Manual de servicio técnico e instalación.
Central de alarmas
ATENEA G4

Seguridad IP

Invescon Technologies

ÍNDICE

1. INTRODUCCION

La Central de Alarmas Atenea G4 es la nueva generación de centrales de alarma de Invescon Technologies, con la que además de ofrecerle la doble vía de comunicación TCP/IP y GPRS supervisada de forma constante, podemos ofrecerle nuevas características. Dispone de 9 zonas ampliables a 181 (160 Detectores) e integra de forma completa tanto la funcionalidad de los teclados ICPA, como la de los expansores ICP2E-G4.

Permite actuar sobre el sistema de seguridad tanto por medio de teclados (ICPA) y llaves electrónicas, como mediante mensajes SMS y software de telegestión.

La programación y configuración de la central de alarmas Atenea G4, se realiza mediante el software de configuración ProgG4.

En este manual se explica todo lo necesario para la instalación de la Central, léalo detenidamente y consérvelo para posteriores consultas.

1.1. CARACTERÍSTICAS DEL SISTEMA

- Central de Alarmas con transmisión y control mediante protocolo TCP/IP.
- Polling constante con CRA a intervalos de 10 s.
- Respaldo GPRS, manteniendo toda la funcionalidad de la central a través de él.
- Hasta 21 ETDs o periféricos (0 a 20, ETD 0 = central Atenea G4) controlados por un bus RS485. Y de los cuales, hasta un máximo de 8 pueden ser del tipo teclado ICPA.
- Capacidad para controlar hasta 181 zonas (160 Detectores).
- Dispone de 8 zonas analógicas en placa para la conexión de hasta 8 detectores de seguridad con todos los parámetros que estos puedan generar y una zona digital para el tamper tanto de apertura como de desprendimiento.
- Hasta 32 salidas de relé (a elegir entre las 3 salidas en placa y las salidas proporcionadas por los periféricos ICP2E-G4 e ICPA).

- Hasta 32 códigos de usuario que permiten realizar maniobras de armado/desarmado sobre el sistema de seguridad.
- Hasta 32 llaves electrónicas numeradas.
- Hasta 5 particiones.
- Capacidad para almacenar hasta 1000 eventos.
- Identificación y registro de la ejecución de maniobras por distintas vías.
- Hasta 96 acciones diferentes de tipo ON, OFF ó temporizadas.
- Hasta 12 macros formadas cada una de ellas por hasta 8 acciones.
- Interacción por apps para smartphones y SMS con el cliente.
- Transmisión de eventos por SMS o E-mail.
- Posibilidad de transmitir eventos a una CRA principal y dos ECOS más.
- Posibilidad de descarga de forma remota del listado completo de eventos.
- Orden de reconexión con CRA desde bidireccionalidad.
- Reinicio del sistema de forma remota.
- Comprobación del estado del sistema desde bidireccionalidad.
- Comprobación del estado de todas las zonas en tiempo real.
- Posibilidad de conocer y modificar el estado de todas las particiones del sistema (armadas/desarmadas).
- Software para la ejecución de los mantenimientos de forma remota.

Este producto está certificado con el mayor grado de seguridad según el estándar EN50131-3 (Grado 4), pero el uso de algunas de sus funciones puede hacer que este se reduzca (Ver anexo 10.1).

IMPORTANTE: En caso del uso o configuración de alguna de las funciones que reduzcan el grado de seguridad en el que ha sido certificado el equipo, será necesario adaptar el etiquetado usando el juego de adhesivos facilitado.

2. INSTRUCCIONES DE INSTALACION

2.1. INSTRUCCIONES DE SEGURIDAD IMPORTANTES

NORMAS DE SEGURIDAD ELECTRICA

- No debe trabajar una persona sola en situaciones que presenten peligro
- Una corriente alta de cortocircuitos en materiales conductivos puede producir quemaduras graves.
- Es necesario que la instalación del cableado eléctrico del equipo se lleve a cabo por un electricista o personal cualificado para ello.
- Compruebe que los cables de suministro eléctrico y los enchufes estén en buenas condiciones.
- No utilice ningún tipo de componentes metálicos sin desconectar el equipo antes.

BATERÍAS.

- Las baterías deben ser recicladas. Deje la batería en un depósito de recogida selectiva o entregarla al proveedor en el embalaje original de las baterías.
- No arroje las baterías echándolas al fuego ya que pueden explotar.
- No abra o cierre las baterías, contienen un electrolito que es tóxico y dañino para la piel y los ojos.
- A fin de evitar daños personales causados por corrientes peligrosas evite llevar relojes de pulsera y joyas tales como anillos cuando reemplace las baterías.
- Utilice herramientas con el aislamiento adecuado.
- Reemplace las baterías con el mismo número y tipo de baterías instaladas en el equipo.
- Consulte a su distribuidor para obtener información acerca de la sustitución de las baterías y el reciclaje de las mismas.
- Es necesario sujetar las baterías a la caja con dos tiras de cinta adhesiva doble cara al fondo de la misma.

El siguiente símbolo se puede encontrar en el interior de los equipos:

Advertencia: Riesgo de descarga eléctrica. Antes de manipular las conexiones eléctricas, asegúrese de que la alimentación principal del equipo está apagada.

2.2. PRECAUCIÓNES PARA LA INSTALACIÓN

Como cualquier aparato electrónico, este sistema puede funcionar de forma errática o dañarse cuando está sujeto a una alta descarga eléctrica. Sin embargo, el daño puede ser reducido mediante la conexión de la apropiada conexión a tierra del sistema.

No apriete los tornillos más de la cuenta. Este sistema contiene componentes sensibles a la estática .Asegúrese de haber descargado la electricidad estática de su cuerpo antes de manipular los paneles de circuitos.

Siga las instrucciones de los manuales de instalación, uso y programación. Estas instrucciones se deben seguir para evitar daños en el panel de control y el equipo asociado.

2.3. INSTALACIÓN

IMPORTANTE: La central Atenea G4 y las ETD´s o expansores ICP2E-G4 se deben instalar dentro de las zonas supervisadas por el sistema.

La central Atenea G4 y todos los equipos asociados, al igual que cualquier otro equipo electrónico, pueden deteriorarse debido a condiciones ambientales extremas. Por lo tanto, el lugar elegido para la instalación debe estar limpio, seco y no estar sometido a altos niveles de vibración y choque.

MONTAJE EN LA PARED.

Atenea G4 o ICP2E-G4: Coloque la caja en la pared en el lugar deseado (Asegúrese de que la pared es lisa). Marque las ubicaciones de los tornillos superiores (véase el anexo 10.7) y asegúrese de que hay por lo menos un espacio de 50 mm entre la pared y la parte inferior de la caja. Este espacio es necesario para que la tapa se pueda abrir.

Introducir los tornillos en las posiciones marcadas e instalar temporalmente el cuadro en la pared. Asegúrese de que la altura es correcta. Marque la ubicación de la parte inferior del tornillo y el perno de la pared para el tamper por retirada del equipo. Retire la caja, haga los agujeros, coloque el perno y fije firmemente la carcasa con tres tornillos. La elección de los tornillos para la fijación debe hacerse en función del tipo de superficie sobre la que se esté haciendo el montaje.

Ajuste la altura del micro interruptor micro para que este permanezca cerrado al entrar en contacto con el perno.

Teclado ICPA: Coloque el teclado en la pared en el lugar deseado (Asegúrese de que la pared es lisa). Marque las ubicaciones de los tornillos superiores (véase el anexo 10.8) y asegúrese de que hay por lo menos un espacio de 100 mm entre la pared y la parte inferior del teclado, y la pared y ambos laterales del teclado. Este espacio es necesario para abrir la tapa y tener acceso a los tres tornillos.

Introducir los tornillos en las posiciones marcadas e instalar temporalmente el teclado en la pared. Asegúrese de que la altura es la correcta (1,5 m aproximadamente). Marque la ubicación de los tornillos inferiores y el tornillo para el tamper por retirada del equipo. Retire el teclado, haga los agujeros, coloque el tornillo para el tamper por retirada y fije firmemente la carcasa con cuatro tornillos. La elección de los tornillos

para la fijación debe hacerse en función del tipo de superficie sobre la que se esté haciendo el montaje.

CABLEADO

Los cables han de introducirse en la caja a través de los orificios habilitados para ello en la parte posterior y los extremos deben tener la longitud suficiente para poder conectarlos a los terminales. Los cables deben estar protegidos y cumplir con las normativas locales sobre conexiones.

Es de vital importancia que el cable utilizado sea de buena calidad y que la instalación se realice correctamente. En general en la instalación del cableado se deben cumplir con los siguientes requisitos:

- El cable de comunicaciones debe ser blindado para proteger el sistema frente a las interferencias de radio frecuencia.
- El cable de alimentación del teclado ICPA debe estar blindado y la pantalla se debe conectar al terminal negativo de la fuente de alimentación.
- La instalación eléctrica debe cumplir con el reglamento técnico de baja tensión (UNE -EN 20460)
- Se facilitará un dispositivo de desconexión externo al equipo y de fácil acceso, con una separación de contacto de al menos 3,0 mm.
- Las entradas y salidas en placa, que se utilizan para conectar dispositivos cableados al panel de control Atenea G4 y el expansor ICP2E-G4, deberán estar conectados a circuitos que operan a la tensión SELV.
- Los cables deben fijarse cerca de los terminales para evitar que entren en contacto con las partes activas del circuito de alimentación.
- El extremo del conductor trenzado no será consolidado por soldadura blanda en los lugares donde el conductor se somete a la presión de contacto.
- El tipo de cable utilizado debe ser distinto para el cable de alimentación y para las conexiones SELV.

