento;
b. La FIG. 2 es un diagrama esquemático de un sistema de voladura sincronizada divulgado en este documento;
c. La FIG. 3 es un diagrama esquemático de una primera disposición de dispositivos electrónicos de voladura del sistema de voladura dual o del sistema de voladura sincronizada, en donde los dispositivos electrónicos de voladura incluyen uno o más dispositivos electrónicos de voladura inalámbricos (WEB) y uno o más dispositivos de sistema electrónico de voladura (EBS) en pozos separados;
d. La FIG. 4 es un diagrama esquemático de una segunda disposición de dispositivos electrónicos de voladura del sistema de voladura dual o del sistema de voladura sincronizada, en donde los dispositivos electrónicos de voladura incluyen uno o más dispositivos WEB y uno o más dispositivos EBS en cada pozo;
e. La FIG. 5 es un diagrama esquemático de un sistema de antena de bucle del sistema de voladura dual o del sistema de voladura sincronizada, en donde el sistema de antena incluye una antena de bucle;
f. La FIG. 6 es un diagrama de flujo de un método de voladura dual realizado por el sistema de voladura dual;

g. La FIG. 7 es un diagrama de flujo de un método de voladura sincronizada realizado por el sistema de voladura sincronizada;
h. La FIG. 8 es un diagrama esquemático de un sistema de control de acceso para una pluralidad de máquinas de voladura electrónicas (“explotadoras remotas”) del sistema de voladura dual o del sistema de voladura sincronizada; y

i. La FIG. 9 es un diagrama de flujo de un método de control de acceso realizado por el sistema de control de acceso de la FIG. 8.

DESCRIPCIÓN DETALLADA

Descripción general

[0065] Como se muestra en las FIG. 1 y 2, se describen aquí sistemas de voladura combinables o combinados, cada uno de los cuales incluye:

a. un sistema de voladura electrónica inalámbrica (WEB), que incluye al menos un sistema de antena 102 configurado para enviar señales de inducción magnética (MI) 104 a través de la tierra/suelo/etc. (TTE) a dispositivos WEB 302 de dos o más dispositivos de voladura electrónica 110 en dos o más orificios 306 en la tierra/suelo/etc.; y
b. un sistema de voladura electrónica con cables (EBS) acoplado al sistema WEB, en donde el EBS incluye al menos un detonador remoto 106 configurado para enviar señales no inalámbricas a través de cables 108 a dispositivos EBS 304 de los dispositivos de voladura electrónica 110 en los pozos 306.

[0066] Los sistemas de voladura combinados (denominados "sistemas de disparo centralizados") pueden controlar una o varias voladuras mediante la combinación del sistema WEB y el EBS. Cada voladura suele tener uno o más (hasta 10) identificadores de voladura (o identificadores de grupo) que identifican cuáles de los dispositivos WEB 302 se han seleccionado para dicha voladura: el identificador puede denominarse "ID de grupo" (GID), que define el grupo de dispositivos WEB 302 seleccionados, o "ID de voladura" (BID), que

define el grupo de dispositivos WEB 302 seleccionados dentro de la voladura. Por lo tanto, el GID o el BID son compartidos por un grupo de varios dispositivos WEB 302. Por ejemplo, el término "ID de grupo" puede utilizarse para dispositivos de tipo WebGen 100, mientras que el término "ID de voladura" puede utilizarse para dispositivos de tipo WebGen 200. Ambos términos se refieren al mismo tipo de identificador, normalmente un código o código de cifrado, que permite a los dispositivos WEB 302 seleccionados en un lugar de voladura... Se pueden direccionar como un grupo, por ejemplo, para transmitir y verificar las órdenes de voladura. Por ejemplo, se pueden seleccionar/asignar de 1 a 10 GID o BID diferentes entre sí a entre 1 y 10 grupos respectivos de dispositivos WEB 302 en un sitio de voladura. El BID o GID es diferente de un identificador individual de cada dispositivo WEB: cada dispositivo WEB puede tener un identificador individual, conocido como ID de dispositivo o ID de unidad (UID), y cada identificador individual difiere de todos los demás identificadores individuales del dispositivo WEB (al menos los dispositivos WEB en cada voladura o sitio).

[0067] El sistema WEB presenta diferentes tipos de retardos de comunicación (también denominados "latencias") respecto al EBS cableado. Por consiguiente, los sistemas de voladura combinables o combinados están configurados para operar según los métodos de voladura combinados, descritos a continuación, en los que los comandos de los dispositivos EBS se combinan (en el sistema de voladura dual 100) o se sincronizan (en el sistema de voladura sincronizada 200) con las señales MI 104 del sistema WEB, de forma que se gestionen y gestionen dichos retrasos de forma segura y eficaz.

[0068] Los sistemas de voladura combinables o combinados incluyen un sistema de voladura dual 100 (también denominado "sistema de voladura concurrente") o un sistema de voladura sincronizada 200, que se describe a continuación. El/cada sistema de antena 102 incluye al menos un generador de corriente ("CG") para impulsar corriente eléctrica a través de al menos una antena MI para controlar, generar y modular las señales MI 104. Aunque solo se muestra un sistema de antena 102 y el sistema WEB correspondiente en las figuras 1 y 2, 2. Los sistemas 100 y 200 pueden incluir cada uno dos o más sistemas de antena 102, todos controlados y sincronizados por el controlador central 112. En una o más implementaciones, uno de los emisores remotos 106 y al menos uno de los sistemas de antena 102 pueden ser físicamente un dispositivo combinado o un dispositivo unitario (es decir, un dispositivo/unidad con uno de los emisores remotos 106 y uno de los sistemas de antena 102), por ejemplo, para una mejor

sincronización o el uso de un "retardo de disparo de MI predeterminado" que se describe más adelante.

[0069] Como se describe a continuación, los sistemas de voladura combinables o combinados están configurados para controlar los mensajes EBS 114 dirigidos al menos a un detonador remoto 106 del EBS, de modo que los dispositivos EBS 304 y los dispositivos WEB 302 detonen/inicien con la temporización seleccionada o aproximadamente con la temporización seleccionada, incluyendo las temporizaciones del plan de voladura. Este control de la temporización (en el sistema de voladura dual 100) o la sincronización (en el sistema de voladura sincronizada 200) no está disponible o es insuficiente en los sistemas de la técnica anterior, en parte porque los protocolos de señalización de los sistemas EBS y WEB de la técnica anterior son sustancialmente diferentes, y en parte porque la técnica anterior... Los dispositivos WEB a menudo sólo pueden recibir comandos de explosión inalámbricos unidireccionales (por ejemplo, comandos ARM/DETONAR) y necesitan conservar energía (por lo que tienen un modo de suspensión), mientras que los dispositivos EBS pueden estar en contacto eléctrico constante a través de los cables/alambres en el orificio 108, lo que permite una carga continua y una comunicación bidireccional con los dispositivos EBS.

Dispositivos electrónicos de explosión

[0070] Como se muestra en las FIG. 3 y 4, el sistema de voladura dual 100 o el sistema de voladura sincronizada El dispositivo 200 incluye uno o más dispositivos WEB 302 (p. ej., dispositivos WebGen) y uno o más dispositivos EBS 304 (p. ej., dispositivos i-kon o eDev™ de ORICA), desde uno hasta docenas o cientos de cada uno, que se despliegan en los barrenos 306 en el campo (p. ej., en una mina a cielo abierto/superficial/cantera, en una mina de exploración geofísica/sísmica o en una mina subterránea). Los barrenos 306 pueden denominarse "barrenos de voladura". Antes de su despliegue, los dispositivos WEB 302 y los dispositivos EBS 304 pueden almacenarse en uno o más cargadores de dispositivos, p. ej., transportarse a una zona o ubicación específica del campo en un vehículo.

[0071] Los orificios 306 pueden prepararse para la voladura para incluir, como se muestra en las FIGS. 3 y 4:

a. al menos una cubierta interior (también denominada “cubierta inferior” para pozos de fondo), que puede incluir una primera cubierta interior 308,408 y una segunda cubierta interior 310,410, una más profunda que la otra; y
b. al menos una cubierta exterior 312,412 (también denominada “cubierta superior” para pozos de fondo).

[0072] Cada cubierta interior incluye una porción más profunda de cada barreno con uno de los dispositivos de voladura, una composición explosiva a granel 314 (por ejemplo, un explosivo a base de nitrato de amonio (AN), como un explosivo de emulsión a base de AN) alrededor del dispositivo de voladura en el barreno, y materiales de contención 316 que tapan/sellan el extremo superior/superficial de la composición explosiva a granel 314. La cubierta exterior 312,412 incluye una porción menos profunda de cada barreno con uno de los dispositivos de voladura, la composición explosiva a granel 314 alrededor del dispositivo de voladura en el barreno y que se extiende hacia un collar del barreno, y los materiales de contención 316 que tapan/sellan un extremo superior/superficial de la composición explosiva a granel 314 en o hacia el collar. Los dispositivos de voladura dentro y a través de una plataforma de voladura expuesta, externa o superior pueden configurarse para iniciarse o iniciarse para volar dicha plataforma. Los dispositivos de voladura dentro y a través de una o más plataformas de voladura no expuestas, internas, más profundas o inferiores pueden iniciarse en los intervalos seleccionados tras la iniciación de los dispositivos externos para volar la siguiente plataforma expuesta, externa o superior, y así sucesivamente para plataformas más profundas con los dispositivos WEB. Como se muestra en las figuras 3 y 4, un conjunto de barrenos puede contener más de dos plataformas de voladura, y las plataformas internas incluyen dos o más capas de dispositivos de voladura, por lo que se pueden colocar tres o más dispositivos de voladura en cada barreno.

[0073] Como se muestra en las figuras 1 a 4, los dispositivos EBS 304 se conectan al lanzador remoto 106 mediante los respectivos cables 108 que se extienden desde los dispositivos EBS 304 hacia el collar de su orificio. Los cables 108 conectan los dispositivos EBS 304 al lanzador remoto 106 directamente (p. ej., para los dispositivos e-Dev™ de ORICA) o mediante un registrador (no mostrado) (p. ej., para los dispositivos i-kon). Los dispositivos EBS 304 se controlan mediante comandos de disparo (p. ej., comandos de ACTIVAR/DISPARAR/ABORTAR) desde el lanzador remoto 106 a través de los cables 108

y, si está presente, mediante el registrador. Como se muestra en las figuras 1 a 4. 3 y 4, cada dispositivo WEB 302 puede configurarse para su despliegue dentro de los pozos de explosión de tal manera que un eje longitudinal, o central, del dispositivo WEB 302 esté naturalmente alineado al menos casi coincidente o paralelo a un eje longitudinal, o central del pozo de explosión en el que se despliega.

[0074] Como se describió anteriormente, cada dispositivo WEB 302 puede tener, ser asignado o ser programado con su identificador único de unidad (UID) almacenado en la memoria del dispositivo de iniciación, por ejemplo, durante o después de su fabricación. Como se describió anteriormente, adicionalmente o alternativamente, grupos seleccionados de dispositivos WEB 302 pueden tener, ser asignados o ser programados con el GID/BID almacenado en la memoria de los dispositivos WEB 302, por ejemplo, antes, durante o después del despliegue en un conjunto de barrenos. El GID o BID se refiere a una voladura completa o a una sección de una voladura. Por ejemplo, si a cada anillo de una voladura se le ha asignado un BID diferente, se pueden disparar varios anillos a la vez, seleccionando esos BID en una sola voladura, o se pueden disparar anillo por anillo con un solo BID por voladura.

Sistema de voladura dual (“Sistema de voladura concurrente”)

[0075] Como se muestra en la FIG. 1, el sistema de voladura dual 100 puede incluir un controlador de sistema de voladura central 112, que también puede conocerse como “controlador de voladura”, “estación de control”, “estación de comando central”, “controlador de voladura centralizado”, “controlador de sistema de voladura remoto” o “controlador de sistema de voladura omnirremoto (ORBS)”.

[0076] En el sistema de voladura dual 100, el controlador 112 incluye al menos un microprocesador y una memoria asociada con instrucciones leídas por el microprocesador para proporcionar dos máquinas de estados, que incluyen:

a. una máquina de estados WEB que controla los estados del sistema WEB, incluyendo dichos estados un estado de SUSPENSIÓN, un estado DESPIERTO, un estado ACTIVADO, un estado DETONACIÓN y un estado DESHABILITADO; y

b. una máquina de estados EBS que controla los estados del EBS, incluyendo un estado PROGRAMADO, un estado CALIBRADO, un estado COMPROBADO, un estado ARMADO, un estado PRIMERO-ÚLTIMO DET PROBADO, un estado DISPARADO y un estado DESHABILITADO.

[0077] En algunos ejemplos, la máquina de estados WEB puede incluir uno o más estados de la misma máquina de estados en el producto DETONADOR W de ORICA.

[0078] En algunos ejemplos, la máquina de estados EBS puede incluir uno o más estados de la misma máquina de estados que en el producto controlador central B3000 de ORICA.

[0079] En el sistema de voladura dual 100 (y en el sistema de voladura sincronizada 200), el controlador 112 está configurado para enviar mensajes EBS 114 al detonador remoto 106 (o a varios emisores remotos 106) a través de un acoplamiento, vía, enlace o conexión de comunicación de red de datos, denominado en este documento conexión de red EBS 116. Esta conexión de red EBS 116 proporciona comunicación bidireccional, por ejemplo, según los protocolos existentes, como LTE o Wi-Fi. El controlador 112 está configurado para enviar mensajes WEB 118 al sistema de antena 102 a través de un acoplamiento, vía, enlace o conexión de red de datos, denominado conexión de red WEB 120, que también proporciona comunicación bidireccional, por ejemplo, según los protocolos existentes, como LTE o Wi-Fi. Las conexiones de red de datos (la conexión de red EBS 116 y la conexión de red WEB 120) pueden incluir partes de una red de área local (LAN) o de datos en el sitio, denominada "red de la mina". El controlador 112 cuenta con interfaces de datos con la conexión de red EBS 116 y la conexión de red WEB 120, y está configurado para controlar tanto el sistema WEB como el EBS, y para recibir mensajes, incluidos los mensajes de protocolo de enlace 122, del detonador remoto 106. El sistema de antena 102 (incluido el CG) cuenta con una interfaz de datos con la conexión de red WEB 120, que es una interfaz de datos bidireccional, de modo que el controlador central 112 puede recibir mensajes de protocolo de enlace WEB 119 del sistema de antena 102. El detonador remoto 106, o cada uno de ellos, cuenta con una interfaz de datos con la conexión de red EBS 116.

[0080] El controlador 112 puede comunicarse con el sistema de antena 102 cuando está conectado a través de la conexión de red WEB 120, por ejemplo, que puede utilizar una parte de la red de la mina, como se describió anteriormente.

[0081] En el sistema de voladura dual 100 (y en el sistema de voladura sincronizada 200), los dispositivos WEB 302 están configurados para recibir comandos de voladura en las señales MI 104 del sistema de antena 102. Estos comandos de voladura se controlan mediante las instrucciones de voladura correspondientes del controlador 112, que se envían al sistema de antena 102 en los mensajes WEB 118. Los comandos de voladura incluyen una secuencia MI ARM y una secuencia MI DETONAR. La secuencia MI ARM incluye un comando WAKE-UP, un comando START, los BID y un comando MI ARM. La secuencia MI DETONAR incluye un comando MI SINCRONIZAR y un comando MI DETONAR. Al recibir el comando MI SINCRONIZAR, los dispositivos WEB 302 están configurados para sincronizar sus relojes internos y calcular el tiempo necesario para emitir señales DETONACIÓN a sus respectivos detonadores electrónicos (p. ej., detonadores i-kon o detonadores i-kon W que tienen una interfaz de conector en lugar de un cable).

[0082] Los mensajes EBS 114 dependen de y representan los estados de la máquina de estados EBS.