3. CENTRAL ATENEA G4

3.1 ESPECIFICACIONES TECNICAS ATENEA G4

- 9 Zonas en placa (8 analógicas y una digital) ampliables hasta un máximo de 181 mediante expansores (160 detectores).
- 3 Salidas en placa (2 Relés y 1 en colector abierto) ampliable hasta 32 mediante expansores.
- 1 Salida en placa (colector abierto) para la indicación de fallo del microprocesador.
- Fuente de alimentación integrada tipo A
- Alimentación 230VAC / 16 -15%/+10%
- Frecuencia 50/60 Hz
- Corriente
  - 50mA en espera (Max 145 mA) a 230 V
  - 200mA a 12 Vdc
- Rizado máximo: 520mV a 230V
- Salida de batería 13,6 Vdc a 25˚C (Batería 12 V 9 Ah ó 12 V 7 Ah)
- Salida de alimentación auxiliar 13,5Vdc ±15%. La máxima corriente de salida depende de la batería usada.
  - 30 mA para la batería de 7 AH.
  - 100 mA para la batería de 9 Ah.
- 1 Puerto de comunicaciones RS-845 reservado para la comunicación con los teclados y las ETD´s o expansores de entradas y salidas. Las comunicaciones RS485 están cifradas mediante algoritmo AES de128 bits.
- 1 Puerto de comunicaciones RS-232 reservado para GPRS/GSM mod MC55iw.
- 2 Puertos serie TTL.
- 1 Conector RJ45 para la comunicación Ethernet.
- Según norma EN50131-3 el sistema tiene dos opciones de notificación: C o D.
- Dimensiones (Al x An x Pr): 32,5 x 30 x 8,5 cm
- Peso (Sin incluir batería): 3,4 Kg
- Compatibilidad electromagnética: EN 301489-1 v1.9.2, EN 301489-7 v1.3.1
- Grado 4 (EN50131-3 / EN50131-6)
- Clase ambiental Clase II (-10ºC +40ºC)

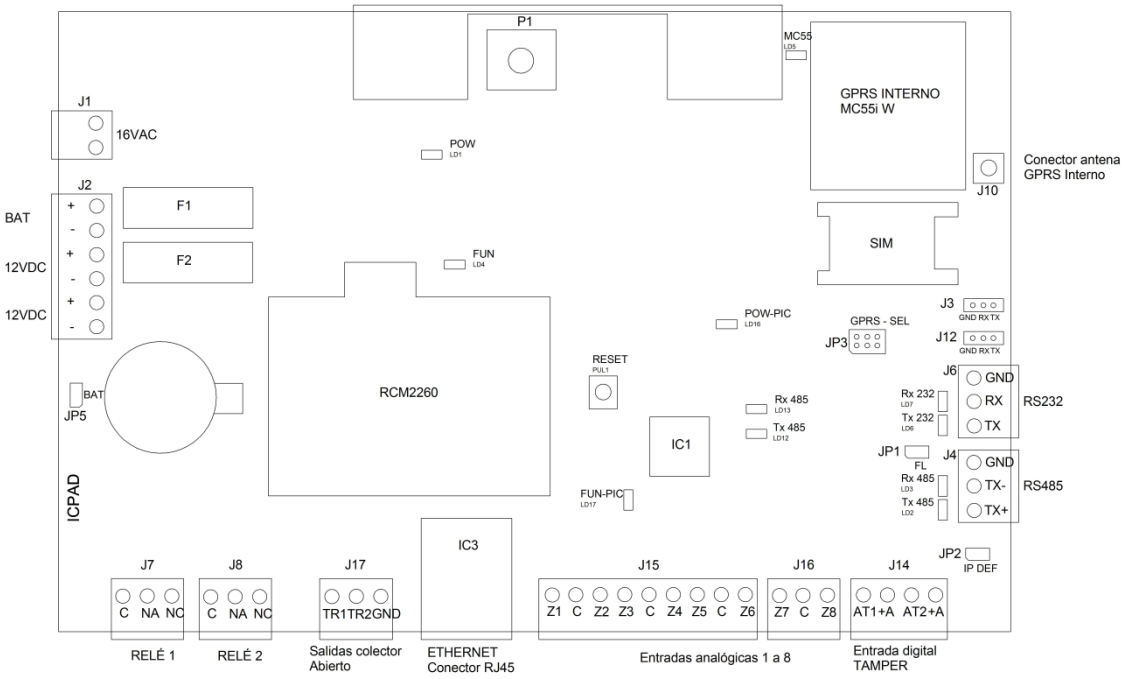
La central de alarmas Atenea G4 cumple con los estándares EN 50136-1:2012 EN 50136-2:2013 y EN 50131-10:2014 en sus comunicaciones, incluyendo en placa y de forma nativa la posibilidad de realizarlas por Ethernet y/o GPRS.

En función de los medios de transmisión y de la configuración del tiempo de polling que tenga, la podemos clasificar de la siguiente manera:

ATP Principal	ATP Alternativo	Tiempo de polling	Categoría
Ethernet	-	10 segundos	SP6
GPRS	-	10 segundos	SP6
Ethernet	GPRS	10 segundos	DP4
Ethernet	-	30 segundos	SP5
GPRS	-	30 segundos	SP5
Ethernet	GPRS	30 segundos	DP4
Ethernet	-	60 segundos	SP4
GPRS	-	60 segundos	SP4
Ethernet	GPRS	60 segundos	DP3
Ethernet	-	120 segundos	SP4
GPRS	-	120 segundos	SP4
Ethernet	GPRS	120 segundos	DP3

Cuando la central de alarmas Atenea G4 utiliza doble sistema de transmisión gestiona ambos medios de forma balanceada manteniendo toda su potencia, control y funcionalidad en todos ellos independientemente del medio activo y del tiempo de polling programado.

3.2 CONEXIONADO CENTRAL ATENEA G4



3.3 ENTRADAS CENTRAL ATENEA G4

ZONAS:

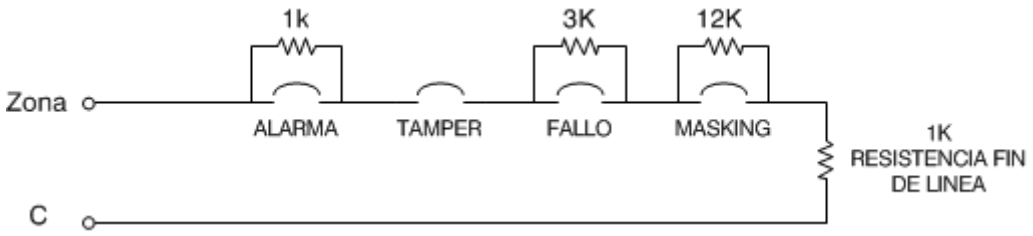
La central de alarmas Atenea G4 tiene 8 zonas analógicas supervisadas por resistencias, de forma que en cada una de ellas se puede conectar un detector y disponer de todos los parámetros de alarma que es capaz de generar (Alarma, Tamper, Masking y Fallo sensor).

De todos los parámetros asociados a una zona, tan solo el primero (Alarma) es configurable mediante el software de programación ProgG4 para indicar de qué tipo de alarma se trata (Interior, Perimetral, CO2,…). El resto son fijos.

IMPORTANTE: El uso de los parámetros técnicos, tales como gas, incendio, inundación, etc., no están cubiertos por la norma, aunque se permite su uso y este no anula la certificación mientras no interfieran en ninguna de las otras funciones del sistema. Puede encontrar una lista de todos estos parámetros en el anexo 10.2

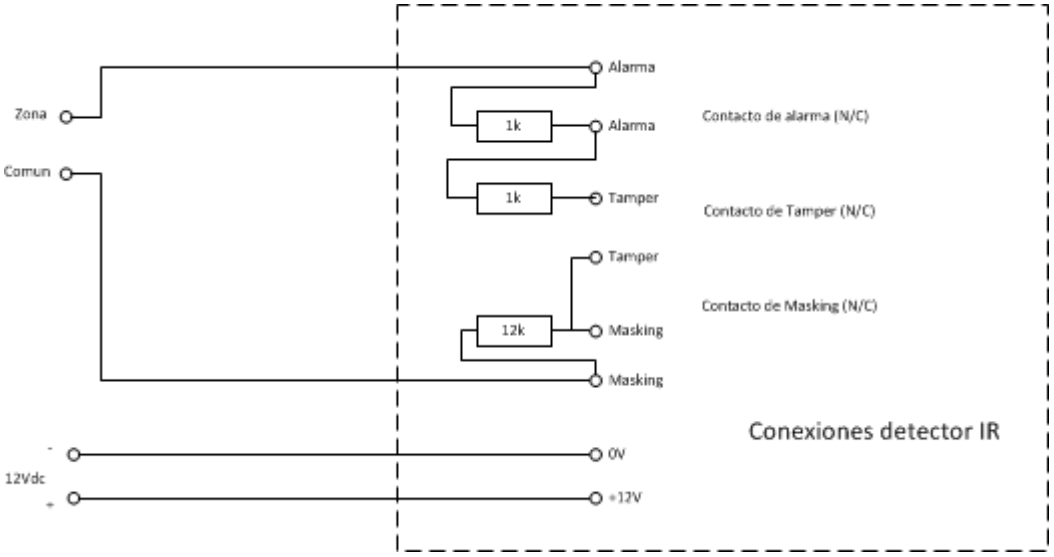
Además de estos parámetros, por cada zona la central podrá reportar cortocircuito.

En la siguiente figura se muestra como sería el cableado de una zona:



IMPORTANTE: La tolerancia de las resistencias utilizadas siempre ha de ser de 1%.

Ejemplo de conexionado de un detector:



TAMPER:

La central de alarmas Atenea G4 tiene una zona digital entre los terminales "AT1" y "+A". Esta zona está configurada de forma predeterminada como 24 Hr Tamper y se usa para vigilar las 2 detecciones de tamper de la caja de la central (apertura y desmontaje de pared).

16VAC:

En esta entrada se conectan los terminales del secundario del transformador, para dar tensión a la placa. Junto con la central de alarmas se facilita ya un transformador. La conexión del primario del transformador está protegida por un fusible de 160mA. (Fusible: T160mA L, 250 V).

Esta entrada esta supervisada e indicará un fallo de la fuente de alimentación si el valor de la tensión en ella es menor que 11,4 Vac y está protegida contra sobretensiones con una tensión de disparo de 17Vac.

BATERÍA:

La central tiene dos contactos identificados como BAT, para conectar una batería recargable de 12VDC 9Ah o de 12Vdc 7Ah. La conexión de batería está protegida frente a posibles cortocircuitos por el fusible F1 de 3,15A. (Fusible F1: T3,15A L,250V).

Además esta salida está provista de un dispositivo (Resistencia NTC) para garantizar que durante la carga en flotación, las características de carga están dentro de las especificaciones del fabricante de la batería para la clase ambiental II (Regulación del voltaje de salida para la carga de la batería basado en las temperaturas, 13,6 Vcc a 25 ° C). La resistencia NTC debe de ser fijada con cinta adhesiva a la batería para un correcto funcionamiento.

Hasta que no se le proporciona tensión a la central, los terminales de batería están aislados y no tienen tensión. De igual forma, aunque conectáramos una batería en ellos, la central tampoco funcionaría.

En caso de querer hacer funcionar en un momento determinado la central tan solo con batería, sería necesario además de conectar una batería en los contactos, poner el puente JP5 BAT.

IMPORTANE: Durante el funcionamiento normal de la central es necesario que el JP5 no este puesto.

En caso de fallo de la alimentación principal, la batería proporcionará la tensión necesaria para el funcionamiento de la central Atenea G4. En este caso, la tensión suministrada por la batería es supervisada y si ésta es inferior a 11,5 Vcc el sistema reportará fallo de la fuente de alimentación auxiliar.

También posee una protección contra la descarga profunda de la batería, entrando en operación esta función cuando la tensión de la batería cae por debajo de 8,5 Vcc.

NOTA: El sistema tiene una pila de botón modelo CR2032 para mantener la fecha y hora del equipo en caso de pérdida de tensión. Se recomienda sustituirla cada 4 años.

ETHERNET:

La central dispone de un conector RJ45 para poder conectarla a la red o a un PC directamente. En caso de quererse conectar directamente con ella mediante un PC, será necesario hacerlo con un cable cruzado.

3.4 SALIDAS CENTRAL ATENEA G4

12 VOLTIOS:

La central de alarmas Atenea G4 proporciona una salida de 13,5Vdc +-15% para la alimentación de los equipos. Esta está protegida por un fusible reseteable de 600mA. (F3 MF-R040) y con un fusible de 1A (Fusible F2: T1A L, 250 V).

La corriente máxima de la salida de alimentación auxiliar depende de la batería utilizada:

- 30 mA de la batería 7 Ah
- 100mA para la batería 9Ah

Nota: El máximo rizado de la tensión pico a pico en esta salida es 640mVpk a 253VAC y 480mVpk a 195Vac.

RELÉS:

La central de alarmas Atenea G4 dispone de 2 salidas de relé y 2 salidas de colector abierto. Los dos relés y un colector abierto son configurables por software ProgG4.

IMPORTANTE: Algunas configuraciones pueden hacer que el grado de certificación se vea reducido (véase el anexo 10.1).

La otra salida de colector abierto indica el fallo de micro procesador y no es programable. Esta salida se activará de forma automática si el sistema no funciona correctamente durante más de 40 segundos. (Además, si un fallo de microprocesador está presente en el teclado se muestra el mensaje "ICPA Versión XX".)

En caso de utilizar un GSM/GPRS externo, el relé 2 se utilizará para su control, y no podrá ser configurado para otro uso.

Los relés pueden ser configurados como relés de “Auto test” mediante el software ProgG4. Estos se utilizan para iniciar de forma remota el auto test de los detectores en caso de que estos dispongan de esta funcionalidad. De esta forma podremos comenzar de manera automática un test de cada uno de los detectores, sirenas o cualquier tipo de dispositivo conectados a ellos (La conexión depende del tipo de dispositivo a testear.)

IMPORTANTE:

- *El uso del módulo GSM / GPRS externo no se incluye en la certificación Grado 4.*
- Los relés solo pueden operar con la tensión SELV del circuito.

RS485:

El puerto RS485 se utiliza para comunicación de la central con el resto de periféricos y detectores con conexión a bus. La topología de este ha de ser la de un Bus 485 a dos hilos estándar y su longitud nunca podrá superar los 1000 metros.

Las comunicaciones en el Bus RS485 están cifradas mediante AES de 128 bits para garantizar la sustitución o pérdida de señales/mensajes.

IMPORTANTE: Es necesaria la instalación de un ferrita de impedancia Z 119Ω o 89Ω a 10 Mhz en bus tal y como se explica en el anexo 10.10. Ver también el anexo 10.4.

RS232:

Este puerto es utilizado para la comunicación con el GSM/GPRS externo y el cable de conexión nunca podrá superar los 12 metros de longitud.

IMPORTANTE: El uso del módulo GSM / GPRS externo no se incluye en la certificación Grado 4.

PUERTOS TTL:

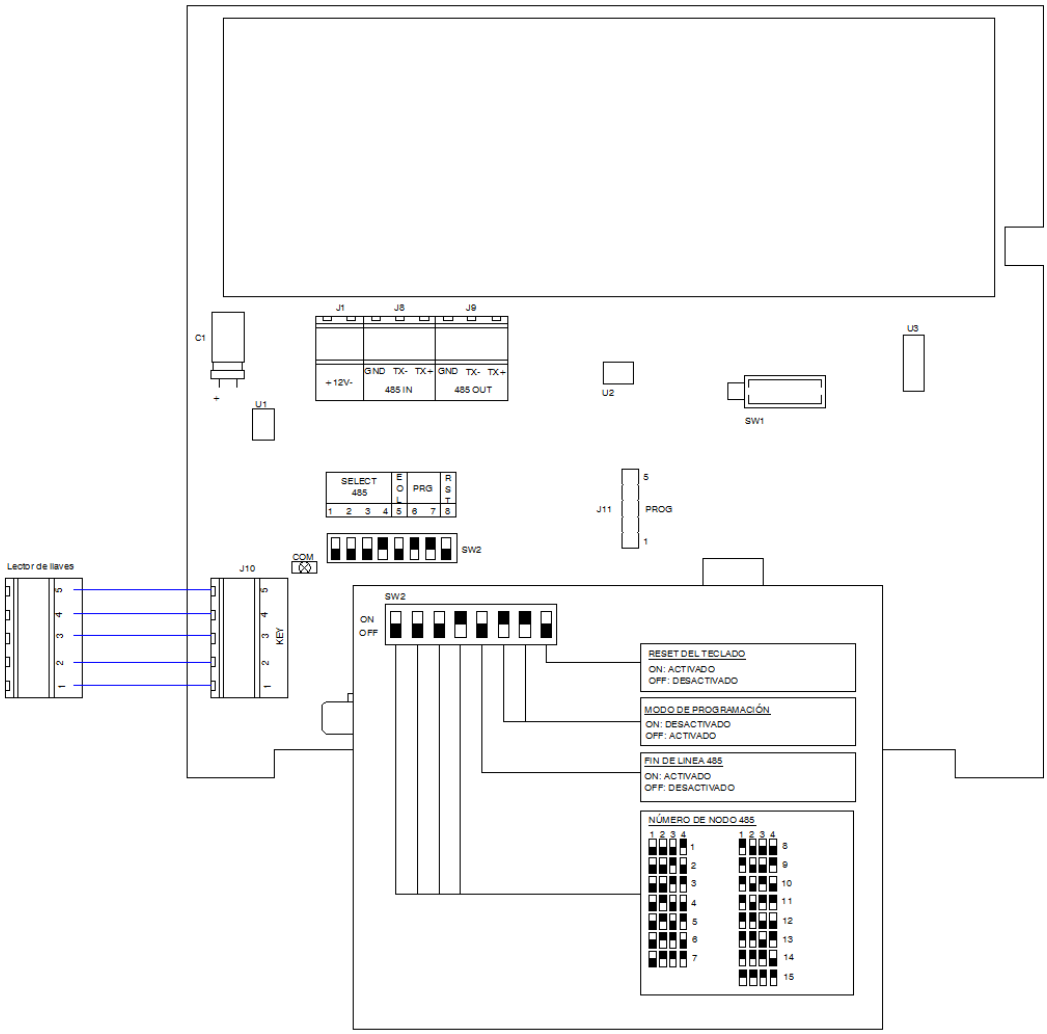
Dispone de dos puertos TTL para usos futuros.