[0083] En el sistema de voladura dual 100 (y en el sistema de voladura sincronizada 200), el controlador 112 incluye un puerto de comunicaciones configurado para recibir una llave de voladura 124 (p. ej., una memoria USB u otra unidad de memoria extraíble manualmente legible por máquina que incluye una interfaz de datos (para conectarse comunicativamente al controlador 112, p. ej., USB) integrada con la memoria legible por máquina que proporciona almacenamiento electrónico no volátil en memoria informática, p. ej., memoria flash), también conocida como "llave de voladura" o "llave de disparo/detonación", que tanto la máquina de estados WEB como la máquina de estados EBS requieren para entrar en los estados de ACTIVACIÓN/DISPARO y, por lo tanto, enviar los comandos de ACTIVACIÓN/DISPARO para los dispositivos WEB 302 y EBS 304. La llave de voladura 124 es una clave de autorización para el tirador a cargo (que puede ser el operador) que le permite operar el controlador 112 a través de los estados de ambas máquinas de estados (EBS y WEB). El EBS requiere la llave de detonación 124 para activar los detonadores de los dispositivos EBS 304 a

la tensión de disparo, lo cual ocurre antes de la programación (descrita más adelante). La llave de detonación 124 contiene códigos de activación que el controlador 112 lee y envía cada pocos segundos a los detonadores remotos 106. Estos códigos son necesarios para reiniciar el temporizador de activación de cada detonador remoto 106, que permite la generación de la tensión de disparo. (El temporizador de activación es una función de seguridad funcional). Si ninguno de los detonadores remotos 106 recibe los códigos de activación, este permanece o regresa automáticamente a un nivel de tensión inherentemente seguro, al cual los dispositivos EBS 304 asociados no disparan. Si se quita el dispositivo de disparo 124 del controlador 112 durante la secuencia de disparo, los códigos de mantenimiento de actividad ya no están disponibles y los dispositivos EBS remotos 106 pasan al estado DESHABILITADO en el cual no pueden disparar los dispositivos EBS 304 (incluso si algo sale mal con la máquina de estados EBS).

[0084] En el sistema de voladura dual 100 (y en el sistema de voladura sincronizada 200), el controlador 112 también incluye un puerto de comunicaciones configurado para recibir un dispositivo físico de clave de archivo de voladura (no mostrado), por ejemplo, una memoria USB u otra unidad de memoria extraíble manualmente legible por máquina. El dispositivo físico de clave de archivo de voladura contiene una clave de archivo que incluye los BID que se dispararán en una voladura específica, junto con información adicional que permite el seguimiento y una ejecución segura de la voladura. La clave de archivo de voladura se genera durante la planificación de la voladura mediante un sistema de planificación de voladuras, luego se añade la información de codificación y, finalmente, una vez realizada la voladura, se añade información posterior. Por lo tanto, se puede decir que la clave de archivo de voladura contiene un "Currículum Vitae" (CV) de cada voladura (inalámbrica). La clave de archivo de voladura es requerida por la máquina de estados WEB, pero no por la máquina de estados EBS. La máquina de estados WEB puede requerir la clave del archivo blast para ingresar a los estados ARM/DETONAR y así enviar los comandos ARM/DETONAR para los dispositivos WEB 302. Los BID de la clave del archivo blast son necesarios para activar/disparar los dispositivos WEB 302.

[0085] En el sistema de voladura dual 100 (y en el sistema de voladura sincronizada 200), el lanzador remoto 106 está configurado para enviar los mensajes de protocolo de enlace 122 al controlador 112, generalmente a través de la conexión de red EBS 116. El controlador 112

utiliza el protocolo de enlace 112 para controlar las máquinas de estados WEB y EBS, y así sincronizar el sistema WEB con EBS, como se explica más adelante con referencia al método de voladura dual 600 (también denominado "método de voladura concurrente") y al método de voladura sincronizada 700.

[0086] El sistema de voladura dual 100 (y el sistema de voladura sincronizada 200) puede incluir uno o más dispositivos de medición de MI (también denominados "dispositivos de medición de MI") configurados para medir la relación señal-ruido (SNR) de las señales de MI 104, que, durante su uso, se comprueba que esté preferiblemente por encima de un umbral predefinido. En el sistema de voladura dual 100, los dispositivos de medición de MI proporcionan mediciones de MI, no sincronización, y se realizan antes de una voladura, por ejemplo, para comprobar/confirmar la recepción de la señal de MI en una mina/entorno, pero no durante la misma. En el sistema de voladura dual 100 y el sistema de voladura sincronizada 200, los dispositivos de medición de MI se utilizan generalmente antes de la voladura para evaluar la mina y determinar una SNR suficientemente buena en un proceso independiente de la voladura. Durante su uso, los dispositivos de medición de MI se disponen, ubican o se insertan en la trayectoria de las señales de MI 104. Cada dispositivo incluye una antena y un receptor de MI sintonizados adecuadamente (p. ej., desde un DRX de un dispositivo WebGen) y puede generar una señal de salida electrónica/eléctrica que representa la relación señal-ruido (SNR) medida y enviarla al controlador 112, por ejemplo, a través de la conexión de red EBS 116, de una red de datos en el sitio o por cable al controlador 112 o al dinamitero remoto 106. Como alternativa, los dispositivos de medición de MI pueden recopilarse y leerse físicamente mediante una interfaz cableada, y sus datos pueden revisarse para determinar si la relación señal-ruido (SNR) medida en la zona es suficiente para una dinamita segura.

[0087] El sistema de voladura dual 100 (y el sistema de voladura sincronizada 200) puede incluir una interfaz de usuario (IU) 126 conectada al controlador 112 y controlada por él para mostrar información a un operador humano y recibir sus comandos. La IU 126 incluye un botón de DISPARO para que el operador inicie las secuencias de disparo.

[0088] El sistema de voladura dual 100 puede utilizarse para dos o más voladuras independientes, con sus respectivos BID e identificadores EBS diferentes. Por ejemplo, un BID para los dispositivos WEB 302 y un conjunto de identificadores (ID) independientes para los

dispositivos EBS 304. Los dispositivos EBS 304 no tienen BID; en su lugar, tienen sus respectivos ID individuales, que se almacenan en el detonador remoto 106 correspondiente (por ejemplo, para dispositivos eDev) o en los registradores correspondientes (por ejemplo, para dispositivos i-kon). Puede resultar útil preparar y ejecutar estas múltiples voladuras independientes juntas, por ejemplo, dentro de un periodo de tiempo seleccionado durante el cual se despeja el sitio, lo que mitiga la necesidad de despejar el sitio para cada voladura, incluso si son independientes, por ejemplo, si no forman parte del mismo plan de voladura.

Método de voladura dual (“Método de voladura concurrente”)

[0089] El sistema de voladura dual 100 ejecuta el método de voladura dual 600 de forma automática o prácticamente automática. El sistema de voladura dual 100 y el método de voladura dual 600 pueden ser útiles en aplicaciones donde la sincronización de la voladura cableada (mediante los dispositivos EBS 304) y la inalámbrica (mediante los dispositivos WEB 302) no necesita ser tan precisa como la proporcionada por el sistema de voladura sincronizada 200. Como se muestra en la figura 1, el sistema de voladura dual 100 no requiere un dispositivo de sincronización MI (también denominado "caja de sincronización 202", mostrado en la figura 2) para ejecutar el método de voladura dual 600 descrito. En el método de voladura dual 600, la voladura cableada se dispara independientemente de la inalámbrica, lo que significa que, si se produce un fallo en el sistema de antena 102 (que incluye el CG) durante el envío de la secuencia MI DETONAR, la voladura inalámbrica fallará mientras que la cableada se disparará. En otras palabras, el sistema de doble voladura 100 y el método de doble voladura 600 proporcionan voladuras simultáneas de explosiones cableadas e inalámbricas, pero pueden no soportar la voladura sincrónica de sistemas EBS y WEB, lo que implica que el método de doble voladura 600 solo se recomienda en aplicaciones/operaciones en las que las explosiones cableadas y las explosiones inalámbricas son independientes y están separadas localmente, ya que la explosión cableada puede dispararse independientemente de si el sistema de antena 102 (y el CG) transmite o no el comando MI DETONAR al detonador inalámbrico, por ejemplo, si el sistema de antena 102 falla antes de finalizar la transmisión del comando MI DETONAR, las explosiones cableadas se dispararán de todos modos.

[0090] Como se muestra en la FIG. 6, el método de doble voladura 600 incluye:

a. en una fase preparatoria (P), codificar y cargar los dispositivos WEB 302 (602), que incluye: codificar los dispositivos WEB 302 con un codificador (incluyendo codificar el BID seleccionado), cargar los dispositivos WEB 302 en los orificios 306, poner los dispositivos WEB 302 en un estado de SUSPENSIÓN (poniendo así la máquina de estados WEB en el estado de SUSPENSIÓN), y cargar la(s) plataforma(s) correspondiente(s) alrededor/sobre los dispositivos WEB 302;

b. en la fase preparatoria (P), registrar, cargar, conectar y probar los dispositivos EBS 304 (604A), que incluye: registrar los dispositivos EBS 304, por ejemplo, con un registrador, cargar los dispositivos EBS 304 en los orificios 306, probar los dispositivos EBS 304, conectar los dispositivos EBS 304 al detonador remoto 106 mediante los respectivos cables 108 (opcionalmente, con uno o más registradores entre los dispositivos EBS 304 y el detonador remoto 106 también conectados mediante los respectivos cables 108 para algunos tipos de dispositivos EBS 304 (por ejemplo, para dispositivos i-kon), y cargar las plataformas correspondientes alrededor de/sobre los dispositivos EBS 304;

c. en la fase preparatoria (P), conectar el controlador 112 al detonador remoto 106 (604B), que incluye: una interfaz de datos del detonador remoto 106 que se conecta a la conexión de red EBS 116, y el detonador remoto 106 enviando un protocolo de enlace de COMUNICACIONES de los mensajes de protocolo de enlace 122 al controlador 112 a través de la interfaz de datos y la conexión de red EBS 116: este protocolo de enlace de COMUNICACIONES confirma que el controlador 112 está conectado comunicativamente al o a cada detonador remoto 106;

d. en la fase preparatoria (P), conectar el controlador 112 al sistema de antena 102 (604B), que incluye: la interfaz de datos bidireccional del sistema de antena 102 que se conecta a la conexión de red WEB 120, y el sistema de antena 102 enviando un protocolo de enlace de COMUNICACIONES de los mensajes de protocolo de enlace de WEB 119 al controlador 112 a través de la interfaz de datos bidireccional y la conexión de red WEB 120: este protocolo de enlace de

COMUNICACIONES confirma al controlador 112 que está conectado comunicativamente al o a cada sistema de antena 102;

e. en una primera fase (1), el controlador 112 configura una voladura concurrente (608), que incluye seleccionar el EBS y el sistema WEB, que incluye seleccionar el o cada detonador remoto 106 y el sistema de antena 102 para el método de voladura 600, por ejemplo, mediante la selección por parte del operador de una voladura dual "concurrente" a través de la UI 126 del controlador 112;

f. en una segunda fase (2), el controlador 112 recibe entradas de inicialización (610), que incluye: (i) el controlador 112 recibe la clave del archivo de blast proporcionada por el operador al controlador 112, (ii) el controlador 112 recibe una confirmación de autorización de baliza, p. ej., leyendo un ID de baliza (p. ej., en un dispositivo RFID), para confirmar que la clave del archivo de blast está asociada con la ubicación de blast definida por el ID de baliza, y (iii) recibe una entrada manual del usuario, p. ej., a través de la GUI, para inicializar el blast—en esta fase, la clave del archivo de blast y el ID de baliza solo son necesarios para el blast WEB y la máquina de estados WEB, y la información proporcionada solo se almacena en el controlador 112 en esta etapa; además, la inicialización del blast en esta fase solo se relaciona con el blast EBS y la máquina de estados EBS;

g. en una tercera fase (3), el detonador remoto 106 inicializa los registradores (612A)—si están presentes—y el detonador remoto 106 verifica la comunicación a través de la conexión de red EBS 116 con el controlador 112, e informa cualquier fallo (incluidos los fallos potenciales) de los dispositivos EBS al controlador 112 en un mensaje de protocolo de enlace adicional de los mensajes de protocolo de enlace 122 (612B);

h. en una cuarta fase (4), si no se verifica la comunicación con el o cada detonador remoto 106 o si se informa un fallo en el siguiente mensaje de protocolo de enlace (de los mensajes de protocolo de enlace 122), el controlador 112 sabe

por el detonador remoto 106 que algo en el proceso falló y por lo tanto el controlador 112 aborta tanto el detonador WEB como el EBS, ya sea automáticamente o por acción del operador;

i. en la cuarta fase (4), si no hay fallos reportados en los mensajes de protocolo de enlace 122, el controlador 112 puede recibir una entrada de programa del operador (mediante un botón de programa en la UI 126), y recibir el dongle de voladura 124 (614), y—en respuesta a la entrada de programa y al dongle de voladura 124 que se recibe—enviar instrucciones de programación al detonador remoto 106 en los mensajes EBS 114;

j. en una quinta fase (5), en respuesta a las instrucciones de programación, el detonador remoto 106 programa los dispositivos EBS 304 (616A) e informa sobre cualquier falla (incluidas las fallas potenciales) al controlador 112 (616B); esto incluye el envío por parte del detonador remoto 106 de un protocolo de enlace PROGRAMADO de los mensajes de protocolo de enlace 122 que indican que los dispositivos EBS 304 están programados para el disparo (y están en el estado PROGRAMADO);

k. en una sexta fase (6), el controlador 112 confirma/acepta posibles fallas en el protocolo de enlace PROGRAMADO (por ejemplo, si el protocolo de enlace PROGRAMADO tarda más que un tiempo de espera seleccionado para recibirse, en ejemplos entre 10 segundos y 3 minutos, dependiendo del tamaño de la ráfaga EBS), o aborta (618), por ejemplo, basándose en la entrada del operador a través de la UI 126;

l. en una séptima fase (7), el controlador 112 envía automáticamente una instrucción de comando ARM al sistema WEB (específicamente al o a cada sistema de antena 102) en los mensajes WEB 118, en donde la instrucción de comando ARM incluye el BID de los dispositivos WEB 302 en esta ráfaga (620)—si el sistema de antena 102 recibe válidamente la instrucción de comando ARM, el sistema de antena 102 envía automáticamente un protocolo de enlace ARM ACKNOWLEDGE al controlador 112 en los mensajes de

protocolo de enlace WEB 119, y si el controlador 112 no recibe este protocolo de enlace ARM ACKNOWLEDGE dentro de un tiempo de espera seleccionado, el controlador 112 aborta automáticamente el método 600 (en los ejemplos, el tiempo de espera seleccionado es entre 2 minutos y 4,5 minutos, dependiendo del tamaño de la ráfaga WEB);

m. en la séptima fase (7), cada detonador remoto 106 mantiene sus dispositivos EBS 304 cargados, por tanto en un estado cargado (622);

n. en la séptima fase (7), el sistema de antena 102 (que incluye el CG) transmite la secuencia MI ARM en las señales MI 104 (624)—como se mencionó anteriormente, la secuencia MI ARM incluye el comando WAKE-UP, el comando START, el/los BID(es) y el comando MI ARM;

o. en una octava fase (8), los dispositivos WEB 302 se despiertan en respuesta al comando WAKE-UP (626);

p. en una novena fase (9), el controlador 112 inicia una ventana de tiempo para que el operador presione/active/seleccione el botón de DETONACIÓN, y detecta cuándo el operador presiona/activa/selecciona el botón de DETONACIÓN, y, en respuesta a que el botón de DISPARO se presione/active/seleccione a través de la UI 126, el controlador 112 envía una instrucción en los mensajes EBS 114 al detonador remoto 106 para controlar el detonador remoto 106 para emitir el comando CHECK, el comando ARM y la secuencia first-last-det-check a los dispositivos EBS conectados 304 (628);

q. en una décima fase (10), en respuesta a la instrucción del controlador 112, el o cada detonador remoto 106 emite el comando CHECK, el comando ARM y la secuencia first-last-det-check a sus dispositivos EBS conectados 304 (630A), e informa cualquier falla al controlador 112 en un mensaje de protocolo de enlace adicional de los mensajes de protocolo de enlace 122 (630B);

r. En una undécima fase (11), el controlador 112 aborta automáticamente si falla la secuencia de comprobación de primera y última detonación (como se informa

en el mensaje de protocolo de enlace adicional) en la décima fase (632A); de lo contrario, el controlador 112 accede automáticamente a un tiempo predeterminado para ordenar a los dispositivos WEB 302 y a los dispositivos EBS 304 que disparen (incluido un intervalo predeterminado denominado "retardo de disparo de MI" que se describe más adelante), y luego el controlador 112, en el tiempo T = 0, instruye automáticamente al sistema de antena 102 para que transmita la secuencia MI DETONAR enviando una instrucción de comando de disparo al sistema de antena 102 en los mensajes WEB 118 (632B). Si el sistema de antena 102 recibe válidamente la instrucción de comando MI DETONAR, el sistema de antena 102 envía automáticamente un protocolo de enlace de reconocimiento de MI DETONAR al controlador 112 en los mensajes de protocolo de enlace WEB 119, y si el controlador 112 no recibe esto. Cuando MI DETONAR reconoce el protocolo de enlace dentro de un tiempo de espera seleccionado, el controlador 112 cancela automáticamente el método 600 (en los ejemplos, el tiempo de espera seleccionado es de aproximadamente 4 segundos (solo para DETONACIÓN) o aproximadamente 30 segundos (en implementaciones en las que SINCRONIZAR está configurado para realizarse después de que el usuario presione el botón DETONACIÓN);

s. en una duodécima fase (12), en respuesta a las instrucciones del controlador 112, el sistema de antena 102 (a través del CG 504) transmite la secuencia MI DETONAR, incluyendo el comando MI SINCRONIZAR y el comando MI DETONAR (634);

t. en una decimotercera fase (13), los dispositivos WEB 302 reciben el comando MI SINCRONIZAR y sincronizan sus relojes internos (636)—en respuesta al comando MI SINCRONIZAR, todos los dispositivos WEB 302 sincronizan sus relojes, por ejemplo, inician de manera sincrónica un cronómetro que hace tictac exactamente una vez cada 0,5 segundos;

u. en una decimocuarta fase (14), el controlador 112, de acuerdo con el retardo de disparo MI predeterminado, es decir en T = (retardo de disparo MI), instruye automáticamente al o a cada detonador remoto 106, mediante el envío de una

instrucción de comando EBS DETONAR, para emitir el comando de preparación para disparar y el comando DETONACIÓN (638);

v. en una decimoquinta fase (15), en respuesta a la instrucción de comando DETONAR del EBS, desde el controlador 112 en la decimocuarta fase (14), el o cada detonador remoto 106 transmite el comando de preparación para disparar seguido del comando DETONAR a los dispositivos EBS 304 (640);

w. en la decimoquinta fase (15), los dispositivos WEB 302 reciben el comando MI DETONAR y emiten señales DETONAR a sus respectivos detonadores electrónicos de acuerdo con sus relojes sincronizados (642)—cuando los dispositivos WEB 302 han recibido el comando MI DETONAR, cada uno espera hasta el siguiente tic de tiempo que ocurre (por ejemplo, en la marca de 0,5 segundos), y envían el comando DETONAR a sus detonadores electrónicos en ese tic de tiempo; y

x. en una decimosexta fase (16), los dispositivos EBS 304 se disparan, en respuesta al comando DETONAR (del detonador remoto 106) (644), y los dispositivos WEB 302 se disparan sustancialmente de manera concurrente con los dispositivos EBS 304, en respuesta a las señales DETONACIÓN (646).