4 TECLADO ICPA

4.1 ESPECIFICACIONES TECNICAS ICPA

- Pantalla oled de 2 líneas de 16 caracteres alfanuméricos cada una.
- 21 teclas con retroiluminación.
- Tamper de carcasa y pared.
- Zumbador interno.
- Led indicador de alimentación y comunicaciones.
- Conexión RS485 para conexión por bus. Las comunicaciones RS-845 están cifradas mediante AES de 128 bits
- Teclas de acceso rápido a funciones.
- Conexión para lectores de llaves.
- Tensión de funcionamiento 12Vcc ±15%
- Corriente: 70mA en espera (Máx. 190mA)
- Dimensiones (Al x An x Pr): 142 x 128 x 31 mm
- Peso: 310 gr
- Grado 4 (EN50131-3 y EN50131.6)
- Clase ambiental II (-10°C - +40°C)

4.2 CONEXIONADO ICPA



4.3 ENTRADAS/SALIDAS TECLADO ICPA

12V:

En esta entrada se conectan los 12Vdc para la alimentación del teclado.

RS485:

El puerto RS485 se utiliza para comunicación con la central. La topología de este ha de ser la de un Bus 485 a dos hilos estándar y su longitud nunca podrá superar los 1000 metros.

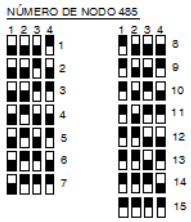
Las comunicaciones en el Bus RS485 están cifradas mediante AES de 128 bits para garantizar la sustitución o pérdida de señales/mensajes.

En caso de ser el último periférico del bus es necesario poner una resistencia final de línea a este. Para ello será necesario poner el DIP 5 (EOL) del SW1 a ON.

IMPORTANE: Este puente DIP solo ha de estar a ON en caso de que el teclado sea final de bus.

Para la asignación de un número de nodo al teclado hemos de utilizar los contactos DIP 1 a 4 del interruptor SW2. En este hemos de marcar su número en binario siendo el 4 el de menor peso (2^0) y 1 el de mayor (2^3).

Ejemplo:



LECTOR DE LLAVES:

Son 5 terminales numerados del 1 al 5, donde se conectan los lectores de llaves.

TAMPER:

El teclado dispone de un micro interruptor integrado que sirve para la detección de la apertura o la retirada de montaje. Esta zona está configurada de forma predeterminada como 24 Hr Tamper, y aparece automáticamente en la programación del ProgG4 una vez se agrega un teclado al sistema.

ZUMBADOR:

El teclado dispone de un zumbador integrado que hace las veces de sirena. Está configurado de forma predeterminada como un relé sirena, y aparece automáticamente en la programación del ProgG4 una vez se agrega un teclado al sistema.

IMPORTANTE: Algunas configuraciones pueden hacer que el grado de certificación se vea reducido (véase el anexo 10.1).

5 LECTOR DE LLAVES ICQB

El lector de llaves ICQB es el accesorio necesario para el uso de llaves electrónicas ICQ2A con la central Atenea G4. Este lector se conecta a un teclado ICPA.

5.1 ICQB ESPECIFICACIONES TÉCNICAS

- Conexión para Teclados ICPA.
- Dimensiones (alto x ancho x profundidad): 60 x 57 x 27 mm
- Peso: 120 gr
- ACE tipo A, grado 4 (EN50131-3)
- Clase ambiental II (-10°C - +40°C)

5.2 ICQB ENTRADAS / SALIDAS

LECTOR DE LLAVE:

5 terminales numerados del 1 al 5 para conectar a un teclado ICPA.

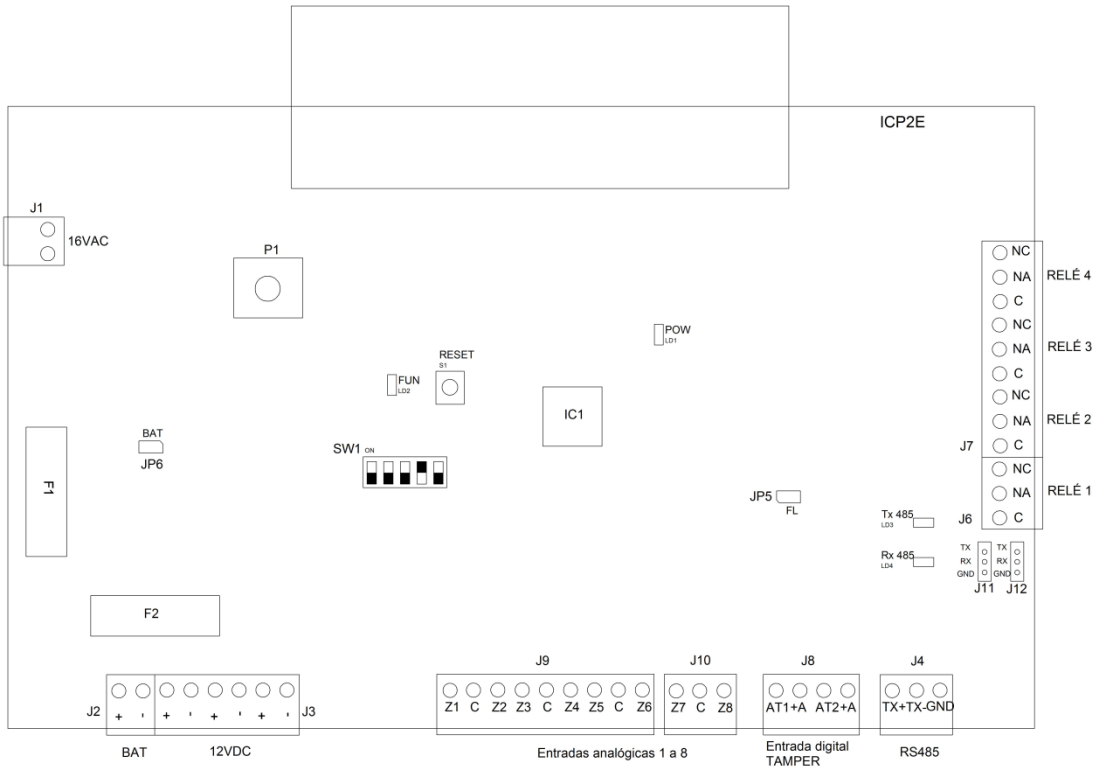
Nota: La conexión del lector de llaves a un teclado ICPA se puede encontrar en el apartado 4.2 (Conexionado ICPA) de este manual.

6 EXPANSOR ICP2E-G4

6.1 ESPECIFICACIONES TECNICAS ICP2E-G4

- 9 Zonas en placa (8 analógicas y una digital)
- 4 Salidas de relé en placa
- Fuente de alimentación integrada tipo A
- Alimentación 230VAC -15%/+10%
- Frecuencia 50/60Hz
- Corriente:
  - 40mA (Max 145mA) a 230 Vac.
  - 70 mA a 12Vdc.
- Rizado máximo: 500mV a 230V
- Salida de batería de 13,6Vdc a 25˚C (Batería 12V 9Ah o 12V 7Ah.)
- Salida de alimentación auxiliar 13,6Vdc ±15%. La máxima salida de corriente depende de la batería utilizada.
  - 160 mA para batería de 7Ah
  - 230 mA para batería de 9Ah
- 1 Puerto de comunicaciones RS-845 reservado para la comunicación con los teclados y las ETD´s o expansores de entradas y salidas. Las comunicaciones RS485 están cifradas mediante algoritmo AES de128 bits.
- 2 puertos serie TTL.
- Dimensiones (Al x An x Pr): 32,5 x 30 x8,5 cm
- Peso (Sin incluir batería): 3,4 Kg
- ACE tipo B, Grado 4 (EN50131-3 / EN50131-6)
- Clase ambiental Clase II (-10ºC +40ºC)

6.2 CONEXIONADO ICP2E-G4



6.3 ENTRADAS EXPANSOR ICP2E-G4

ZONAS:

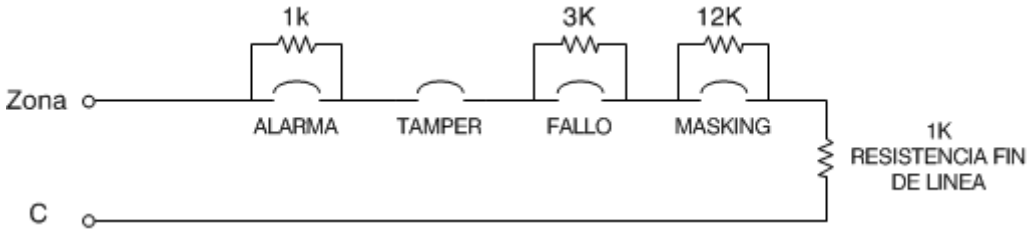
El expansor ICP2E-G4 al igual que la central de alarmas Atenea G4 tiene 8 zonas analógicas supervisadas por resistencias, de forma que en cada una de ellas se puede conectar un detector y disponer de todos los parámetros de alarma que es capaz de generar (Alarma, Tamper, Masking y Fallo sensor).