[0091] En el método de doble disparo 600, el lanzador remoto 106 no espera la orden MI ARM ni la orden MI DETONAR, ya que no hay una caja de sincronización 202 en el sistema de doble disparo 100. En su lugar, el controlador 112 primero ordena automáticamente al sistema de antena 102 que transmita la secuencia MI DETONAR (en 632) y, posteriormente, en un momento determinado por el intervalo predeterminado denominado "retardo de disparo MI", ordena al lanzador remoto 106, según la temporización del EBS, que emita la orden de preparación para disparar y la orden DETONACIÓN (en 638). Por lo tanto, el retardo de disparo de MI representa de forma aproximada, sustancial o precisa los retrasos esperados/medidos en el sistema WEB (incluidos los retrasos en los mensajes WEB 118, el sistema de antena 102, las señales MI 104 y los dispositivos WEB 302) en comparación con los retrasos en el EBS (incluidos los retrasos en los mensajes EBS 114, el detonador remoto 106, los cables 108, los registradores, si los hay, y los dispositivos EBS 304). Dependiendo de

los detalles de la implementación, el retardo de disparo de MI puede representar con precisión el retardo de DISPARO de MI (dentro de un margen de error que no afecta los resultados de la voladura). El retardo de disparo de MI predeterminado puede determinarse para cada implementación del sistema de voladura dual 100, como se describe a continuación con referencia a la undécima fase (11). El uso del retardo de disparo de MI supone que la orden de DISPARO de MI llegará a los dispositivos iniciadores inalámbricos 302.

[0092] En la segunda fase (2), tras el envío del protocolo de enlace PROGRAMADO, o antes en el método 600, el operador inserta la clave del archivo de envío en el controlador 112 y confirma la autorización de la baliza. El controlador 112 recibe así una entrada manual del operador (p. ej., la inserción de la clave del archivo de envío o la operación de la interfaz de usuario 126) para mover ambas máquinas de estados al siguiente modo, p. ej., el modo ARM (p. ej., mediante la pulsación, activación o selección del botón ARM en el controlador 112 por parte del operador). En el método 600, la clave del archivo de envío puede insertarse en cualquier momento hasta el envío de la secuencia ARM. La confirmación de la autorización de la baliza se relaciona con el sistema WEB: el operador debe presentar el ID de la baliza (p. ej., una tarjeta o etiqueta RFID) al controlador 112 para garantizar que los BID del envío WEB estén vinculados a la ubicación del envío. El identificador de la baliza se encuentra en la voladura o en el tajo y debe obtenerse antes de la voladura. La confirmación de la autorización de la baliza puede evitar que se dispare una voladura incorrecta y confirma que la ubicación de la voladura y los identificadores de la baliza coinciden con el plan de voladura.

[0093] Con referencia a la cuarta fase (4), el controlador 112 sabe por el detonador remoto 106 que algo en el proceso falló porque el detonador remoto 106 responde a las solicitudes del controlador 112, por ejemplo, el controlador 112 puede ordenar al detonador remoto 106 que programe todos los dispositivos EBS y, después de un cierto tiempo, el controlador 112 comienza a sondear al detonador remoto 106 para confirmación y, una vez que llega la confirmación, el controlador 112 establece su máquina de estados interna en el estado "dets programados" o, si la confirmación falla, el controlador 112 aborta el lanzamiento.

[0094] Con referencia a la sexta fase (6) —incluida la confirmación/aceptación por parte del controlador 112 de los fallos potenciales o la cancelación (618)— el detonador remoto 106 puede confirmar que algunos/la mayoría (por ejemplo, alrededor de 100) de los dispositivos

EBS 304 están programados con éxito, pero algunos/pocos (por ejemplo, 2) no lo están, en cuyo caso el operador recibe un mensaje de fallo dedicado en la UI 126 para decidir si desea cancelar o disparar el detonador con algunos o pocos de los dispositivos EBS 304 no programados (confirmando/aceptando así los fallos de encendido) seleccionando proceder mediante la UI 126.

[0095] Con referencia a la séptima fase (7), después de que ambas máquinas de estado entran en el modo ARM, el controlador 112 envía la secuencia MI ARM en los mensajes WEB 118 al sistema de antena 102, en respuesta a lo cual el sistema de antena 102 transmite la secuencia MI ARM a los dispositivos WEB 302, y en respuesta a lo cual los dispositivos WEB 302 validan la secuencia MI ARM recibida (utilizando un método de validación automático en los dispositivos WEB 302, por ejemplo, como lo hacen los dispositivos WebGen) y los dispositivos WEB 302 pueden sincronizar sus respectivos relojes (por ejemplo, como lo hacen los dispositivos WebGen 100).

[0096] En la novena fase (9), el controlador 112 puede controlar que las comprobaciones de detonación primera-última se realicen lo más cerca posible del momento de la explosión mediante la emisión de una señal de la secuencia de comprobación de detonación primera-última (en 628).

[0097] En la décima fase (10), el detonador remoto 106 envía los comandos CHECK, ARM y la secuencia de comprobación de primer y último det a sus dispositivos EBS 304 conectados (en 630A), a través de los registradores conectados, si los hay (que transmiten los comandos CHECK y ARM a los dispositivos EBS 304). Si los hay, cada registrador comprueba que el primer y el último det de su red estén correctamente armados. A continuación, el registrador informa al detonador remoto 106 si la comprobación fue exitosa. El detonador remoto 106 informa al controlador 112 de cualquier fallo (en 630B), que podría ser la respuesta a una siguiente solicitud de estado del controlador 112.

[0098] En la undécima fase (11), si la comprobación de detección falla en cualquiera de los dispositivos EBS conectados 304 (como se indica en 630B), el controlador 112 cancela automáticamente la transmisión EBS y la transmisión WEB. Si la comprobación falla, el registrador (si está presente) informa "no armado correctamente" al detonador remoto 106, y

el detonador remoto 106 informa al controlador 112 en la siguiente respuesta de estado en los mensajes de protocolo de enlace 122.

[0099] En la undécima fase (11), el controlador 112 accede automáticamente al tiempo predeterminado para ordenar a cada detonador remoto 106 que emita el comando de preparación para disparar para que sus registradores pasen los siguientes comandos a sus dispositivos EBS conectados 304. El controlador 112 recibe/accede al retardo de disparo de MI (que incluye un valor de tiempo de retardo esperado predeterminado), que es el tiempo que se espera que transcurra entre el envío del comando de DISPARO DE MI en las señales MI 104 y el envío de las señales de DISPARO de los dispositivos WEB 304 a sus detonadores. El retardo de disparo de MI se predetermina en función de las propiedades, la configuración y las mediciones del sitio y la conexión de red WEB 120, por ejemplo, el tiempo de propagación de las señales MI 104, la configuración de la conexión de red WEB 120 y la configuración del sistema de antena 102. A partir del retardo de disparo de MI, el controlador 112 selecciona el momento de enviar las instrucciones de disparo de EBS para proporcionar un disparo prácticamente simultáneo de ambos sistemas (WEB y EBS); por lo tanto, el momento de envío de las instrucciones de disparo de EBS se selecciona para que coincida sustancialmente con el retardo de disparo de MI. Sin embargo, como esto no está sincronizado y puede incluir una inexactitud, por ejemplo, de aproximadamente un segundo debido a una latencia impredecible, este método 600 se describe como voladura "concurrente" en lugar de sincronizada. El valor del retardo de disparo de MI puede predeterminarse en ensayos de laboratorio o pruebas experimentales. Las latencias impredecibles pueden alcanzar prácticamente un segundo, incluyendo la latencia de red entre el controlador 112 y el CG 504 del sistema de antena 102 (p. ej., latencia LTE o Ethernet) y una latencia en los dispositivos WEB 302 que el controlador 112 desconoce, ya que depende de la calibración de sus relojes. Cuando el sistema de antena 102 envía el comando MI DETONAR y los dispositivos WEB 302 lo reciben, todos envían la señal DETONACIÓN a sus dispositivos simultáneamente, pero en un intervalo de hasta prácticamente medio segundo tras recibir el MI-DETONAR, dependiendo de la sincronización (como se describió anteriormente). El tiempo entre la recepción del comando DETONACIÓN y su envío es impredecible y se denomina latencia en los dispositivos WEB 302.

[0100] En la decimotercera fase (13) y la decimoquinta fase (15), los dispositivos WEB 304 que reciben los comandos de voladura MI (incluido el comando MI SINCRONIZAR y el

comando MI DETONAR) validan automáticamente los comandos de voladura, por ejemplo, utilizando el proceso de validación de dispositivos WebGen existentes, por ejemplo, basándose en la coincidencia de un BID en el comando de voladura con un BID codificado en cada dispositivo WEB 304.

Sistema de voladura sincronizada

[0101] En el sistema de voladura sincronizada 200, como se muestra en la FIG. 2, el controlador 112 está configurado para enviar los mensajes WEB 118 al sistema de antena 102 a través de la conexión de red WEB 120 de manera equivalente a las conexiones en el sistema de voladura dual 100.

[0102] A diferencia del sistema de doble voladura 100, el sistema de antena 102 envía los mensajes WEB 118 (a través de las señales MI 104) a un módulo receptor MI 202 (denominado en este documento "dispositivo de sincronización MI" o "caja de sincronización 202"), configurado para generar señales de sincronización 204 (que representan los mensajes WEB 118 y, opcionalmente, las mediciones de SNR) y las envía al detonador remoto 106 a través de una interfaz de comunicación, denominada en este documento "interfaz SINCRONIZAR 206" (por ejemplo, una interfaz serie RS485 en la caja de sincronización 202). Las señales de sincronización 204 sincronizan (lo que incluye el control de la temporización) el detonador remoto 106 con los mensajes WEB 118 recibidos. Esta sincronización permite un funcionamiento seguro y eficaz de los dispositivos WEB 302 y los dispositivos EBS 304 en una voladura combinada, también denominada "voladura sincronizada". La caja de sincronización 202 extrae eficazmente los mensajes WEB 118 y sincroniza y envía las señales de sincronización 204 al detonador remoto 106 conectado. La caja de sincronización 202 cuenta con un detonador remoto 106, por lo que puede requerirse una caja de sincronización 202 dedicada para cada detonador remoto 106, incluso cuando los emisores remotos 106 se encuentran en diferentes puntos del sitio y cada uno necesita una captación para las señales MI 104 que transportan los mensajes WEB 118. El detonador remoto 106 sincroniza (lo que incluye controlar la temporización) los comandos EBS con las señales de sincronización recibidas 204 que representan los mensajes WEB 118, mediante el método de emisión sincronizada 700, como se describe a continuación.

[0103] Puede existir una latencia incontrolable entre el controlador 112 y el sistema de antena 102, lo que dificulta la coordinación, sincronización y control precisos de la temporización de los mensajes en las señales MI 104 para los dispositivos WEB (320) con los mensajes para los dispositivos EBS (304). La caja de sincronización 202 permite al sistema 200 gestionar la latencia incontrolable entre el controlador 112 y el sistema de antena 102.

[0104] Como se muestra en la Fig. 2, la o cada caja de sincronización 202 puede ser una unidad/módulo independiente del detonador remoto 106, por ejemplo, ubicada en un túnel de acceso 208 durante su uso en la obra, de modo que las señales MI 104 del sistema de antena 102 lleguen de forma fiable y sustancial a la caja de sincronización 202, preferiblemente con una relación señal-ruido (SNR) de MI superior al umbral predefinido (las mediciones de SNR proporcionan información para confirmar si se reciben correctamente las señales MI; sin embargo, no son necesarias para una explosión sincronizada). La caja de sincronización 202 puede incluir una carcasa protectora para protegerla en el túnel de acceso 208 y del entorno de la obra, incluyendo el polvo, el calor y la presión. En uso, la o cada caja de sincronización 202 se dispone/ubica/entierra en la trayectoria de las señales MI 104. La o cada caja de sincronización 202 incluye un magnetómetro en forma de una antena y un receptor MI sintonizados adecuadamente, p. ej., equivalente a un DRX de un dispositivo WebGen, y está configurada para generar una salida electrónica/eléctrica que representa las señales de sincronización 204 para la interfaz SINCRONIZAR 206. Como alternativa o adicional a que la o cada caja de sincronización 202 sea la unidad/módulo separado del detonador remoto 106, la o cada caja de sincronización 202 puede ser una unidad/módulo incorporado al detonador remoto 106 correspondiente, p. ej., acoplado directamente al detonador remoto 106 (p. ej., en una carcasa/estuche protector del detonador remoto 106, con la interfaz SINCRONIZAR 206 que incluye una conexión de enchufe/toma eléctrica en lugar de un cable largo como para el emisor separado La caja de sincronización 202 proporciona al detonador remoto 106 la antena y el receptor MI sintonizados adecuadamente para recibir las señales MI 104. La caja de sincronización 202 y/o el detonador remoto 106 pueden incluir blindaje conductor/magnético entre la antena MI y/o el receptor de la caja de sincronización 202 y los componentes eléctricos/electrónicos del detonador remoto 106 para bloquear/mitigar la interferencia electromagnética (EMI) radiativa del detonador remoto 106 que genera señales/ruido espurios/indeseables en la caja de sincronización 202; Si la caja de sincronización 202 está

incorporada al detonador remoto 106 correspondiente, el blindaje conductor/magnético está dispuesto para bloquear/mitigar la EMI del detonador remoto 106, permitiendo al mismo tiempo la recepción/detección de las señales MI 104 por el magnetómetro de la caja de sincronización 202. La caja de sincronización 202 y/o el detonador remoto 106 pueden configurarse para tener frecuencias operativas separadas (denominadas, por tanto, una "separación de frecuencia EMI"), de modo que las frecuencias operativas de los componentes del detonador remoto 202 prácticamente no se superpongan con las frecuencias operativas de la antena MI sintonizada y el receptor de la caja de sincronización 202. De esta manera, si el detonador remoto 106 genera una EMI no deseada, el receptor de la caja de sincronización 202 no la detecta o, al menos, no la confunde con las señales MI 104 debido a la separación de frecuencias. Esta separación de frecuencias Para mitigar la EMI se incluye que la antena MI tenga una o más frecuencias centrales/resonantes que no se superpongan con las frecuencias radiativas operativas del detonador remoto 106. La caja de sincronización 202 puede insertarse de forma extraíble y/o conectarse manualmente al detonador remoto 106, lo que permite configurar convenientemente el detonador remoto 106 para una operación sincronizada (mediante el método de detonación sincronizada 700) si es necesario; por lo tanto, el detonador remoto 106 puede reconfigurarse entre detonación EBS pura, detonación dual según el método de detonación dual 600 y detonación sincronizada según el método de detonación sincronizada 700. La caja de sincronización 202 puede estar dispuesta en lo profundo del túnel de acceso 208, que puede ser un pozo (y la interfaz SINCRONIZAR 206 puede incluir un cable/alambre de comunicaciones), puede estar dispuesta cerca o en el collar del túnel de acceso 208, puede estar dispuesta dentro de una línea de visión (LOS) del detonador remoto 106 (y la interfaz SINCRONIZAR 206 puede incluir un enlace de comunicaciones LOS o por aire (TTA) con Prácticamente sin latencia (p. ej., mediante wifi), o puede instalarse en el detonador remoto 106 o en su interior (con blindaje EMI o separación de frecuencia EMI). La caja de sincronización 202 no requiere certificación SIL3, ya que no puede generar un voltaje de disparo suficiente para disparar un detonador, a diferencia de los dispositivos WEB 302.