De todos los parámetros asociados a una zona, tan solo el primero (Alarma) es configurable mediante el software de programación ProgG4 para indicar de qué tipo de alarma se trata (interior, perimetral, CO2,…). El resto son fijos.

IMPORTANTE: El uso de los parámetros técnicos, tales como gas, incendio, inundación, etc., no están cubiertos por la norma, aunque se permite su uso y este no anula la certificación mientras no interfieran en ninguna de las otras funciones del sistema. Puede encontrar una lista de todos estos parámetros en el anexo 10.2

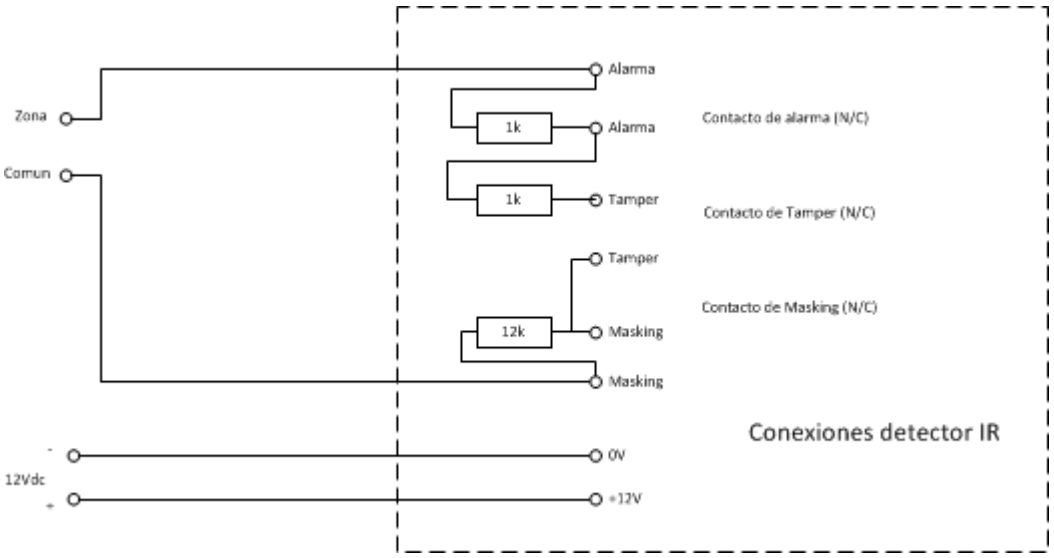
Además de estos parámetros, por cada zona la central podrá reportar cortocircuito.

En la siguiente figura se muestra como sería el cableado de una zona:



IMPORTANTE: La tolerancia de las resistencias utilizadas siempre ha de ser de 1%.

Ejemplo de conexionado de un detector:



TAMPER:

Tiene una zona digital entre los terminales “AT1” y “+A”. Esta zona esta configurada de forma predeterminada como 24 Hr Tamper y se usa para vigilar las 2 detecciones de tamper de la caja del expansor (apertura y desmontaje de pared).

16VAC:

En esta entrada se conectan los terminales del secundario del transformador, para dar tensión a la placa. Junto con al expansor se facilita ya un transformador. . La conexión del primario del transformador está protegida por un fusible de 160mA. (Fusible: T160mA L, 250 V).

Esta entrada esta supervisada e indicará un fallo de la fuente de alimentación si el valor de la tensión en ella es menor que 11,4 Vac y está protegida contra sobretensiones con una tensión de disparo de 17Vac.

BATERÍA:

El expansor tiene dos contactos identificados como BAT, para conectar una batería recargable de 12VDC 9Ah o de 12Vdc 7Ah. La conexión de batería está protegida frente a posibles cortocircuitos por el fusible F1 de 3,15A. (Fusible F1: T3,15A L,250V).

Además esta salida está provista de un dispositivo (Resistencia NTC) para garantizar que durante la carga en flotación, las características de carga están dentro de las especificaciones del fabricante de la batería para la clase ambiental II (Regulación del voltaje de salida para la carga de la batería basado en las temperaturas, 13,6 Vcc a 25 ° C). La resistencia NTC debe de ser fijada con cinta adhesiva a la batería para un correcto funcionamiento.

Hasta que no se le proporciona tensión a la central, los terminales de batería están aislados y no tienen tensión. De igual forma, aunque conectáramos una batería en ellos, la central tampoco funcionaría.

En caso de querer hacer funcionar en un momento determinado la central tan solo con batería, sería necesario además de conectar una batería en los contactos, poner el puente JP5 BAT.

IMPORTANE: Durante el funcionamiento normal de la central es necesario que el JP5 no este puesto.

En caso de fallo de la alimentación principal, la batería proporcionará la tensión necesaria para el funcionamiento de la central Atenea G4. En este caso, la tensión suministrada por la batería es supervisada y si ésta es inferior a 11,5 Vcc el sistema reportará fallo de la fuente de alimentación auxiliar.

También posee una protección contra la descarga profunda de la batería, entrando en operación esta función cuando la tensión de la batería cae por debajo de 8,7 Vcc.

6.4 SALIDAS EXPANSOR ICP2E-G4

12 VOLTIOS:

El expansor de zonas ICP2E-G4 proporciona una salida de 13,5Vdc ±15% para alimentación de los equipos. Esta está protegida por un fusible reseteable de 600mA. (F3 MF-R040) y con un fusible de 1A (Fusible F2: T1A L, 250 V).

La corriente máxima de la salida de alimentación auxiliar depende de la batería utilizada:

- 160 mA de la batería 7 Ah
- 230 mA para la batería 9Ah

Nota: El máximo rizado de la tensión pico a pico en esta salida es 640mVpk a 253VAC y 480mVpk a 195Vac.

RELÉS:

El expansor dispone de 4 Salidas de relé libres de tensión. Todas ellas son configurables mediante el software ProgG4.

Los relés pueden ser configurados como relés de “Auto test” mediante el software ProgG4. Estos se utilizan para iniciar de forma remota el auto test de los detectores en caso de que estos dispongan de esta funcionalidad. De esta forma podremos comenzar de manera automática un test de cada uno de los detectores, sirenas o cualquier tipo de dispositivo conectados a ellos (La conexión depende del tipo de dispositivo a testear.)

IMPORTANTE:

- *Algunas configuraciones pueden hacer que el grado de certificación se vea reducido (véase el anexo 10.1).*
- Los relés solo pueden operar con la tensión SELV del circuito.

RS485:

El puerto RS485 se utiliza para la comunicación con la central y detectores con conexión a bus. La topología de este ha de ser la de un Bus 485 a dos hilos estándar y su longitud nunca podrá superar los 1000 metros.

Las comunicaciones en el Bus RS485 están cifradas mediante AES de 128 bits para garantizar la sustitución o pérdida de señales/mensajes.

IMPORTANTE: Es necesaria la instalación de un ferrita de impedancia Z 119Ω o 89Ω a 10 Mhz en bus tal y como se explica en el anexo 10.10. Ver también el anexo 10.4.

En caso de ser el último periférico del bus es necesario poner una resistencia final de línea a éste. Para ello será necesario poner el puente JP5 FL.

IMPORTANE: Este puente JP5 solo ha de estar puesto en aquel periférico que sea final de bus.

Para la asignación de un número de nodo al expansor ICP2E-G4 hemos de utilizar los contactos DIP 1 a 5 del interruptor SW1. En este hemos de marcar su número en binario siendo el 5 el de menor peso (2^0) y 1 el de mayor (2^4).

PUERTOS TTL:

Dispone de dos puertos TTL para usos futuros.

7 FUNCIONALIDAD

7.1 ETDs

La Central de Alarmas Atenea G4 integra los expansores ICP2E-G4 y los teclados ICPA.

El número máximo de ETDs es 21 (0 a 20, La ETD=0 es la central Atenea G4), de los cuales hasta un máximo de 8 pueden ser teclados.

La comunicación entre la central de Alarmas y estos periféricos se realiza mediante el bus RS-485.

Las comunicaciones en el Bus RS485 están cifradas mediante AES de 128 bits para garantizar la sustitución o pérdida de señales/mensajes.

La central de alarmas se comunica con cada expansor o teclado programado de forma independiente y secuencial. Para comodidad del usuario se permite indicar su actividad, es decir, si se tiene en cuenta la comunicación con ella, sus zonas y salidas o no.

El máximo timeout será de 55 milisegundos para cada respuesta. Se establece una penalización de 1 minuto para cada expansor o teclado que exceda el timeout de espera de tres intentos, además de remitirse su avería a la CRA. Al finalizar ese minuto se volverá a preguntar de nuevo al expansor o teclado penalizado.

El teclado que no tenga comunicación mostrará en su display el mensaje "ICPA Versión XX" y el resto de teclados mostrarán el mensaje “HAY ALERTAS”. La alerta mostrada será “FALLO COM CON ETDS, COM 485”[1].

[1] Este aviso se mostrará tanto si el fallo de comunicación es de un teclado ICPA como si lo es de un expansor ICP2E-G4.

7.2 PARTICIONES

La Central de Alarmas es capaz de trabajar con 5 particiones distintas.

Es posible configurar una acción o macro para los eventos parciales de armado y/o desarmado.

El armado de la última partición desarmada desencadenará un armado total pero la acción que se ejecuta es la asociada a la maniobra parcial (igualmente para el desarmado).

Para cada partición se pueden definir un subconjunto de zonas. Pueden existir zonas comunes a varias particiones. En el caso de tener configuradas zonas comunes a varias particiones, estas no serán vigiladas hasta que todas las particiones a las que pertenezcan estén armadas.

Desde cualquier teclado se puede actuar sobre ellas y para mayor comodidad se pueden asociar particiones[2] a cada uno de ellos para que al Armar/Desarmar sin indicar partición, se actúe sobre las asociadas[3].

Además se puede tener conectado en cada teclado un lector de llaves y al igual que para los teclados también se pueden asociar particiones a cada uno de ellos para que al introducir una llave se Armen/Desarmen las particiones asociadas.

7.3 ZONAS

La central de alarmas es capaz de controlar hasta 181 zonas compuestas por:

- 8 zonas analógicas y una digital en la propia central.

2 Si se asignan todas las particiones significará una maniobra TOTAL.
3 Si se asocia más de una partición, la maniobra a realizar será la contraria al estado actual si todas tienen el mismo estado o DESARMADO si se tienen distintos estados.

- Zonas de los periféricos ICP2E-G4 e ICPA.

La central interpreta alarma de zona a intervalos configurables de 2 a 10 minutos, es decir, una vez ha habido una alarma en una zona, nuevas alarmas ocurridas sobre esta misma zona no se tendrán en cuenta hasta pasado el intervalo de tiempo configurable (Tiempo refresco alarmas), no obstante, desde las opciones de Monitor de zonas o Listado de zonas del Menú de Usuario es posible visualizar el estado en tiempo real de cada una de ellas. La central de alarmas no reporta a la CRA Restauración de alarma de ninguna de sus zonas.

Para cada zona es posible configurar los siguientes puntos:

- *Activa:* la central de alarmas tendrá en cuenta las zonas que estén activas, las demás serán ignoradas, es decir, no formarán parte de su mapa lógico y no se vigilarán. Si se desactiva el expansor o teclado, las zonas que le pertenecen se desactivarán de forma automática.
- *Tipo de Zona:* se puede indicar si una zona es Primaria o Secundaria.
- *Parámetro:* parámetro configurable a registrar y reportar ante su alarma.
- *En Ruta*: la central esperará los tiempos de entrada/salida hasta reportar alarma de dicha zona.

  En caso de tener zonas en ruta (temporizadas), se habrá definido un Tiempo de Salida que será el mismo para todas ellas. Es posible configurar hasta 5 rutas de entrada distintas y cada una de ellas tendrá un Tiempo de Entrada asociado y una zona de inicio de ruta asociada.

  El Tiempo de Salida es aquel que se da tras el armado para poder salir sin originar alarmas en aquellas zonas que estén temporizadas. Durante este tiempo no se permitirá realizar ninguna maniobra sobre el sistema hasta que este haya concluido.

  Una vez acabado el tiempo de salida, si cualquiera de las zonas temporizadas permanece en alarma, la maniobra de armado no se efectuará, se informará a la central receptora con el parámetro "Fallo en Armado" y para avisar de esta circunstancia sonarán todas las sirenas de la instalación durante 10 segundos.

De igual manera, si durante el Tiempo de Salida se activará cualquiera de las zonas no temporizadas, la maniobra de armado tampoco se llevará acabo, se informará a la central receptora con el parámetro "Fallo en Armado" y sonaran todas las sirenas de la instalación durante 10 segundos.

El Tiempo de Entrada es el que se inicia al darse una alarma en la zona temporizada definida como zona de Inicio de ruta, para dar la oportunidad de Desarmar la partición o la central. Durante el tiempo de entrada ninguna de las zonas temporizadas originarán alarmas hasta que éste haya finalizado.

En caso de que la primera alarma se origine en una zona temporizada pero que no fuera zona de inicio de ruta, esta zona se comportará como instantánea, dando alarma de forma inmediata.

En caso de que el Tiempo de Entrada marcado finalice sin haber realizado la maniobra de desarmado o de que en el transcurso del Tiempo de Entrada se detectara una alarma en una zona no temporizada o de ruta, el sistema registrara la alarma y activaran todas las acciones asociadas a este evento, pero no reportará la alarma a la CRA hasta que los dispositivos de aviso (Sirenas, flashes, etc…) hayan funcionado durante 30 segundos. Si en el transcurso de estos 30 segundos el sistema fuera desarmado, la señal no se reportara a la CRA.

Si el aviso acústico está activado, éste sonará durante el Tiempo de Entrada en todos aquellos teclados en los que se haya configurado y durante el Tiempo de Salida en el teclado desde el que se hizo la maniobra.

- *Timbre:* ante la apertura de zonas de este tipo y siempre y cuando el estado de la Central de alarmas o de la partición a la que pertenezca sea Desarmado, los teclados de la instalación emitirán un aviso acústico[4].
- *Texto descriptivo:* es el texto que se muestra en caso de alarma y en el que describimos al detector o ubicación.

4 Este aviso no estará ligado a ninguna temporización interna (interpretación de zonas a intervalos de 5 minutos), es decir, el timbre sonará en función del estado en tiempo real de la zona.

- *Permiso SMS:* ante su apertura, estando la partición/particiones armadas, la central enviará un mensaje SMS como máximo a 3 de los 8 números de teléfono autorizados.
- *Permiso E-mail:* ante su apertura, estando la partición/particiones armadas, la central enviará un correo electrónico como máximo a 3 de las 8 direcciones de correo autorizadas.
- *Acción/Macro asociada:* acción o macro que se ejecutará ante la alarma de dicha zona.

  Si una zona pertenece a varias particiones sólo se pondrá en vigilancia cuando TODAS las particiones a las que pertenece estén armadas. Y si es temporizada, evidentemente, solo comenzará a correr el tiempo de salida cuando se ponga en vigilancia.

7.4 SALIDAS

La Central de alarmas dispone de 32 salidas de relé como máximo. 3 salidas en la propia central (2 de relé y 1 de colector abierto) y el resto en los expansores de tipo ICP2E-G4 e ICPA.

Cada una de ellas puede estar programadas como sirenas o no, o si son "auto-test" o no, de forma independiente.

Todas las salidas definidas como sirenas se apagan desde la opción “Sirenas” del menú de usuario, o si se realiza una maniobra parcial o total de desarmado.

Todas las salidas establecidas como "auto-test" se encienden durante 10 segundos a partir de la opción "Autotest Detectores" en el menú de servicio técnico.

Las acciones que se pueden realizar sobre las salidas son ON, OFF y temporización de 2 a 476 segundos (Aprox. 8 minutos) y para una mayor versatilidad se permite definir un retardo para el comienzo de la acción.

7.5 CODIGOS DE USUARIOS

La central de alarmas permite crear 32 códigos de usuario de 6 dígitos para realizar maniobras de armado/desarmado sobre el sistema de seguridad y de 2 códigos especiales también de 6 dígitos para las situaciones de Coacción y Pánico. El uso o no de estos dos códigos es configurable.

Los códigos de usuario, además, permiten navegar por los menús informativos mediante los teclados alfanuméricos ICPA.

IMPORTANTE: De los 32 códigos que se definen, por defecto tan solo el primero (número 1) se utiliza como el código maestro o código de nivel 3. Ver el anexo 10.9.

A continuación se muestra un resumen del uso de códigos de usuario en los teclados ICPA, así como otras acciones posibles.

Código de usuario: CCCCCC

Descripción	Entrada de códigos
Menú de Alertas	A + CCCCCC + ENTER
Menú de Usuario	B + CCCCCC + ENTER
Menú de Mensajes	A + ENTER
Armado/Desarmado[5], Pánico o Coacción[6]	CCCCCC + ENTER
Armado/Desarmado parcial	CCCCCC + 1..5 + ENTER
Desarmado Total (si existen particiones)[7]	CCCCCC + 7 + ENTER

5 Bien del estado general o de ciertas particiones si el código o el teclado tienen una o varias particiones asignadas.
6 Ante el código de coacción la Central desarma el sistema y transmite el evento de coacción. Ante el de Pánico sólo se transmite el evento.
7 Para esta opción el código sí que debe tener permiso en TODAS las particiones, si no, la maniobra no se realizará.

Descripción	Entrada de códigos
Armado Total (si existen particiones)	CCCCCC + 9 + ENTER
Pánico Rápido	B + 6 (simultáneamente)
Des/Bloqueo del Teclado	CONTROL + ENTER (simultáneamente)
Ejecución de Acciones	CONTROL + NN+ ENTER
Ejecución de Macros	B + NN + ENTER

Para cada código se debe indicar las particiones sobre las que tiene permiso para actuar.

Se pueden asignar permisos de uso de código en cada teclado ICPA, de tal forma que para cada teclado solo serán admitidos como válidos aquellos códigos registrados en la tabla general y con permiso en el mismo.

Además, es posible asignar particiones[8] a cada código, de manera, que cada vez que se introduzcan los 6 dígitos numéricos seguidos de la tecla ENTER, se armen o desarmen dichas particiones[9] sin necesidad de introducir un dígito a mayores o de realizar varias maniobras si se quiere actuar sobre varias, aunque tendrán prioridad las particiones asignadas al teclado si las tuviera.