[0105] Además de los dispositivos de medición de MI descritos anteriormente, en el sistema de voladura sincronizada 200, como se muestra en la figura 2, la medición de la relación señal-ruido (SNR) puede ser generada por la caja de sincronización 202, que incluye o actúa como uno de los dispositivos de medición de MI. Por lo tanto, la caja de sincronización 202 verifica

la buena comunicación de MI consigo misma. Esta medición de la SNR proporciona un control para mitigar el riesgo de que los dispositivos WEB 302 se disparen, pero no los dispositivos EBS 304, debido a una señal de disparo de MI demasiado débil. En el proceso de voladura proporcionado por el sistema de voladura sincronizada 200, las mediciones de MI de la caja de sincronización 202 determinan si las señales de MI recibidas son lo suficientemente buenas para una recepción segura.

Método de voladura sincronizada

[0106] El sistema de voladura sincronizada 200 ejecuta el método de voladura sincronizada 700 de forma automática o prácticamente automática. En el sistema de voladura sincronizada 200, la voladura EBS solo se dispara si la caja de sincronización 202 detecta y valida la secuencia MI DETONAR con suficiente relación señal-ruido (SNR). Por lo tanto, si el sistema de antena 102 se interrumpe durante la transmisión de la secuencia MI DETONAR, la voladura EBS y la voladura WEB no se dispararán.

[0107] Como se muestra en la FIG. 7, el método de voladura sincronizada 700 incluye:

a. en fase preparatoria (P), codificando y cargando el dispositivo WEB 302 (702) como en el método de doble voladura 600;

b. en la fase preparatoria (P), registro, carga, conexión y prueba de los dispositivos EBS 304 (704A) como en el método de voladura dual 600;

c. en la fase preparatoria (P), conectar el controlador 112 al detonador remoto 106 (704B) como en el método de detonador dual 600, paso 604B;

d. en la fase preparatoria (P), conectar el controlador 112 al sistema de antena 102 (704B) como en el método de doble voladura 600, paso 604B;

e. en la fase preparatoria (P), codificar y conectar la caja de sincronización 202 (706), que incluye conectar la caja de sincronización 202 al detonador remoto 106 y al controlador 112 - la codificación se puede hacer antes de la carga, o más tarde en el método 700, por ejemplo, directamente antes de la explosión;

f. en la fase preparatoria (P), conectando el controlador 112 a la caja de sincronización 202 (706B), que incluye: la interfaz SINCRONIZAR 206 de la caja de sincronización 202 que se conecta a la red de datos (por ejemplo, la red de minas, por ejemplo, a través del detonador remoto 106) y la caja de sincronización 202 envía un protocolo de enlace de COMUNICACIONES de los mensajes de protocolo de enlace 122 al controlador 112 o al detonador remoto 106 a través de la interfaz de SINCRONIZACIÓN 206; este protocolo de enlace de COMUNICACIONES confirma al controlador 112 y/o al detonador remoto 106 que la caja de sincronización 202 está conectada comunicativamente a ellos;

g. en una primera fase (1), el controlador 112 configura una explosión sincronizada (708), por ejemplo, mediante la selección por parte del operador de una explosión sincronizada a través de la IU 126 del controlador 112 (en lugar de seleccionar una explosión dual/concurrente como en el método de explosión dual 600), y el controlador 112 recibe información para la explosión inalámbrica a partir de la clave del archivo de explosión y la identificación de la baliza;

h. en una segunda fase (2), el controlador 112 recibe entradas de inicialización (710) como en el método de doble voladura 600, y luego instruye al detonador remoto 106 para que inicialice los dispositivos EBS 304 e instruye al sistema de antena 102 para que inicialice los dispositivos WEB 302;

i. en una tercera fase (3), el detonador remoto 106 inicializa los dispositivos EBS 304 —a través de los registradores (712A) si están presentes (712A)— como en el método de detonador dual 600;

j. En la tercera fase (3), el detonador remoto 106 y/o el controlador 112 verifican la comunicación con la caja de sincronización 202 a través de la interfaz SINCRONIZAR. (712B);

k. en la tercera fase (3), el detonador remoto 106 verifica la comunicación a través de la conexión de red EBS 116 con el controlador 112, y reporta cualquier falla

(incluyendo fallas potenciales) de los dispositivos EBS 304 al controlador 112 como en el método de doble voladura 600, y cualquier falla de comunicación con la caja de sincronización 202 (712C);

l. en una cuarta fase (4), si no se verifica la comunicación con el o cada detonador remoto 106 y la caja de sincronización 202 o si se reporta un fallo en el proceso 712C, el controlador 112 aborta tanto el detonador WEB como el EBS (714), como en el método de detonador dual 600;

m. en la cuarta fase (4), si no hay fallos, el controlador 112 recibe una entrada de programa del operador y recibe el dongle de voladura 124 (714), como en el método de voladura dual 600;

n. en una quinta fase (5), en respuesta a las instrucciones del controlador 112, el detonador remoto 106 programa los dispositivos EBS 304 (716A), y reporta cualquier falla (incluyendo fallas potenciales) al controlador 112 (716B), como en el método de doble voladura 600 ;

o. en una sexta fase (6), el controlador 112 confirma/acepta fallos potenciales o aborta (718), como en el método de doble voladura 600;

p. en una séptima fase (7), el controlador 112 ordena a la caja de sincronización 202 (por ejemplo, a través del detonador remoto 106 que utiliza los mensajes EBS 114) que espere un comando MI ARM, o alternativamente el detonador remoto 106 ordena a la caja de sincronización 202 de manera autónoma basándose en su propia máquina de estados; y luego, en respuesta a la instrucción de espera, la caja de sincronización 202 espera el comando MI ARM (719A), y el controlador 112 muestra una indicación al operador de que la caja de sincronización 202 está esperando que se detecte el comando MI ARM (719B);

q. en una fase de ocho (8), el controlador 112 envía automáticamente una instrucción de comando ARM al sistema WEB (específicamente al o a cada sistema de antena 102) en los mensajes WEB 118, en donde la instrucción de comando ARM incluye el BID de los dispositivos WEB 302 (y el

SINCRONIZAR-box 202) en esta ráfaga (720), como en el método de ráfaga dual 600 excepto que el SINCRONIZAR-box 202 está presente—y, como en el método de ráfaga dual 600, si el sistema de antena 102 recibe válidamente la instrucción de comando ARM, el sistema de antena 102 envía automáticamente un protocolo de enlace ARM ACKNOWLEDGE al controlador 112 en los mensajes de protocolo de enlace WEB 119, y si el controlador 112 no recibe este protocolo de enlace ARM ACKNOWLEDGE dentro de un tiempo de espera seleccionado, el controlador 112 aborta automáticamente el método 700;

r. en la octava fase (8), cada detonador remoto 106 mantiene sus dispositivos EBS 304 cargados, por tanto en un estado cargado (722), como en el método de detonador dual 600;

s. en la octava fase (8), el sistema de antena 102 (que incluye el CG) transmite la secuencia MI ARM en las señales MI 104 (724), como en el método de doble voladura 600;

t. en una novena fase (9), los dispositivos WEB 302 se despiertan en respuesta al comando WAKE-UP (726A), como en el método de doble voladura 600;

u. en la novena fase (9), la caja de sincronización 202 recibe el comando WAKE-UP, y opcionalmente otras señales MI 104 de la secuencia MI ARM, y opcionalmente mide/determina al menos un valor SNR de las señales MI 104 (726B);

v. En la novena fase (9), la caja de sincronización 202 informa el valor de la relación señal-ruido (SNR) y/o si es “buena” (en relación con el umbral predefinido). al controlador 112 y/o al detonador remoto 106 utilizando la señal de salida electrónica/eléctrica que representa la SNR medida, incluso a través de la interfaz de sincronización 206 al detonador remoto 106, que envía información que representa la SNR medida al controlador 112 (726C);

w. en una décima fase (10), el controlador 112 muestra el valor SNR y/o si es bueno, y aborta automáticamente la explosión si el SNR está por debajo del umbral predefinido (726D);

x. en una undécima fase (11), el o cada detonador remoto 106 ejecuta los comandos CHECK y ARM, y la secuencia first-last-det-check (730A), e informa cualquier falla al controlador 112 (730B), como en el método de voladura dual 600;

y. en una duodécima fase (12), el controlador 112 aborta automáticamente si la secuencia de comprobación de primera-última detonación falla en la undécima fase (732A), como en el método de voladura dual 600; de lo contrario muestra al operador que la voladura está lista para disparar (732B);

z. en una decimotercera fase (13), el controlador 112 detecta cuando el operador presiona/activa/selecciona el botón DETONACIÓN, y—en respuesta a que el botón DETONACIÓN sea presionado/activado/seleccionado a través de la UI—el controlador 112 envía una instrucción de comando MI DETONAR en los mensajes WEB 118 al sistema de antena 102 para emitir la secuencia MI DETONAR (732C) —y, como en el método de doble voladura 600, si el sistema de antena 102 recibe válidamente la instrucción de comando MI DETONAR, el sistema de antena 102 envía automáticamente un protocolo de enlace de reconocimiento MI DETONAR al controlador 112 en los mensajes de protocolo de enlace WEB 119, y si el controlador 112 no recibe este protocolo de enlace de reconocimiento MI DETONAR dentro de un tiempo de espera seleccionado, el controlador 112 aborta automáticamente el método 700 ;

aa. en una decimocuarta fase (14), en respuesta a la instrucción de comando MI DETONAR en los mensajes WEB 118, el sistema de antena 102 (con el CG) transmite la secuencia MI DETONAR, incluyendo el comando SINCRONIZAR y el comando MI DETONAR (734), como en el método de doble voladura 600;

bb. en una decimoquinta fase (15), los dispositivos WEB 302 reciben el comando MI SINCRONIZAR, sincronizando en respuesta sus relojes internos (736);

cc. en la decimoquinta fase (15), la caja de sincronización 202 recibe el comando MI SINCRONIZAR (737) y sincroniza en respuesta su reloj;

dd. en la decimoquinta fase (15), si el EBS incluye los registradores, tanto la caja de sincronización 202 como el detonador remoto 106 acceden a/determinan un tiempo para ordenar al detonador remoto 106 que emita la orden de preparación para disparar a los registradores ("T1") con antelación de modo que, después de que la caja de sincronización 202 reciba el comando MI DETONAR y se produzca el siguiente tictac del reloj, la caja de sincronización 202 pueda emitir un comando DETONACIÓN en la interfaz de sincronización 206 (de forma síncrona con todos los dispositivos WEB 304 enviando comandos DETONACIÓN a sus detonadores) que se reenvía inmediatamente (con el borde de la señal de salida siguiendo al borde de la señal de entrada) por el detonador remoto 106 a los dispositivos EBS 306, por tanto sin latencia impredecible, incluso a través de los registradores si están presentes, como se describe más adelante en una decimoséptima fase (17);

ee. En una decimosexta fase (16), (i) la caja de sincronización 202, según su sincronización determinada "T1" para el detonador remoto 106 en la decimoquinta fase (15) y con base en un reloj interno de la caja de sincronización 202, ordena al detonador remoto 106 o a cada detonador remoto 106 que emita la orden de preparación para disparar a los registradores, y en respuesta, el detonador remoto 106 o cada detonador remoto 106 emite la orden de preparación para disparar; o (ii) el detonador remoto 106 emite por sí mismo la orden de preparación para disparar según su sincronización determinada "T1" para la decimoquinta fase (15) y con base en un reloj interno del detonador remoto 106 (738).

ff. en la decimoséptima fase (17), la caja de sincronización 202 y los dispositivos WEB 302 reciben sustancialmente de manera simultánea el comando MI DETONAR (740);

gg. en la decimoséptima fase (17), la caja de sincronización 202, en respuesta al comando MI DETONAR, emite el comando DETONAR al o a cada detonador remoto 106 según su reloj sincronizado, y luego el o cada detonador remoto 106, de manera responsiva e inmediata (prácticamente sin latencia), reenvía el comando DETONAR a todos sus dispositivos EBS 304 conectados (a través de los registradores, si están presentes); y

hh. en la decimoséptima fase (17), los dispositivos WEB 302, en respuesta al comando MI DETONAR, emiten señales de DETONACIÓN a sus respectivos detonadores electrónicos de acuerdo con sus relojes sincronizados (742); y

ii. en una decimoctava fase (18), los dispositivos EBS 304 disparan, en respuesta a sus comandos de DISPARO (del o de cada detonador remoto 106) (744); y los dispositivos WEB 302 disparan sustancialmente en simultáneo con los dispositivos EBS 304, en respuesta a las señales de DISPARO (746).

[0108] En la fase preparatoria (P), la codificación, conexión y carga del SINCRONIZAR-box 202 (706) incluye opcionalmente codificar el SINCRONIZAR-box 202 con el BID usando el codificador, que incluye el mismo proceso que la codificación de los dispositivos WEB 302—esto es opcional porque la asignación del BID al SINCRONIZAR-box 202 puede lograrse alternativamente de manera automática a través del detonador remoto 106 una vez que el controlador 112 ha leído la clave del archivo blast, o el BID puede ser fijo, asignado permanentemente al SINCRONIZAR-box 202—en cualquier caso, el controlador 112 tiene el BID del SINCRONIZAR-box 202 almacenado de tal manera que el BID del SINCRONIZAR-box 202 se usa en los mensajes WEB 118 y así estos mensajes son reconocidos/decodificados/validados por el SINCRONIZAR-box 202 a través de la comparación con su BID almacenado/asignado.

[0109] En la octava fase (8), después de enviar la secuencia MI ARM en los mensajes WEB 118, el controlador 112 puede determinar opcionalmente (y mostrar opcionalmente a un

operador en la UI 126 y/o el detonador remoto 106) la SNR de las señales MI tal como las reciben los dispositivos de medición de MI (por ejemplo, la caja de sincronización 202) y, si la SNR medida está por debajo del umbral predefinido, el controlador 112 puede abortar automáticamente la ráfaga EBS y la ráfaga WEB. En un escenario de sincronización (con la caja de sincronización 202), cuando la caja de sincronización 202 recibe/mide una relación señal-ruido (SNR) demasiado baja, y la caja de sincronización 202 le dice al controlador 112 directamente que la SNR es demasiado baja, o la caja de sincronización 202 le dice al detonador remoto 106, que a su vez le dice al controlador 112 en la siguiente solicitud de estado que la SNR es demasiado baja, y luego el controlador 112 decide abortar.

[0110] La novena fase (9) puede incluir la recepción por parte del SINCRONIZAR-box 202 del comando MI ARM y luego la validación del comando MI ARM recibido (utilizando un método de validación automático en los dispositivos WEB 302, por ejemplo, como lo hacen los dispositivos WebGen), y, si la validación falla, el envío de una señal ABORT/DISABLE al controlador 112, a través de las señales de sincronización 204, el detonador remoto 106 y los mensajes de protocolo de enlace 122, en respuesta a lo cual el controlador 112 aborta automáticamente el envío EBS y aborta el envío WEB.