Evidentemente, si se asigna una o varias particiones a un código, para que éste pueda realizar maniobras de armado/desarmado sobre las mismas deberá tener permiso en ellas[10].

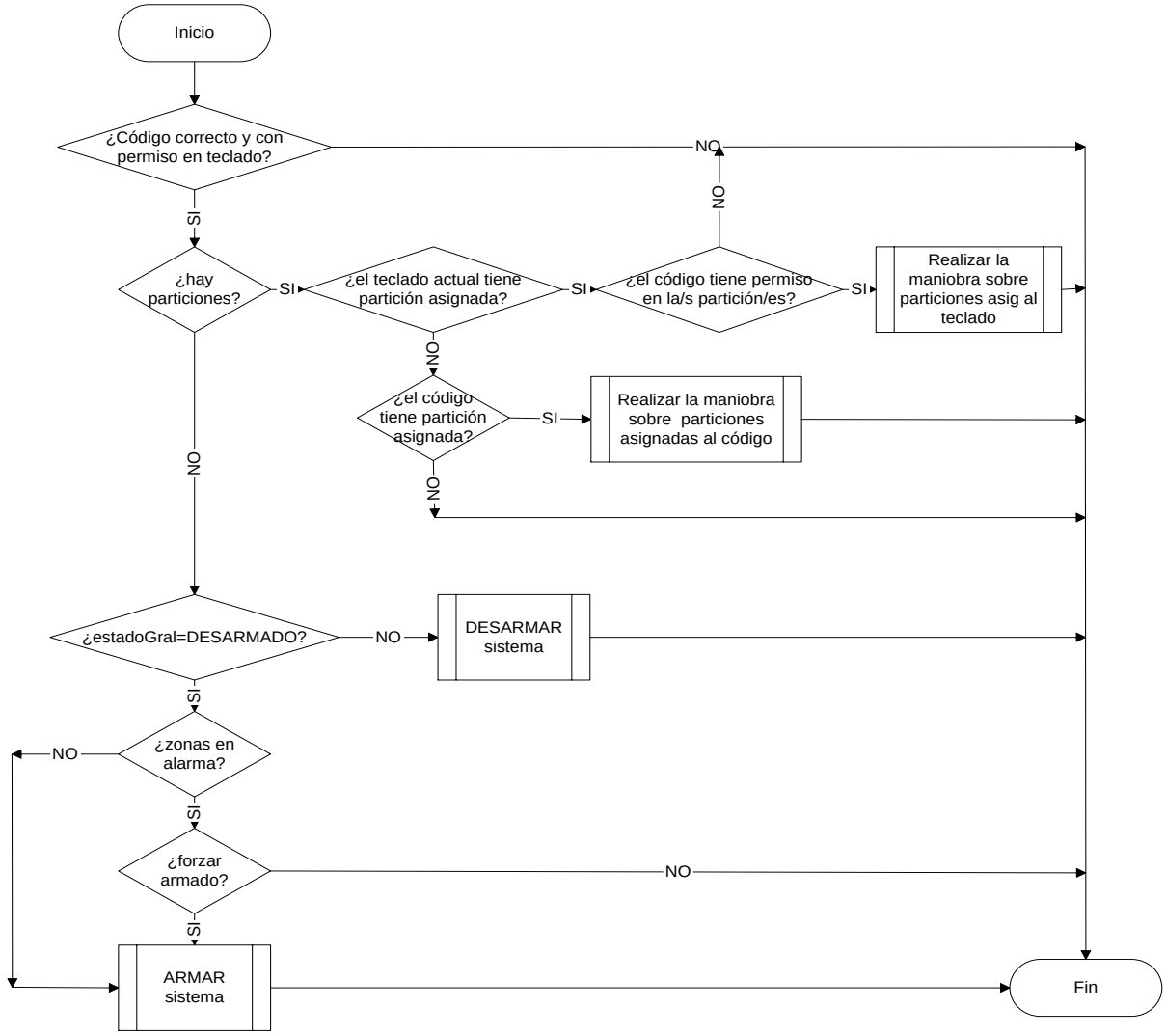
Por otro lado, para el caso concreto de maniobras de Armado/Desarmado se permite identificar el permiso de SMS y permiso E-mail por cada uno de los

[8] Si se asignan todas las particiones significará una maniobra TOTAL.
[9] Si se asocia más de una partición, la maniobra a realizar será la contraria al estado actual de las particiones con permiso si todas tienen el mismo estado o DESARMADO si se tienen distintos.
[10] Para el caso de actuar sobre las particiones asignadas al teclado, ya que aquí no es factible el control del permiso de cada código sobre las distintas particiones, solo se actuará sobre las que tenga permiso el código y siguiendo el criterio indicado en la nota anterior.

códigos para que solo se envíen los eventos de dichos códigos y no de todos. Será necesario antes habilitar el permiso de SMS y E-Mail al parámetro fijo general.

En la Figura1 se puede ver el diagrama de flujo donde se representan las comprobaciones efectuadas en cada maniobra.

Figura 1



Además se puede configurar si se permite utilizar las combinaciones de teclas que permiten el bloqueo del teclado para dar seguridad ante pulsaciones indeseadas.

A continuación se muestra el listado con la identificación de todos los códigos usados por la central de alarmas para registrar maniobras así como su interpretación/significado:

ID Código	Descripción
[1-32]	Códigos de usuario [000000 -999999][11]
35	Código de Coacción
36, 60 y 61	Código de acceso TCP (Principal, ECO1 o ECO2)
37	Código de Pánico
38	Código de Pánico Rápido[12]
41-48	Código reservado para maniobras por SMS por medio de los teléfonos 1-8 definidos
51-58	Código reservado para maniobras por SMS por medio de las claves 1-8 definidas

7.6 LLAVES ELECTRÓNICAS

La Central de Alarmas Atenea G4 permite trabajar con tres tipos diferentes de llaves electrónicas para poder actuar sobre el estado del sistema al igual que se hace con los códigos de usuario:

- Llaves Maestras
- Llaves de Usuario
- Llaves de Servicio Técnico.

[11] Uno de los códigos definidos en el Software de Configuración. Si es necesario, rellenar con ceros a la izquierda hasta obtener los 6 dígitos.
[12] Usando la combinación de teclas B+6.

Se puede elegir el permiso de uso de forma independiente. Cada una se identificará por su número[13].

7.6.1 Llaves maestras

Si se activa el permiso de uso de llaves maestras se podrá actuar sobre el estado del sistema[14] con cualquier llave Maestra configurada con el mismo número de Maestreamiento definido en la central y siempre que la llave tenga permiso sobre esta central maestreada.

Nota: Si se desea hacer uso de este tipo de llaves póngase en contacto con su proveedor.

7.6.2 Llaves de usuario

Aunque tampoco existe limitación en la cantidad de llaves de usuario en uso, bien es cierto que solo se podrán asignar permisos de llave en partición y permisos de llave en lectores así como particiones asignadas por defecto a número máximo de 32. Los números de las llaves electrónica están comprendidos entre 1-255.

IMPORTANTE: De las 32 llaves electrónicas que se pueden definir, por defecto tan solo la primera de ellas será la llave maestra o llave de nivel 3. Ver el anexo 10.9

El cliente con ayuda de las llaves de usuario podrá realizar maniobras de Armado/Desarmado Parcial/Total[15] siempre y cuando la llave tenga el mismo Número de Sistema y número de Reprogramación que el definido en la central. Evidentemente, si se asigna una o varias particiones a una llave, para que ésta pueda realizar maniobras de armado/desarmado sobre las mismas

[13] Actualmente el número de llave más alto admisible es el 255.
[14] Maniobras de Armado/Desarmado Total
[15] Si se asignan todas las particiones significará una maniobra TOTAL. Si se asocia más de una partición, la maniobra a realizar será la contraria al estado actual, de aquellas sobre la que tenga permiso, si todas tienen el mismo estado o DESARMADO si se tienen distintos estados.

deberá tener permiso en ellas, aunque tendrán prioridad las particiones asignadas al lector si las tuviera[16]

*Nota: El número de sistema es único para cada central. Este número estará comprendido entre 1 a 2^{32}, por lo que pueden existir 2^{32} * 255 llaves diferentes.*

También para el caso concreto de maniobras de Armado/Desarmado se permite identificar el permiso de SMS y permiso E-mail por cada una de las llaves para que solo se envíen los eventos de dichas llaves y no de todas. Pero, al igual que para los códigos, primero será necesario habilitar el permiso de SMS y E-Mail al parámetro fijo general.

El funcionamiento de estas llaves de usuario se puede ver en la figura 2

7.6.3 Llaves de servicio técnico

La Central de Alarmas puede usar, si así se le configura, una llave de Servicio Técnico que junto con el código de Servicio Técnico servirá para poder acceder a los menús de Servicio Técnico e Ingeniero.