[0111] En la decimoquinta fase (15), en respuesta a la validación del comando de DISPARO por parte de la caja de sincronización 202, la caja de sincronización 202 (y/o el detonador remoto 106) o cada detonador remoto 106 utiliza automáticamente el tiempo "T1". El tiempo "T1" es el tiempo que tarda el detonador remoto 106 en emitir el comando de preparación para disparar para que sus registradores transmitan todos los comandos posteriores a todos los dispositivos conectados. Dispositivos EBS 304 sin retardo/latencia. "T1" es un tiempo fijo predeterminado/seleccionado para la implementación del sistema de voladura sincronizada 200 y depende del tiempo predeterminado durante el cual los registradores pasan activamente todos los comandos después de recibir la orden de preparación para disparar, lo que se conoce como estado de "preparación para disparar". Cuando los registradores reciben la orden de preparación para disparar del dinamitero remoto 106, solo permanecen en estado de "preparación para disparar" durante unos segundos. En algunas implementaciones, el tiempo entre MI-SINCRONIZAR y MI-DETONAR es de aproximadamente 7 segundos, y "T1" se determina/selecciona de tal manera que la señal de preparación para disparar no se envíe demasiado pronto antes de que llegue la señal MI-DETONAR, manteniendo así a los

registradores en estado de "preparación para disparar" el tiempo suficiente para ejecutar la orden de DISPARO sin retardo/latencia. El comando de preparación para disparar solo puede ser necesario en una implementación del sistema de voladura sincronizada 200 que incluya los registradores, ya que este comando controla a los registradores para que envíen el siguiente comando (que normalmente será "DISPARO" en el método de voladura sincronizada 700) a los dispositivos EBS 304 sin retardo ni latencia para sincronizarse con los dispositivos WEB 302. El tiempo "T1" es necesario porque los registradores tienen un tiempo límite después de prepararse para disparar; por lo tanto, el comando "DISPARO" debe llegar antes de que finalice este tiempo límite para evitar latencia o retrasos; de lo contrario, los registradores podrían responder con errores de tiempo límite en lugar de disparar los dispositivos EBS 304 con sincronía. El tiempo "T1" es entonces un tiempo de retardo constante (para cada implementación del sistema de voladura sincronizada 200, dependiendo de sus registradores) que está predeterminado/seleccionado en función del período de tiempo de espera predeterminado de los registradores (por ejemplo, sustancialmente 5 segundos) y el intervalo de tiempo predeterminado entre los comandos MI-SINCRONIZAR y MI-DETONAR (por ejemplo, sustancialmente 7 segundos), por ejemplo, el tiempo "T1" puede estar entre sustancialmente 2 segundos y 6 segundos.

Sistema de antena 102

[0112] Como se muestra en la FIG. 5. El sistema de antena 102 puede incluir un sistema de antena de bucle 500 que incluye una antena de bucle 502 (p. ej., como la utilizada en sistemas WebGen existentes con antenas más grandes, p. ej., con diámetros de 40 m) dimensionada y ubicada para generar y dirigir las señales MI 104 en la dirección o área requerida, hacia los dispositivos de detonación electrónica 110, el dispositivo de medición de MI y la caja de sincronización 202. La antena de bucle 502 es accionada por un generador de corriente 504 ("CG", p. ej., como el utilizado en sistemas WebGen existentes) del sistema de antena 102. El generador de corriente 504 está configurado y opera para recibir los mensajes WEB 118 del controlador 112 y los codifica en la modulación de una corriente de excitación hacia la antena de bucle 502 para modular/codificar las señales MI 104. Las señales MI 104 se generan en un área sustancial del plano de la antena de bucle 502 con una frecuencia portadora

sustancialmente igual. Modulación y fase. La antena de bucle 502 puede incluir dos o más bucles/bobinados, todos alimentados por una única fuente de corriente.

Codificación y carga de dispositivos WEB 302

[0113] Un trabajador autorizado o un cargador automático puede obtener un dispositivo WEB 302 del almacén. El trabajador autorizado puede usar un codificador portátil para programar el dispositivo WEB 302 mediante un procedimiento de codificación manual, o el cargador automático puede usar un codificador integrado para programar el dispositivo WEB 320 mediante un procedimiento de codificación. Durante el procedimiento de codificación, el codificador puede comunicar (a) información sobre el tiempo de detonación correspondiente a un retardo de inicio para el dispositivo WEB 302 (p. ej., correspondiente a un retardo preciso que este dispositivo WEB 302 está programado para esperar antes de activar la unidad de iniciación explosiva después de que reciba la orden de DISPARO); y, opcionalmente, (b) el GID/BID. Una vez codificado el dispositivo WEB 302 mediante el procedimiento de codificación, este puede procesar y ejecutar comandos, incluyendo, por ejemplo, los comandos MI de DESPERTAR, ACTIVAR y DISPARO. Tras su codificación, si el dispositivo WEB 302 se encuentra dentro del alcance de comunicación de la señal del sistema de antena 102, se activará para provocar la iniciación explosiva de la(s) composición(es) explosiva(s) transportada(s) por su unidad de iniciación, al menos cuando se hayan activado o desactivado los protocolos o sistemas de seguridad, por ejemplo, como se describe en la Publicación de Solicitud de Patente Internacional n.° WO 2022/019841 A1 del documento PCT/SG2021/050432 (“Sistemas, métodos y dispositivos para operaciones de voladura comerciales”), que se incorpora por referencia al presente documento. Una vez codificado o programado, el dispositivo WEB 302 puede cargarse en uno de los barrenos, junto con la carga de la(s) composición(es) explosiva(s) 314 y, posiblemente, de los materiales de contención 316 en el barreno, como parte de un procedimiento de carga del barreno. La carga de la composición explosiva puede ocurrir por medio de una plataforma o vehículo mecanizado, automatizado o autónomo configurado para transportar y dispensar composiciones explosivas en pozos de explosión, por ejemplo, un vehículo convencionalmente denominado Unidad de Fabricación

Móvil (MMU), por ejemplo, basado en un ORICA LTD BM-7 (TM) disponible comercialmente.

Sistema de control de acceso 800

[0114] En al menos algunas implementaciones, el sistema de voladura dual 100 y el sistema de voladura sincronizada 200 pueden incluir un sistema de control de acceso 800 para controlar el acceso a los lanzadores remotos 106 y al sistema de antena 102. En el sistema de control de acceso 800, el controlador central 112 adopta la forma de un controlador central 804 que proporciona una clave de configuración 808 a los lanzadores remotos 106 y al sistema de antena 102. En la descripción del sistema de control de acceso 800 que se presenta a continuación, los lanzadores remotos 106 y el sistema de antena 102 se describen como similares en el sentido de su conexión con el controlador central 804: específicamente, cada uno de los lanzadores remotos 106 y el sistema de antena 102 se denomina "unidad remota 802", que, por lo tanto, puede ser uno de los lanzadores remotos 106 o el sistema de antena 102, ya que los métodos proporcionados por el sistema de control de acceso 800 permiten el control de cada uno de los... Los emisores remotos 106 y el sistema de antena 102 (o cada uno de los sistemas de antena 102, si hay más de uno) son controlados por el controlador central 804. Por lo tanto, en este contexto, los emisores remotos 106 pueden denominarse "emisores remotos EBS" y el sistema de antena 102, o cada uno de ellos, "emisores remotos WEBS", siendo todos ellos "unidades remotas 802".

[0115] A diferencia del controlador 112 configurado para funcionar sin la red de control de acceso 800, el controlador central 804 está configurado para conectarse comunicativamente a tres (3) dispositivos de control de acceso físicos mutuamente diferentes: (i) el dispositivo de protección de voladura 124, (ii) el dispositivo de clave de archivo de voladura; y (iii) un dispositivo de protección de configuración física (que incluye memoria legible por máquina para almacenamiento de datos) en forma de un dispositivo de registro remoto 806 (descrito más adelante), o las unidades remotas 802 por medio de una interfaz de comunicaciones seguras directa (descrita más adelante).

[0116] Como es una forma del controlador 112, el controlador central 804 está configurado para transmitir las instrucciones de comando de explosión (por ejemplo, que representan el

comando de DISPARO, etc. descrito anteriormente) a una unidad remota seleccionada de las unidades remotas 802, o a un grupo seleccionado de las unidades remotas 802 (seleccionadas en función de una ID, por ejemplo, la ID del grupo, la ID de explosión o las ID del dispositivo).

[0117] Cada unidad remota 802 está sustancialmente alejada del controlador central 804, por lo que se encuentra a una distancia espacial significativa del controlador central 804 durante el funcionamiento, donde la distancia espacial significativa puede ser tan cercana como un metro, o hasta varias decenas de kilómetros.

[0118] El controlador central 804 está configurado para conectarse comunicativamente a cada detonador remoto 802 durante la configuración utilizando una interfaz de comunicaciones seguras del controlador central 804 y una interfaz de comunicaciones seguras correspondiente de la unidad remota 802, en algunos casos a través de una interfaz de comunicaciones seguras basada en dispositivo de un dispositivo de registro remoto 806, descrito a continuación.

[0119] En una o más implementaciones, la interfaz de comunicaciones seguras y la correspondiente interfaz de comunicaciones seguras proporcionan una conexión de comunicaciones directa entre el controlador central 804 y cada una de las unidades remotas 802, ya sea individualmente o por turnos (ya que las unidades remotas 802 generalmente se configuran una por una). En una o más implementaciones, la interfaz de comunicaciones seguras y la correspondiente interfaz de comunicaciones seguras pueden incluir una interfaz inalámbrica de comunicaciones de campo cercano (NFC), configurada, por ejemplo, para comunicarse mediante un protocolo de identificación por radiofrecuencia (RFID) o un protocolo de comunicación de campo cercano (NFC). En una o más implementaciones, la interfaz de comunicaciones seguras y la correspondiente interfaz de comunicaciones seguras pueden incluir una interfaz inalámbrica de corto alcance, configurada, por ejemplo, para comunicarse mediante un protocolo Bluetooth, por ejemplo, Bluetooth de baja energía. En una o más implementaciones, la interfaz de comunicaciones seguras y la interfaz de comunicaciones seguras correspondiente pueden incluir una interfaz de comunicaciones cableada para usar con un cable correspondiente (que tiene terminales de conector) y/o un enchufe, por ejemplo, configurado para conectarse comunicativamente usando una interfaz de bus serie universal y un cable USB, por ejemplo, USB 3, o una interfaz de bus de un cable, o una interfaz Secure Digital (SD). En una o más implementaciones, la interfaz de

comunicaciones seguras y la interfaz de comunicaciones seguras correspondiente pueden incluir una interfaz de comunicaciones cableada para su uso con un cable correspondiente (con terminales de conector), por ejemplo, configurada para conectarse mediante una interfaz de Bus Serie Universal y un cable USB, por ejemplo, USB 3. Durante su uso, la unidad remota 802 puede probarse y configurarse en una sala segura (accesible solo para personas autorizadas) con el controlador central 804. Puede haber un "día de puesta en servicio" para cada área de una mina, y las unidades remotas 802 que se pongan en servicio ese día pueden acercarse mucho al controlador central 804, por ejemplo, en contacto con este o conectadas mediante el cable correspondiente (mencionado anteriormente), sin necesidad de un dispositivo de configuración físico individual/único que contenga una clave de configuración 808, como se describe más adelante.

[0120] En una o más implementaciones, la interfaz de comunicaciones seguras del controlador central 804 proporciona una conexión de comunicación directa entre dicho controlador y el dispositivo de registro remoto 806. El dispositivo de registro remoto 806 es un dispositivo físico único que incluye la interfaz de comunicaciones seguras y una memoria legible por máquina para el almacenamiento de datos, que puede describirse como "memoria persistente", por ejemplo, un chip de memoria flash. El dispositivo de registro remoto 806 lee la clave de configuración 808 del controlador central 804, la almacena en la memoria legible por máquina y la escribe en la unidad remota 802 conectada. El dispositivo de registro remoto 806 puede denominarse "dongle" o "dongle de registro remoto", y la clave de configuración 808 puede denominarse "llave de dongle". En estas implementaciones, la interfaz de comunicaciones segura correspondiente de cada unidad remota 802 proporciona una conexión de comunicación directa entre el dispositivo de registro remoto 806 y cada una de las unidades remotas 802 (debido a que las unidades remotas 802 generalmente se configuran individualmente). En estas implementaciones, el controlador central 804 no se conecta directamente a las unidades remotas 802 durante las puestas en servicio, ya que el dispositivo de registro remoto 806 se utiliza para transferir la clave pública generada por el controlador central 804. En estas implementaciones, puede ser conveniente proporcionar solo un dispositivo de registro remoto 806, o solo un número limitado de dispositivos de registro remoto 806 capaces de transferir la clave pública, para mejorar la seguridad de las unidades remotas 802 y, por lo tanto, la seguridad del sitio. En una o más implementaciones, la interfaz de comunicaciones seguras, la

interfaz de comunicaciones seguras basada en dispositivo y la interfaz de comunicaciones seguras correspondiente pueden incluir una interfaz de comunicaciones inalámbricas de campo cercano (NFC), configurada, por ejemplo, para comunicarse mediante un protocolo de identificación por radiofrecuencia (RFID) o un protocolo de comunicación de campo cercano (NFC). Si la interfaz de comunicaciones seguras basada en dispositivo es la interfaz de comunicaciones inalámbricas de campo cercano, el dispositivo de registro remoto 806 puede ser alimentado por la interfaz de comunicaciones inalámbricas de campo cercano para su funcionamiento, y puede estar en forma de tarjeta RFID, tarjeta NFC o tarjeta inteligente. En una o más implementaciones, la interfaz de comunicaciones seguras, la interfaz de comunicaciones seguras basada en dispositivo y la interfaz de comunicaciones seguras correspondiente pueden incluir una interfaz de comunicaciones inalámbricas de corto alcance, configurada, por ejemplo, para comunicarse mediante un protocolo Bluetooth, por ejemplo, Bluetooth de baja energía. En una o más implementaciones, la interfaz de comunicaciones seguras, la interfaz de comunicaciones seguras basada en el dispositivo y la interfaz de comunicaciones seguras correspondiente pueden incluir una interfaz de comunicaciones cableada para su uso con un cable correspondiente (con terminales de conector) o un enchufe, por ejemplo, configurado para conectarse mediante una interfaz de Bus Serie Universal y un cable USB, por ejemplo, USB 3, una interfaz de Bus de un Cable o una interfaz Secure Digital (SD). Si la interfaz de comunicaciones seguras basada en el dispositivo es una interfaz USB, el dispositivo de registro remoto 806 puede denominarse "dongle USB", "unidad USB" o "memoria USB" y puede alimentarse mediante la interfaz USB. El dispositivo de registro remoto 806 es un dispositivo de configuración física con una carcasa que puede ser transportado por una persona, por ejemplo, a mano. Para su funcionamiento, el dispositivo de registro remoto 806 puede alimentarse mediante la interfaz de comunicaciones seguras basada en el dispositivo, como se mencionó anteriormente. Como alternativa, el dispositivo de registro remoto 806 puede contar con una fuente de alimentación interna que alimenta la interfaz de comunicaciones seguras del dispositivo. En algunas implementaciones, el dispositivo de registro remoto 806 es un dispositivo de comunicaciones portátil (p. ej., un teléfono inteligente o celular, o un comunicador personal, p. ej., un iPhone) con memoria legible por máquina y la interfaz de comunicaciones seguras del dispositivo instalada, p. ej., Bluetooth o NFC, como en los teléfonos inteligentes o celulares disponibles comercialmente. El dispositivo de registro remoto 806 puede requerir autenticación personal para operar la interfaz de comunicaciones

seguras del dispositivo, p. ej., un candado biométrico o una combinación de usuario y contraseña, p. ej., una identificación facial o una identificación por huella dactilar. En las implementaciones con la interfaz de comunicaciones cableada, el dispositivo de registro remoto 806 se puede conectar físicamente al controlador central 804, por ejemplo, al puerto 810, para crear la conexión de comunicaciones y recibir la clave de configuración 808. Además, se puede conectar físicamente a cada una de las unidades remotas 802, para, a su vez, crear la conexión de comunicaciones y transmitir la clave de configuración 808 a la unidad remota 802. En uso, tener un dispositivo de configuración físico individual/único para transportar la clave de configuración 808 puede ser más seguro y/o a prueba de errores que permitir conexiones seguras directas entre el controlador central 804 y las unidades remotas 802. En algunas implementaciones, el dispositivo de registro remoto 806 puede incluir varias interfaces de comunicaciones seguras, incluyendo una primera interfaz de comunicaciones seguras correspondiente a la interfaz de comunicaciones seguras del controlador central 804 y una o más segundas interfaces de comunicaciones seguras correspondientes a las interfaces de comunicaciones seguras de las unidades remotas 802, de modo que el controlador central 804 pueda tener... Una interfaz de comunicaciones seguras diferente de una o más unidades remotas 802 permite flexibilidad y retrocompatibilidad entre el controlador central 804 y las unidades remotas 802. Por ejemplo, si el dispositivo de registro remoto 806 es un teléfono inteligente o celular, puede recibir la clave de configuración 808 (y otros datos descritos más adelante) vía USB o Bluetooth (una primera interfaz de comunicaciones seguras basada en el dispositivo) desde el controlador central 804 y, posteriormente, transferir la clave de configuración 808 (y los demás datos) a las unidades remotas 802 vía NFC (una segunda interfaz de comunicaciones seguras basada en el dispositivo). Sin embargo, algunas implementaciones pueden tener solo una interfaz de comunicaciones seguras basada en el dispositivo para fines de prueba y simplificación. Cabe destacar que la(s) interfaz(es) de comunicaciones seguras basada(s) en el dispositivo no limitan los tipos de conexiones de segunda señal 812 que se establecen mediante la clave de configuración 808 y los demás datos: estas conexiones pueden incluir diversas interfaces de comunicación, incluyendo una o más de las siguientes: LAN, 4G/5G, módem de radio y línea telefónica.

[0121] Además de su interfaz de comunicaciones seguras, el controlador central 804 tiene una conexión de red de datos a una red de datos (por ejemplo, una red minera existente como se

describe más adelante) que incluye primeras conexiones de señal 812, mostradas en la FIG. 8, entre el controlador central 804 y cada una de las unidades remotas 802. Las primeras conexiones de señal 812 son, por tanto, conexiones de red de datos para comunicación electrónica como se describe más adelante.

[0122] El sistema de control de acceso incluye el dispositivo de registro remoto 806.

[0123] El controlador central 804 está configurado para proporcionar, mediante generación o acceso aleatorio, un par de claves de cifrado asimétricas pública-privada con una clave pública y una clave privada, y para escribir la clave pública (también denominada en este documento clave de configuración 808) en cada unidad remota 802 cuando se conecta a la interfaz de comunicaciones seguras, ya sea directamente o a través del dispositivo de registro remoto (cuando el dispositivo de registro remoto 806 está conectado comunicativamente al controlador central 804, por ejemplo, en o hacia un puerto 810 del controlador central 804).

[0124] Cada una de las unidades remotas 802 (también denominadas "cajas de voladura remotas" o "máquinas de voladura remotas") tiene una conexión de red de datos a las primeras conexiones de señal 812 de la red de datos. Cada una de las unidades remotas 802 tiene una segunda conexión de señal 814 a al menos un conjunto de iniciadores/detonadores de voladura 816. La segunda conexión de señal 814 puede incluir: (i) una conexión directa desde una unidad remota 802 a sus iniciadores/detonadores de voladura 816; o (ii) una conexión a través de al menos un registrador entre una unidad remota 802 y sus iniciadores/detonadores de voladura 816, por ejemplo, al menos un registrador i-kon™.

[0125] Cada unidad remota 802 está configurada para recibir al menos una instrucción de comando de voladura del controlador central 804 a través de las primeras conexiones de señal 812.

[0126] Las unidades remotas 802 están configuradas para controlar los registradores y/o los iniciadores/detonadores 816 a través de las respectivas segundas conexiones de señal 814.

[0127] Cada unidad remota 802 tiene un puerto 818 configurado para conectar y recibir el dispositivo de registro remoto 806, y para acceder/leer datos en dicho dispositivo, incluyendo específicamente la clave de configuración 808. El dispositivo 806 se comunica con la unidad

remota 802 mediante comunicación electrónica a través del puerto 818. El puerto 818 está configurado para soportar los protocolos de comunicación seguros, que dependen de la implementación, como se describió anteriormente.

[0128] Mientras el dispositivo de registro remoto 806 está conectado comunicativamente a una de la pluralidad de unidades remotas 802, esa unidad remota 802 está configurada para leer la clave de configuración 808 del dispositivo de registro remoto 806, incluso cuando el dispositivo de registro remoto 806 está conectado físicamente a la unidad remota 802 (dependiendo de la implementación).

[0129] Generalmente, el sistema de control de acceso cuenta con un solo controlador central 804, y la interfaz de comunicaciones seguras está configurada de tal manera que la clave de configuración 808 puede transferirse a un dispositivo de registro remoto 806 o a varias unidades remotas 802 en cualquier momento. Generalmente, el dispositivo de registro remoto 806 ("dongle") se conecta a una de las unidades remotas 802 durante la puesta en servicio. El dispositivo de registro remoto 806 ("dongle") puede ser uno de varios dispositivos físicos independientes; por ejemplo, se pueden usar varios dispositivos de registro remoto físicos 806 ("dongles") para configurar varias unidades remotas 802, prácticamente de forma simultánea.

[0130] En lugar de, o además del dispositivo de registro remoto 806, el sistema 800 puede incluir una conexión directa desde el controlador central 804 a cada unidad remota 802 — independiente de las primeras conexiones de señal 812— que puede ser mediante una conexión por cable u otra conexión directa que no almacene la clave de configuración 808 (ni otros datos de configuración) internamente en su memoria legible por máquina. Por lo tanto, la conexión segura directa de la unidad remota 802 al controlador central 804 (por ejemplo, mediante cable o conexión inalámbrica en la sala de control) puede realizar la función del dispositivo de registro remoto 806 ("dongle"). En implementaciones donde el controlador central 804 transfiere la clave de configuración directamente a cada unidad remota 802, la interfaz de comunicaciones seguras puede conectarse a una o más de las interfaces de comunicaciones seguras correspondientes simultáneamente. En algunas implementaciones, se pueden colocar varios emisores remotos 806 (por ejemplo, diez) en una sala segura (por ejemplo, la sala de control) y configurarlos prácticamente de manera simultánea, utilizando las interfaces de comunicaciones seguras (por ejemplo, Bluetooth); Esto puede hacerse al mismo tiempo que

una o más unidades remotas 802 se configuran mediante uno o más de los dispositivos de registro remoto 806 ("dongles"), lo que puede ser relevante si hay una implementación con docenas de unidades remotas 802. Puede ser deseable usar ambas interfaces de comunicaciones seguras simultáneamente en algunas implementaciones, es decir, tanto la interfaz de comunicaciones seguras directas desde el controlador central 804 a cada unidad remota 802 como el al menos un dispositivo de registro remoto 806 ("dongle"), por ejemplo, los dispositivos de registro remoto 806 ("dongles") se pueden usar para evitar la necesidad de ir a la sala de control desde el subsuelo donde se instalan remotamente los detonadors remotos 806 (por ejemplo, para reparaciones, reemplazos y restablecimientos), mientras que la interfaz de comunicaciones seguras directas se puede usar en la sala de control para configurar e instalar nuevos detonadors remotos 806 (por ejemplo, al instalar nuevos controles remotos o poner en servicio nuevos sistemas).

[0131] En implementaciones con el dispositivo de registro remoto 806, puede haber un número limitado de dispositivos de registro remoto 806, p. ej., uno, en el sistema de control de acceso. De esta manera, mientras una de las unidades remotas 802 se comunica con el dispositivo de registro remoto 806 (p. ej., conectada al puerto 818), las demás no lo hacen. Alternativamente, el sistema de control de acceso puede incluir varios dispositivos de registro remoto 806, cada uno con la clave de configuración 808. En este caso, los dispositivos de registro remoto 806 son duplicados, lo que permite registrar varias unidades remotas 802 en paralelo, p. ej., en grandes explotaciones mineras.

[0132] El dispositivo de registro remoto 806 se puede transferir físicamente desde el controlador central 804 (por ejemplo, en superficie) a cada una de las unidades remotas 802 (por ejemplo, subterráneas) mediante un operador humano. El dispositivo de registro remoto 806 solo debe transportarse a cada una de las unidades remotas 802 para su puesta en servicio una vez por cada una. Por ejemplo, esto solo debe ocurrir una vez al conectar por primera vez cada unidad remota 802 al sistema de control de acceso 800. La clave de configuración 808 se almacena en la unidad remota 802 de forma permanente (durante la operación de voladura) y se utiliza en cada nueva sesión de voladura para cifrar una clave de protocolo de enlace 820, que se genera para cada nueva sesión.

[0133] Como se muestra en la FIG. 8, la clave de enlace simétrica cifrada 820 se envía al controlador central 804 en un primer mensaje de enlace 822 (descrito más adelante). Este utiliza su clave asimétrica privada, correspondiente a la clave de configuración 808, para descifrar dicho mensaje y leer, acceder y almacenar la clave 820. Además, envía un segundo mensaje de enlace cifrado 826 ("respuesta de enlace") con una clave de comunicación específica 824 seleccionada para cada unidad remota 802. Todos los demás mensajes de comunicación 830 entre el controlador central 804 y la unidad remota 802 se pueden cifrar con la clave de comunicación específica 824 del detonador remoto. Estos mensajes de comunicación cifrados 830 entre el controlador ORBS 804 y las unidades remotas 802 incluyen los mensajes entre el controlador 112 y el detonador remoto 106, así como los mensajes entre el controlador 112 y el sistema de antena 102, en el método de doble señal. 600 y el método de voladura sincronizada 700, comenzando con los protocolos de comunicación 640A, 704A descritos anteriormente.

[0134] Cada unidad remota 802 está configurada para proporcionar, mediante generación o acceso aleatorio, la clave de protocolo de enlace 820 que es única/casi única para la o cada unidad remota 802, y por lo tanto diferente de las claves de protocolo de enlace 820 de las otras unidades remotas 802 conectadas al controlador central 804. En consecuencia, la clave de protocolo de enlace 820 identifica de forma única cada unidad remota 802 en el sistema de control de acceso 800.

[0135] Cada unidad remota 802 está configurada para cifrar su clave de protocolo de enlace 820 con su clave de configuración recibida 808, y luego enviar la clave de protocolo de enlace cifrada 820 en el primer mensaje de protocolo de enlace cifrado 822 a la unidad controladora central 804 a través de las primeras conexiones de señal 812.

[0136] El controlador central 804 está configurado para recibir el primer mensaje de protocolo de enlace cifrado 822 (con la clave de protocolo de enlace 820) y, en respuesta, descifrarlo utilizando la clave privada, cuya copia se almacena en el controlador central 804, incluso después de retirar el dispositivo de registro remoto 806 del controlador central 804. Tras descifrar el primer mensaje de protocolo de enlace 822, el controlador central 804 está configurado para leer y acceder a la clave de protocolo de enlace 820 del primer mensaje de protocolo de enlace 822 desde cada unidad remota 802.

[0137] El controlador central 804 está configurado para almacenar las claves de protocolo de enlace 820 en un almacén de datos que asocia/identifica las respectivas unidades remotas 802 en los datos del plan de voladuras. Esto permite al controlador central 804 enviar mensajes selectivamente a las unidades remotas 802 seleccionadas utilizando sus respectivas claves de protocolo de enlace 820. En particular, el controlador central 804 está configurado para proporcionar (generar/acceder) una tercera clave de cifrado de datos en forma de clave de comunicación 824 para cada una de las unidades remotas 802, y para cifrar estas claves de comunicación 824 en mensajes cifrados para las unidades remotas 802 en forma de segundos mensajes de protocolo de enlace 826. Cada segundo mensaje de protocolo de enlace 826 contiene la clave de comunicación 824 para una de las unidades remotas 802 seleccionadas. El controlador central 804 está configurado para enviar los segundos mensajes de protocolo de enlace 826 a las respectivas unidades remotas 802 utilizando las primeras conexiones de señal 812.

[0138] Cada unidad remota 802 está configurada para recibir uno de los segundos mensajes de protocolo de enlace 826 y, a continuación, descifrar dicho mensaje utilizando la clave de protocolo de enlace 820 que almacenó/conservó tras enviar el primer mensaje de protocolo de enlace 822. Cada unidad remota 802 está configurada para acceder a su clave de comunicaciones 824 desde el segundo mensaje de protocolo de enlace descifrado 826 y para almacenar/conservar esta clave de comunicaciones 824 para su uso en el cifrado de los mensajes de comunicaciones 830 que se envían al controlador central 804 y en el descifrado de los mensajes de comunicaciones 830 recibidos del controlador central 804. El controlador central 804 está configurado para enviar instrucciones de comando de detonación, por ejemplo, que representan el comando de DISPARO, a cada unidad remota 802 utilizando los mensajes de comunicaciones 830 cifrados por el controlador central 804 para esa unidad remota 802 utilizando la clave de comunicaciones 824 asociada a esa unidad remota 802. La clave de comunicaciones 824, utilizada por cada unidad remota 802 y el controlador central 804, establece así una forma de canal de comunicaciones encriptado entre el controlador central 804 y cada unidad remota respectiva 802 con base en la clave de comunicaciones correspondiente 824. Este uso de encriptación entre el controlador central 804 y cada unidad remota 802 significa que los mensajes, incluyendo mensajes de estado de las unidades remotas 802 y comandos de disparo del controlador central 804, pueden ser seguros, y el acceso al

funcionamiento del sistema de control de acceso 800 puede controlarse de forma segura, por ejemplo, seguro contra manipulación de terceros no autorizados, por ejemplo, escuchas clandestinas, manipulación, suplantación u otras formas de "piratería informática" .

[0139] Además de los mensajes de comunicación 830, cifrados con la clave de comunicación 824, asociada de forma única a una de las unidades remotas 802, y enviados a dicha unidad, el controlador central 804 puede configurarse para generar, cifrar y enviar mensajes de difusión 832, que se envían a todas las unidades remotas 802, por ejemplo, prácticamente de forma simultánea. Ejemplos de mensajes de difusión 832, que son los comandos enviados desde el controlador 804 a todos los expansores remotos 106 y al menos un sistema de antena 102, o a subgrupos seleccionados de estos, incluyen uno o más de los comandos CALIBRAR, COMPROBAR, ARMAR, COMPROBAR DET, SINCRONIZAR Y DISPARAR, y DISPARAR, según la implementación y la explosión. El controlador central 804 puede configurarse para cifrar y enviar el mensaje de difusión 832 con todas las claves de comunicación 824, respectivamente, de modo que todas las unidades remotas 802 puedan descifrar y leer una instancia del mensaje. Alternativamente, el controlador central 804 puede proporcionar (generar/acceder) y almacenar/utilizar una cuarta clave de cifrado de datos en forma de clave de difusión (no mostrada) que puede distribuirse a todas las unidades remotas 802 (al menos a cada unidad remota activa 802). Una vez que todas las unidades remotas activas 802 han recibido la clave de difusión, permite que todas las unidades remotas activas 802 comprendan los mensajes de difusión/multidifusión cifrados 832 (cifrados con la clave de difusión). La clave de difusión se distribuye mediante los mensajes de comunicación 830 o en el segundo mensaje de protocolo de enlace 826, de modo que cada unidad remota 802 puede acceder, leer y almacenar una copia de la clave de difusión, y luego usarla para descifrar el mensaje de difusión 832. En algunas implementaciones, la clave de comunicación 824 es diferente para cada unidad remota 802; por lo tanto, solo la comunicación entre el controlador central 804 y una de las unidades remotas 802 puede cifrarse con ella. Para enviar comunicaciones de difusión/multidifusión entre el controlador central 804 y el grupo seleccionado (incluyendo dos o más, o muchas, o todas) de las unidades remotas 802 a la vez (es decir, prácticamente de forma simultánea), se requiere la clave de difusión, que es conocida, almacenada, accedida y utilizada por todas las unidades remotas 802 conectadas (que forman parte del grupo). La clave de difusión puede ser la segunda clave simétrica generada por el

controlador central 804, después de la clave de comunicaciones 824, que es la primera clave simétrica: en otras palabras, el controlador central 804 puede generar dos conjuntos de claves simétricas mutuamente separadas: un conjunto para las claves de comunicaciones 824 (incluyendo una clave para cada unidad remota activa 802), y otro conjunto para claves de difusión (incluyendo quizás sólo una clave por sesión de voladura o por grupo de iniciadores de explosiones/detonadores 816).

[0140] En resumen, el sistema de control de acceso puede proporcionar y utilizar al menos los primeros tres de los siguientes cuatro conjuntos de claves de cifrado de datos:

a. el par de claves de configuración, que es un par de claves pública/privada (la clave de configuración 808 es la clave pública que es transportada por/en el dispositivo de registro remoto 806 y la clave privada se mantiene segura en el controlador central 804, almacenada en un sistema de archivos de datos seguro del controlador central 804), que es proporcionado por el controlador central 804 (por ejemplo, durante un proceso de configuración, por ejemplo, en respuesta a una entrada/comando del usuario en el controlador central 804), y que cifra el primer mensaje de protocolo de enlace 822;

b. la clave de protocolo de enlace 820, que puede ser una clave simétrica, que se almacena en una memoria de datos de la unidad remota 802, que es proporcionada por la unidad remota 802 (por ejemplo, durante un proceso de registro que incluye registrar la unidad remota 802 en el controlador central 804 como un detonador activo que puede usarse para una o la siguiente secuencia de explosión), que se envía en el primer mensaje de protocolo de enlace 822 desde la unidad remota 802 al controlador central 804 a través de las primeras conexiones de señal 812, y que cifra el segundo mensaje de protocolo de enlace 826 (también denominado "mensaje de respuesta de protocolo de enlace");

c. La clave de comunicaciones 824, que puede ser una clave simétrica, que se almacena en un registro/base de datos (también denominado "gestor de detonador") del controlador central 804 y en la memoria de datos de la unidad remota 802, proporcionada por el controlador central 804 (p. ej., por un servicio

de enrutador del controlador central 804 durante el proceso de registro), que se envía en el segundo mensaje de protocolo de enlace 826 desde el controlador central 804 a la unidad remota 802 a través de las primeras conexiones de señal 812, y que cifra los mensajes de comunicaciones 830 (incluidos los mensajes que no son de difusión/multidifusión); y

d. la clave de difusión, que puede ser una clave simétrica, que se almacena en el registro/base de datos del controlador central 804, y en la memoria de datos de la unidad remota 802, que es proporcionada por el controlador central 804 (por ejemplo, por un servicio de difusión del controlador central 804 durante un proceso de inicio de difusión), que se envía en el segundo mensaje de protocolo de enlace 826 o uno de los mensajes de comunicaciones 830 desde el controlador central 804 a la unidad remota 802 a través de las primeras conexiones de señal 812, y que cifra los mensajes de difusión 832 (incluido cualquier mensaje de difusión/multidifusión).

[0141] En implementaciones de ejemplo, el par de claves de configuración (incluida la clave de configuración compartida 808) puede proporcionar cifrado RSA, la clave de protocolo de enlace 820 puede proporcionar cifrado AES, la clave de comunicaciones 824 puede proporcionar cifrado AES y la clave de difusión puede proporcionar cifrado AES. En otras implementaciones de ejemplo, el par de claves de configuración puede proporcionar cifrado AES u otro cifrado disponible.

[0142] La clave de configuración 808 puede tener una longitud de 8024 bits y puede utilizarse para dos o más explosiones. El par de claves de configuración solo necesita regenerarse selectivamente, por ejemplo, al final del ciclo de vida del sitio. El par de claves de configuración puede generarse mediante una función de la caja de herramientas, por ejemplo, una función de la caja de herramientas de OpenSSL, en el controlador central 804. La clave de configuración 808 puede tener una complejidad considerablemente mayor (en función de la longitud de bits) que la clave de protocolo de enlace 820, la clave de comunicaciones 824 o la clave de difusión: que la clave de comunicaciones 824 y la clave de difusión sean menos complejas que la clave de configuración 808 permite una alta seguridad (ya que la clave de configuración 808 es difícil de piratear) y, al mismo tiempo, un alto rendimiento del sistema

durante las explosiones (ya que el cifrado/descifrado con la clave de comunicaciones 824 y la clave de difusión es más eficiente que con el par de claves de configuración).

[0143] La clave de protocolo de enlace 820 puede generarse mediante una función, por ejemplo, una función OpenSSL, en la unidad remota 802. Esta clave puede ser válida para una sesión de blasting. En implementaciones de ejemplo, puede tener una longitud de 256 bits.

[0144] La clave de comunicaciones 824 puede generarse mediante una función OpenSSL en el controlador central 804. Esta clave puede tener una longitud de 256 bits o ser válida para una sola sesión de comunicación (por lo tanto, puede tener la misma complejidad o duración que la clave de protocolo de enlace 820). Si bien puede tener la misma complejidad o duración que la clave de protocolo de enlace 820, es preferible generarla y usarla para los mensajes de comunicación 830 (en lugar de simplemente reutilizarla), ya que es preferible que la clave de comunicaciones 824 (que se utiliza para la mayor parte de la comunicación cifrada en el sistema de control de acceso 800) la proporcione el controlador central 804 en lugar de las unidades remotas 802, por ejemplo, porque el controlador central 804 ofrece mayor seguridad, supervisión y control que las unidades remotas 802.

[0145] La clave de transmisión puede ser generada por una función OpenSSL en el controlador central 804. La clave de transmisión puede tener 256 bits de longitud y/o puede ser válida para una sesión de transmisión (por lo tanto, la clave de transmisión puede tener la misma complejidad y/o duración que la clave de protocolo de enlace 820 y/o la clave de comunicaciones 824).

[0146] Los mensajes entre el controlador central 804 y cada unidad remota 802 incluyen los mensajes de comunicaciones encriptados 830 y/o los mensajes de difusión 832. Los mensajes entre el controlador central 804 y cada unidad remota 802 también pueden incluir mensajes no encriptados, por ejemplo, mensajes no relacionados con la seguridad, por ejemplo, mensajes que representan solicitudes de intensidad de señal del controlador central 804 y/o que representan respuestas de intensidad de señal de las unidades remotas 802.

[0147] El sistema de control de acceso descrito en este documento permite que las unidades remotas 802 se registren de forma segura y confiable en el controlador central 804, y establezcan comunicaciones seguras (por medio de los mensajes cifrados 830,832) sin la

necesidad de compartir ninguna clave física/dongle cada vez que la unidad remota 802 se enciende para una voladura, o que cada unidad remota 802 tenga un dongle físico transferido desde su ubicación remota a una ubicación segura/central del controlador central 804; una vez que la clave de configuración 808 se ha transferido a cada unidad remota 802 durante la puesta en servicio (en un proceso de puesta en servicio), las unidades remotas 802 y el controlador central 804 comparten las claves públicas y simétricas digitales para una pluralidad de sesiones de voladura en lugar de tener que llevar/transportar un dongle físico para cada sesión de voladura como en los sistemas anteriores. Tras la puesta en servicio, cada unidad remota 802 y el controlador central 804 comparten el par de claves asimétricas de la clave de configuración 808, compuesto por la clave pública (existente en cada unidad remota 802) y la clave privada (ubicada en el controlador central 804). Al encenderse, cada unidad remota 802 proporciona la clave de enlace 820, que se envía, cifrada con la clave de configuración 808, al controlador central 804, que a su vez la descifra mediante la clave privada asimétrica (la clave privada correspondiente a la clave de configuración 808). Tras este descifrado del primer mensaje de enlace 822 para obtener la clave de enlace 820, la clave asimétrica (de la clave de configuración 808) ya no se utiliza para esta sesión de voladura, sino que se utiliza la clave de comunicaciones 824.

[0148] Las ventajas técnicas del sistema de control de acceso descrito aquí incluyen que solo se requiere una llave/dongle física al poner en funcionamiento el sistema de voladura dual 100 o el sistema de voladura sincronizada 200. Una vez registradas las unidades remotas 802 en el controlador central 804, la comunicación sustancial entre el controlador central 804 y las unidades remotas 802 se cifra de forma segura. Por ejemplo, a diferencia del sistema del documento US 6851369, que requiere el transporte físico de una llave/dongle independiente desde cada unidad remota 802, lo que requiere la recolección, el transporte y la conexión por separado de varias llaves/dongles a su controlador central para cada sesión de voladura. A diferencia del sistema del documento US 6851369, el sistema de control de acceso... Lo descrito en este documento puede permitir que hasta muchas, por ejemplo hasta varios miles, de unidades remotas 802 se conecten de forma segura al controlador central 804, y conectar una cantidad tan grande de emisores remotos utilizando tecnología anterior puede haber sido poco práctico o indeseable.

[0149] Para mayor seguridad, el dispositivo de registro remoto 806 solo puede ser creado o escrito por una persona autenticada como administrador del sistema mediante una combinación de nombre de usuario y contraseña proporcionada al controlador central 804 a través de su interfaz de usuario (IU) segura. Específicamente, el controlador central 804 está configurado para permitir la escritura de la clave de configuración 808 únicamente en el dispositivo de registro remoto 806 o directamente en las unidades remotas 802 (según la implementación) tras la autenticación correcta de la combinación de nombre de usuario y contraseña del administrador del sistema en el controlador central 804 a través de su interfaz de usuario (IU) segura.

[0150] Además de la clave de configuración 808, el dispositivo de registro remoto 806 puede incluir información de conexión del sistema que representa un identificador de ubicación de red (ID) del controlador central 804 en la red de datos, que define las primeras conexiones de señal 812. Esta información puede incluir una dirección IP estática o un número de puerto de red del controlador central 804 en la red de datos. Cada unidad remota 802 puede configurarse para leer esta información de conexión del sistema desde el dispositivo de registro remoto 806 y utilizarla para dirigir al menos el primer mensaje de protocolo de enlace 822 y, opcionalmente, los mensajes de comunicación 830 al controlador central 804. Cada unidad remota 802 también puede configurarse para reconocer los mensajes de comunicación 830 o los mensajes de difusión 832 del controlador central 804 basándose en esta información de conexión del sistema.

[0151] Las unidades remotas 802 están configuradas para codificar y enviar sus ID de ubicación de red remota al controlador central 804 en el primer mensaje cifrado de protocolo de enlace 822 o en los mensajes de comunicación 830. El controlador central 804 está configurado para descifrar los respectivos ID de ubicación remota y almacenarlos asociados a los identificadores de las unidades remotas 802, por ejemplo, en el gestor de emisores. Por ejemplo, el ID de ubicación de red remota puede incluir una dirección IP o un número de puerto de red, respectivamente, de cada unidad remota 802 en la red de datos. Las conexiones de red de las unidades remotas 802 definen los extremos remotos de las primeras conexiones de señal 812, y la conexión de red del controlador central 804 define los otros extremos de las primeras conexiones de señal 812. El controlador central 804 utiliza los ID de ubicación remota para dirigir al menos el segundo mensaje de protocolo de enlace 826 ("respuesta de protocolo de

enlace") y, opcionalmente, los mensajes de comunicación 830, a las unidades remotas 802 seleccionadas. Las unidades remotas 802 están configuradas para enviar información adicional sobre sus características al controlador central 804 en el primer mensaje de protocolo de enlace cifrado 822 o en los mensajes de comunicación 830, incluyendo información de interfaz, un ID de detonador de la unidad remota 802, identificación de los registradores conectados a la unidad remota 802, identificación de los iniciadores/detonadores de explosión 816 conectados a la unidad remota 802 y otros datos de registro descritos más adelante. Durante el funcionamiento, los mensajes de comunicaciones 830 pueden transportar lo siguiente desde las unidades remotas 802 al controlador central 804: información del detonador/iniciador, incluidos tiempos de retardo, datos de vibración medidos y/o indicadores de disparo.

[0152] En resumen, los mensajes cifrados generados, transmitidos (a través de las primeras conexiones de señal 812) y utilizados por el sistema de control de acceso incluyen:

a. el primer mensaje de protocolo de enlace 822 (también denominado "comando de protocolo de enlace" o "CMD de protocolo de enlace"), que se transmite desde cada unidad remota 802 al controlador central 804, que está cifrado mediante la clave de configuración 808 (por ejemplo, utilizando cifrado RSA), y que se utiliza para proporcionar contacto/registro inicial de cada unidad remota 802 en el sistema de control de acceso 800, y para proporcionar la clave de protocolo de enlace 820 (una clave simétrica) al controlador central 804 (para su uso en el cifrado del segundo mensaje de protocolo de enlace 826);

b. el segundo mensaje de protocolo de enlace 826 (también denominado "respuesta de protocolo de enlace"), que se transmite desde el controlador central 804 a cada unidad remota 802, que está cifrado mediante la clave de protocolo de enlace 820 (por ejemplo, utilizando cifrado AES), y que se utiliza para enviar la clave de comunicaciones 824 a cada unidad remota 802 (para su uso en el cifrado de los mensajes de comunicaciones 830 al controlador central 804);

c. los mensajes de comunicaciones 830 de cada unidad remota 802 al controlador central 804, que están cifrados por la clave de comunicaciones 824 (por ejemplo, usando cifrado AES), y que pueden incluir un comando register-

detonador que proporciona datos de registro de la unidad remota 802, incluyendo uno o más de: un ID de detonador local único, una contraseña local, un número de serie de detonador, un alias de detonador, información de dirección de interfaz remota de detonador y los ID de ubicaciones de red remotas;

d. los mensajes de comunicaciones 830 del controlador central 804 a cada unidad remota 802, que están cifrados por la clave de comunicaciones 824 (por ejemplo, utilizando cifrado AES), y que pueden incluir: una respuesta de registro-detonador que confirma el registro de cada unidad remota 802 después del procesamiento de un comando de registro-detonador correspondiente (correspondientemente desde cada unidad remota 802), y/o proporciona una identificación de detonador temporal a cada unidad remota 802; y

e. los mensajes de difusión 832 desde el controlador central 804 a cada unidad remota 802, que están cifrados por la clave de difusión (por ejemplo, utilizando cifrado AES), y que pueden incluir comandos de multidifusión o de difusión masiva.

[0153] Como se muestra en la figura 8, el sistema de control de acceso incluye una llave física adicional, además del dispositivo de registro remoto 806, la llave de voladura 124 (también denominada "llave de voladura" o "llave de disparo"). El controlador central 804 está configurado para permitir el envío de las instrucciones de comando de voladura (que representan los comandos de voladura y/o disparo) en los mensajes 830 y 832 únicamente cuando la llave de voladura 124 está físicamente acoplada, o al menos comunicativamente conectada, con el controlador central 804. La llave de voladura 124 es registrada por el controlador central 804. La interfaz de usuario solicita la inserción de la llave de voladura 124, y su registro se realiza en un back-end del controlador central 804, en un servicio de llave. En la mayoría de las operaciones de voladura, solo una llave de voladura 124 es válida por tiempo, y si se registra una nueva llave de voladura 124, las llaves de disparo 834 anteriores se invalidan. Cada dinamitero remoto solo transmitirá códigos de disparo a los iniciadores/detonadores de voladura 816 cuando reciba los comandos y paquetes de datos

correspondientes del controlador central 804, que solo se pueden generar al conectar la llave de voladura 124.

[0154] Como se explicó anteriormente, el controlador central 804 está configurado para:

a. proporcionar (generar o recibir/acceder aleatoriamente) la clave de comunicaciones 824, que puede ser la primera clave de cifrado simétrico, y la clave de difusión, que puede ser la segunda clave de cifrado simétrico;

b. transmitir la clave de comunicaciones 824 a las unidades remotas 802 utilizando un primer canal seguro proporcionado por la clave de protocolo de enlace 820 y las primeras conexiones de señal 812;

c. establecer un segundo canal seguro utilizando la clave de comunicaciones 824 y/o la clave de transmisión (el segundo canal seguro no es igual a la segunda conexión de señal porque el segundo canal de señal se refiere a la comunicación en la primera conexión de señal entre el controlador 804 y las unidades remotas 802); y

d. transmitir comandos/solicitudes (por ejemplo, solicitudes de estado y/o comandos de multidifusión o difusión masiva, por ejemplo, un comando DESARMAR/DESHABILITAR o un comando DISPARAR) a dos o más de las unidades remotas 802 a través del segundo canal seguro.

[0155] Durante el uso, el controlador central 804 proporciona la clave de configuración 808, la clave de comunicación 824 y, opcionalmente, la clave de transmisión. La clave de comunicación 824 puede ser estática, inalterable tras la finalización de una sesión de voladura, o dinámica y aleatoria, generada por el controlador central 804 para cada sesión. La generación dinámica de una nueva clave de comunicación 824, y opcionalmente de una nueva clave de transmisión, puede activarse mediante el registro de una nueva unidad remota 802 en el controlador central 804.

[0156] Durante la puesta en servicio del sistema de voladura dual 100 o del sistema de voladura sincronizada 200 en la obra, cada unidad remota 802 requiere configuración mediante el controlador central 804, que proporciona la clave de configuración 808 (incluida la clave

pública) a cada unidad remota 802. El controlador central 804 cuenta con una interfaz de comunicaciones segura para transmitir la clave de configuración 808: (a) directamente al dispositivo de registro remoto 806 en algunas implementaciones, o (b) directamente a la interfaz de comunicaciones segura correspondiente de cada unidad remota 802 en otras implementaciones. El controlador central 804 genera el par de claves pública-privada para el dispositivo de registro remoto 806 y almacena la clave pública como clave de configuración 808 en el dispositivo físico de registro remoto 806. Un operador humano o un vehículo remoto/autónomo lleva el dispositivo físico de registro remoto 806, único e individual, a cada unidad remota 802 en la obra. Cada unidad remota 802 lee la clave de configuración (clave pública) y la información de conexión (descrita anteriormente) del dispositivo de registro remoto 806. Durante el proceso de registro, cada unidad remota 802 genera la clave simétrica remota única, la clave de protocolo de enlace 820, que corresponde de forma única a la unidad remota 802. Esta clave de protocolo de enlace 820 es cifrada por la unidad remota 802 utilizando la clave de configuración 808 (clave pública) del dispositivo de registro remoto 806. La clave de protocolo de enlace cifrada 820 (clave simétrica) se utiliza posteriormente para el proceso de protocolo de enlace entre la unidad remota 802 y el controlador central 804. El controlador central 804 descifra la clave de protocolo de enlace 820 utiliza su clave privada y utiliza la clave de protocolo de enlace 820 para cifrar su propia clave simétrica en forma de la clave de comunicaciones 824 para una comunicación posterior con la unidad remota 802. La comunicación posterior entre el controlador central 804 y las unidades remotas 802 utiliza la clave de comunicaciones 824 (claves simétricas) para el cifrado.

[0157] La clave de comunicaciones 824 puede almacenarse en el controlador central 804, por ejemplo, en un servicio proporcionado por este (por ejemplo, un servicio Docker™), según el diseño estructural del controlador central 804. Estructuralmente, el controlador central 804 puede incluir un front-end, que incluye una interfaz de usuario web, y un back-end, que incluye varios servicios. Entre los servicios y el front-end se incluyen interfaces de programación de aplicaciones (API) de comunicación. En implementaciones de ejemplo, el controlador central 804 puede incluir un ordenador de placa única, por ejemplo, un ordenador BeagleBone™, y los servicios pueden incluir el servicio de voladuras, el gestor de voladuras, el servicio de adaptador, la interfaz de usuario, el servicio de enrutador, un servicio de proxy o un servicio de LED.

[0158] Las primeras conexiones de señal 812 pueden incluir una o más conexiones de comunicación en serie o en paralelo entre la unidad remota 802 y el controlador central 804, por ejemplo, una red de área local (LAN), una LAN inalámbrica (WLAN, por ejemplo, WiFi), un enlace de comunicaciones LTE, un enlace de comunicaciones por radiofrecuencia (RF), una línea telefónica analógica o una red de alimentación con fugas (por ejemplo, mediante módems RF disponibles comercialmente). Las conexiones de comunicación pueden formar parte de la infraestructura de comunicaciones existente en la mina, por lo que pueden utilizarse para la comunicación con otros equipos in situ, por ejemplo, para comunicaciones de telefonía/datos, al mismo tiempo que se utilizan para las primeras conexiones de señal 812, ya que estas están protegidas por cifrado y, por lo tanto, no son accesibles, legibles ni modificables por ningún otro equipo in situ.

[0159] Las segundas conexiones de señal 814 pueden incluir conexiones cableadas desde la unidad remota 802 a sus registradores y/o iniciadores/detonadores de voladura 816, por ejemplo, mediante un cable o arnés de voladura, o pueden incluir una conexión inalámbrica desde la unidad remota 802 a los iniciadores/detonadores de voladura 816, por ejemplo, mediante señalización de inducción magnética (IM) a través de la tierra (TTE) desde la unidad remota 802 a los iniciadores/detonadores de voladura 816, por ejemplo, como se utiliza en el sistema electrónico inalámbrico de voladura WebGen 200™ de Orica. Las segundas conexiones de señal 814 pueden incluir una conexión por cable de voladura a uno o más registradores, si los hay, y una conexión por arnés de los registradores a los iniciadores/detonadores 816.

[0160] Los iniciadores/detonadores de explosión 816 pueden incluir detonadores o iniciadores electrónicos inalámbricos, por ejemplo, detonadores i-kon de Orica, detonadores eDev (TM) y/o iniciadores WebGen 200 (TM) de Orica.

[0161] El controlador central 804 puede comunicarse con el dispositivo de registro remoto 806, cuando está conectado al puerto 810, utilizando el servicio de dongle, por ejemplo, ejecutándose en un contenedor en el controlador central 804. El controlador central 804 puede incluir servicios adicionales en contenedores respectivos, por ejemplo, servicios de interfaz de usuario (UI), servicios de voladura (para controlar la secuencia de voladura) y servicios de administrador de voladura, como se describió anteriormente **.**

[0162] Las conexiones seguras de primera señal 812 se utilizan para la comunicación bidireccional entre las unidades remotas 802 y el controlador central 804, de modo que este último pueda supervisar el estado de las unidades remotas 802 y, por lo tanto, de los iniciadores conectados, durante una secuencia de programación. El estado puede incluir: activo, sin respuesta, inactivo o con errores.

[0163] El dispositivo de registro remoto 806 incluye una interfaz de comunicaciones seguras, que puede incluir una o más interfaces de bus de un solo cable (One Wire Bus), bus serie universal (USB), Secure Digital (SD), identificación por radiofrecuencia (RFID), Bluetooth (TM) o Bluetooth de baja energía (Bluetooth Low Energy), como se describió anteriormente. Esta interfaz permite la conexión comunicativa a los puertos 810 y 818, integrados con la memoria legible por máquina que proporciona almacenamiento electrónico no volátil, por ejemplo, memoria flash. El dispositivo de registro remoto 806 puede adoptar la forma de una llave USB, una memoria USB o una memoria USB, como se describió anteriormente.

[0164] La unidad remota 802 puede incluir una carcasa impermeable que protege sus componentes electrónicos de la entrada de agua en el sitio, por ejemplo, con una clasificación de protección de entrada (IP) de 54 o superior, o de 67 o superior. Los componentes electrónicos incluyen una fuente de alimentación (por ejemplo, batería interna o conexión de alimentación externa), módulos para comunicaciones cableadas e inalámbricas (por ejemplo, wifi, Bluetooth, Ethernet, chips celulares) a través de la primera conexión de señal, un microprocesador, una memoria legible por máquina que almacena comandos para el microprocesador, un puerto o antena MI para las segundas conexiones de señal 814 y el puerto 818 para la conexión del dispositivo de registro remoto 806 (por ejemplo, una interfaz de soporte de datos físico, que puede incluir un puerto USB, un puerto 1-wire, un puerto de adaptador propietario o una ranura para tarjeta SD).

[0165] El controlador central 804 puede incluir una fuente de alimentación (p. ej., una fuente de alimentación externa), módulos para comunicaciones cableadas e inalámbricas (p. ej., Wi-Fi, Ethernet, chips celulares) a través de la primera conexión de señal, un microprocesador, una memoria legible por máquina que almacena comandos para el microprocesador (incluyendo un sistema operativo y una interfaz de usuario), y el puerto 810 para la conexión del dispositivo de registro remoto 806 (p. ej., una interfaz física de soporte de datos, que puede incluir un

puerto USB, un puerto 1-wire, un puerto para llave electrónica propietaria o una ranura para tarjeta SD). El controlador central 804 incluye el puerto para la llave electrónica de voladura 124 (p. ej., una interfaz física de soporte de datos, que puede incluir un puerto USB, un puerto 1-wire, un puerto para llave electrónica propietaria o una ranura para tarjeta SD).

[0166] Los comandos de voladura incluyen los comandos de ACTIVACIÓN, DISPARO y DESARMACIÓN. El comando de ACTIVACIÓN es el mismo para todos los iniciadores/detonadores de voladura 816; además, no incluye la información de retardo, que es programada previamente por los registradores/explotadores. Cada uno de los iniciadores/detonadores de voladura 816 tiene un ID de dispositivo que el registrador/escáner lee durante la preparación de la voladura. El ID de dispositivo está asociado con el tiempo de retardo. Durante la voladura, cada uno de los iniciadores/detonadores de voladura 816 se programa con su tiempo de retardo asignado, direccionado por el ID de dispositivo, desde un plan de voladura. Tras programar secuencialmente cada uno de los iniciadores/detonadores de voladura 816, la voladura se activa (mediante el envío de un comando de ACTIVACIÓN) y luego se dispara (mediante el envío de un comando de DISPARO). Los comandos de ACTIVACIÓN y DISPARO son comandos de difusión en los mensajes de difusión 832 a todos los iniciadores/detonadores de voladura 816 que participan en la voladura.

[0167] Como se muestra en la FIG. 9, el sistema de control de acceso 800 está configurado para realizar un método 900, que incluye:

a. el controlador central 804 que genera el par de claves de configuración y la clave de comunicaciones 824 para cada sesión de voladura (902);

b. el controlador central 804 escribe la clave de configuración 808 (y la información de conexión del sistema) en el dispositivo de registro remoto 806 mientras está conectado comunicativamente al puerto 810 (904)—o en otras implementaciones, escribe la clave de configuración 808 directamente desde el controlador central 804 a cada una de las unidades remotas 802 individualmente o por turno mediante las conexiones de comunicaciones seguras descritas anteriormente;

c. el dispositivo de registro remoto 806 se transporta físicamente y, por lo tanto, transporta la clave de configuración 808 a cada unidad remota 802 (906) o, en otras implementaciones, cada una de las unidades remotas 802 recibe la clave de configuración 808 directamente desde el controlador central 804 en lugar de hacerlo a través del dispositivo de registro remoto 806;

d. cada unidad remota 802 que genera la clave de protocolo de enlace 820 en el proceso de registro (908);

e. cada unidad remota 802 lee la clave de configuración 808 (y la información de conexión del sistema) desde el dispositivo de registro remoto 806 mientras está conectado comunicativamente al puerto 818 (910);

f. cada unidad remota 802 codifica la clave de protocolo de enlace 820 utilizando la clave de configuración 808 para generar el primer mensaje de protocolo de enlace 822 (912);

g. cada unidad remota 802 envía el primer mensaje de protocolo de enlace 822 al controlador central 804 a través de las primeras conexiones de señal 812 (914);

h. el controlador central 804 descifra el primer mensaje de protocolo de enlace 822 utilizando la clave de configuración 808 para acceder a la clave de protocolo de enlace 820 (916);

i. el controlador central 804 cifra la clave de comunicaciones 824 utilizando la clave de protocolo de enlace 820 para generar el segundo mensaje de protocolo de enlace 826 (también denominado “respuesta de protocolo de enlace”) (918);

j. el controlador central 804 envía el segundo mensaje de protocolo de enlace 826 a cada unidad remota 802 a través de las primeras conexiones de señal 812 (920);

k. cada unidad remota 802 recibe y descifra el segundo mensaje de protocolo de enlace 826 utilizando la clave de protocolo de enlace 820 para acceder a la clave de comunicaciones 824 (922);

l. cada unidad remota 802 encripta información para el controlador central 804 utilizando la clave de comunicaciones 824 y enviando estos mensajes de comunicaciones 830 al controlador central 804 a través de las primeras conexiones de señal 812 (924);

m. el controlador central 804 recibe y descifra los mensajes de comunicaciones 830 de cada unidad remota 802 utilizando la clave de comunicaciones 824 para acceder a la información de cada unidad remota 802 (926);

n. el controlador central 804 cifra información para cada unidad remota 802 utilizando la clave de comunicaciones 824 y enviando estos mensajes de comunicaciones 830 a cada unidad remota 802 a través de las primeras conexiones de señal 812 (928);

o. cada unidad remota 802 recibe y descifra los mensajes de comunicaciones 830 del controlador central 804 utilizando la clave de comunicaciones 824 para acceder a la información del controlador central 804 (930);

p. el controlador central 804 cifra la información de difusión para la pluralidad de unidades remotas 802 utilizando la clave de difusión y enviando estos mensajes de comunicaciones 830 a la pluralidad de unidades remotas 802 a través de las primeras conexiones de señal 812 (932); y

q. la pluralidad de unidades remotas 802 que reciben y descifran los mensajes de difusión 832 desde el controlador central 804 utilizando la clave de difusión para acceder a la información de difusión desde el controlador central 804 (934).

Interpretación

[0168] El término “antena” utilizado en este documento se refiere a una antena, es decir, un transductor configurado para convertir entre ondas electromagnéticas y voltajes/corrientes eléctricas correspondientes.

[0169] El término "iniciación" se refiere a la iniciación o desencadenamiento de una combustión, una deflagración, una transición de deflagración a detonación (DDT) o una detonación en un material o sustancia con una composición explosiva, y la formación asociada de diferentes especies químicas, o al inicio de reacciones químicas que resultan en la combustión y la formación asociada de diferentes especies químicas en el material o sustancia. El término "iniciación explosiva" se refiere a la iniciación que da lugar a una explosión o detonación, cuya ocurrencia corresponde o se define por al menos una liberación rápida de energía, un aumento de volumen, un aumento de temperatura y la producción o liberación de gas, así como la generación de al menos una onda de choque subsónica. El término "detonación" se refiere a la generación de una onda de detonación supersónica o un frente de choque en un material o sustancia explosivos, de una manera comprensible para los expertos en la materia.

[0170] El término "operación de voladura comercial" incluye la iniciación o detonación de materiales o sustancias explosivas dispuestas en medios físicos, por ejemplo, una formación geológica, mediante dispositivos de iniciación como parte de operaciones de minería, canteras, construcción civil/demolición, exploración sísmica u otras operaciones de voladura no militares. Dicha iniciación o detonación provoca la explosión, por ejemplo, de fracturas o levantamientos, del medio físico en el que se realiza la operación de voladura comercial. Dicha iniciación o detonación puede denominarse voladura, de una manera fácilmente comprensible para las personas con conocimientos básicos en la técnica pertinente. El medio físico en el que se realiza la operación de voladura comercial se encuentra en un entorno de voladura comercial, como un entorno minero, por ejemplo, una mina a cielo abierto o subterránea.

[0171] Como se usa en este documento, el término "conjunto" corresponde a o se define como una organización finita no vacía de elementos que exhibe matemáticamente una cardinalidad de al menos 1 (es decir, un conjunto como se define en este documento puede corresponder a una unidad, singlete o conjunto de un solo elemento, o un conjunto de elementos múltiples), de acuerdo con definiciones matemáticas conocidas (por ejemplo, de una manera correspondiente a la descrita en An Introduction to Mathematical Reasoning: Numbers, Sets, and Functions, "Capítulo 11: Propiedades de los conjuntos finitos" (por ejemplo, como se indica en la pág. 140), por Peter J. Eccles, Cambridge University Press (1998)). Por lo tanto, un conjunto incluye al menos un elemento. En general, un elemento de un conjunto puede

incluir o ser una o más porciones de un sistema, un aparato, un dispositivo, una estructura, un objeto, un proceso, un procedimiento, un parámetro físico o un valor dependiendo del tipo de conjunto en consideración.

[0172] Las figuras adjuntas muestran aspectos de realizaciones representativas no limitativas de acuerdo con la presente divulgación, y es posible que los elementos estructurales particulares mostrados en las figuras no se muestren a escala o con precisión entre sí. La representación de un elemento dado, la consideración o el uso de un número de elemento particular en una figura específica, o una referencia al mismo en el material descriptivo correspondiente, puede abarcar el mismo elemento, un elemento equivalente, análogo, categóricamente análogo o similar, o un número de elemento identificado en otra figura o material descriptivo asociado a la misma. La presencia de "/" en una figura o texto del presente documento se entiende como "y/o", a menos que se indique lo contrario; es decir, "A/B" se entiende como "A" o "B" o "A y B". Se entiende que la mención de un valor numérico o rango de valores en particular en este documento incluye o es una mención de un valor numérico o rango de valores aproximado, por ejemplo, dentro de +/- 20%, +/- 15%, +/- 10%, +/- 5%, +/- 2,5%, +/- 2%, +/- 1%, +/- 0,5% o +/- 0%. El término "esencialmente todo" o "sustancialmente" puede indicar un porcentaje mayor o igual al 50%, 60%, 70%, 80% o 90%, por ejemplo, 92,5%, 95%, 97,5%, 99% o 100%.

[0173] Muchas modificaciones serán evidentes para los expertos en la materia sin apartarse del alcance de la presente invención. La referencia a una o más realizaciones en este documento, por ejemplo, como varias realizaciones, muchas realizaciones, varias realizaciones, múltiples realizaciones, algunas realizaciones, ciertas realizaciones, realizaciones particulares, realizaciones específicas o varias realizaciones, no implica necesariamente todas las realizaciones.

[0174] A lo largo de esta especificación y las reivindicaciones que siguen, a menos que el contexto requiera lo contrario, la palabra "comprender", y variaciones tales como "comprende" y "que comprende", se entenderán como que implican la inclusión de un entero o paso o grupo de enteros o pasos indicados, pero no la exclusión de cualquier otro entero o paso o grupo de enteros o pasos.

[0175] El proceso de cifrado descrito en este documento también puede denominarse “codificación” y, correspondientemente, el proceso de descifrado descrito en este documento también puede denominarse “decodificación”.