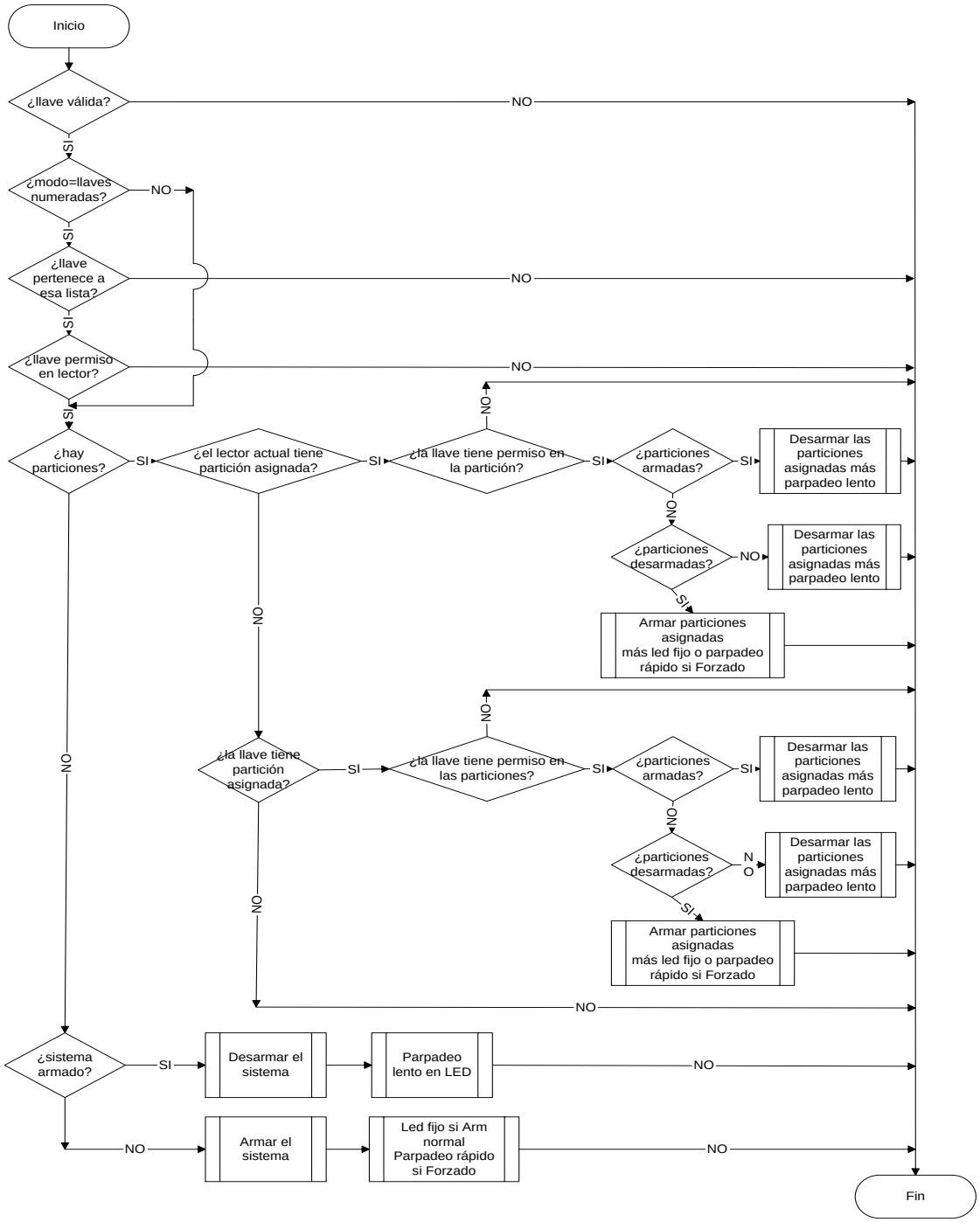
Tras introducir la llave de Servicio Técnico se dispone de 5 minutos para acceder al menú siempre y cuando el sistema no esté Armado por completo. Pasado ese tiempo se saldrá del menú y será necesario introducir de nuevo la llave si se quiere seguir comprobando alguna opción.

Ver apartado siguiente para información sobre dichos menús.

Nota: Si se desea hacer uso de este tipo de llaves póngase en contacto con su proveedor.

[16] Para el caso de actuar sobre las particiones asignadas al lector, ya que aquí no es factible el control del permiso de cada llave sobre las distintas particiones, solo se actuará sobre las que tenga permiso la llave y siguiendo el criterio indicado en la nota anterior.

Figura 2: funcionamiento llave usuario



7.7 CÓDIGOS DE SERVICIO TÉCNICO E INGENIERO

La Central de Alarmas dispone de un código de 6 dígitos que permite acceder tanto al menú de Servicio Técnico como al de Ingeniero.

La siguiente tabla resume el acceso a los distintos menús:

Descripción	Entrada de Códigos
Menú de Servicio Técnico	CHIME + CCCCCC + ENTER
Menú de Ingeniero	CONTROL + CCCCCC + ENTER

El acceso a estos menús permite realizar comprobaciones internas del sistema de seguridad (Comunicación con teclados, Versión del sistema, Conexión con receptoras, Nivel de cobertura GSM, Configuración de red local,…).

Si la marca de usar llaves de Servicio Técnico está activada, se deberá introducir antes ésta para poder hacer uso del código en el teclado.

Nota: El acceso y contenido de estos dos menús se detalla en los puntos 6 y 7 de este mismo manual.

7.8 PARÁMETROS DE LA CENTRAL

La central de alarmas dispone de 44 parámetros internos con sus correspondientes códigos Contact-ID. Son los llamados parámetros fijos.

Asimismo, es posible configurar hasta 32 parámetros relativos a zonas. Éstos son los que forman el conjunto de parámetros configurables.

IMPORTANTE: El uso de los parámetros técnicos, tales como gas, incendio, inundación, etc, no están cubiertos por la norma, aunque se permite su uso y no anula la certificación mientras no interfieran en ninguna de las otras

funciones del sistema. Usted puede encontrar una lista de todos estos parámetros en el anexo 10.2.

A continuación se indican los valores configurables comunes a todos los parámetros (internos o relativos a zonas):

- *Código Contact-ID:* valor unívoco que identifica a cada parámetro en la tabla de eventos Contact-ID universal
- *Permiso SMS:* indica si cuando se produzca este parámetro hay que enviar un mensaje corto a un máximo de 3 números de teléfono de los 8 números de teléfono autorizados informando de la incidencia.
- *Permiso E-Mail:* indica si cuando se produzca este parámetro hay que enviar un correo electrónico a un máximo de 3 direcciones de correo de las 8 direcciones autorizadas informando de la incidencia.
- *Acción/Macro asociada:* indica si hay que ejecutar o no una acción/macro cuando se produzca este parámetro.
- *Texto descriptivo:* es el texto que se muestra en caso de alarma. Sugerencia: indicar descripción del tipo de alarma.

Para el caso de parámetros fijos además se indica si supone un Evento o una Restauración.

Y para los parámetros configurables, si son de tipo 24 horas o no. Esto afecta directamente sobre la máscara de vigilancia.

7.9 ACCIONES

En la Central de Alarmas es posible definir hasta 96 acciones diferentes pudiendo ser de tipo ON, OFF O TEMPORIZADAS.

Para crear estas acciones la central utiliza las salidas de zumbador de sus periféricos ICPA, las salidas de los demás expansores y sus propias salidas de relé.

IMPORTANTE:

- *Algunas configuraciones pueden hacer que el grado de certificación se vea reducido (véase el anexo 10.1).*
- Las acciones programadas para activar dispositivos de aviso (Sirenas, flashes, etc…) y marcadas como "Sirenas" pueden ser desactivadas por un usuario de nivel 2.

La máxima temporización para las salidas es de 476 segundos, aproximadamente 8 minutos. El OFF apaga las salidas y el ON las enciende permanentemente salvo para el caso de los teclados, en los cuales se convierte en una temporización de 255 segundos, casi 5 minutos, debido a considerarse una salida Sirena.

Además se tiene la posibilidad de asignar un retardo de hasta 476 segundos para comenzar cualquier acción.

Por otro lado, es posible ejecutar estas acciones:

- Mediante teclado (usando la combinación numérica CONTROL + NN + ENTER)
- Mediante SMS (usando el preformato de mensaje #C NN#)
- Mediante Bidireccionalidad desde la CRA.
- Mediante asociación de las mismas tanto a parámetros (internos o aplicables a zonas) como a alarma de zonas.

En el caso de la Bidireccionalidad se pueden ejecutar TODAS las acciones definidas en el sistema. Para el resto de medios se podrá definir el permiso individual.

A continuación se muestra el listado de todos los códigos que identifican el origen de las mismas:

ID Código	Descripción. Origen de la acción
36, 60 y 61	Acceso TCP (Principal, ECO1 o ECO2)
40	Maniobras internas (por asociación a parámetros o zonas)
41-48	SMS por medio de los teléfonos 1-8 definidos
50	Teclado.
51-58	SMS por medio de las claves 1-8 definidas

7.10 MACROS

Si la configuración de acciones no resuelve las necesidades de actuación del sistema de seguridad ante una determinada incidencia es posible configurar macros, esto es, conjunto de acciones, y usarlos en su lugar.

IMPORTANTE:

- *Algunas configuraciones pueden hacer que el grado de certificación se vea reducido (véase el anexo 10.1).*
- Las acciones programadas para activar dispositivos de aviso (Sirenas, flashes, etc…) y marcadas como “Sirenas” pueden ser desactivadas por un usuario de nivel 2.

La Central de Alarmas puede manejar hasta 12 macros formada cada una de ellas como máximo por 8 acciones.

Al igual que con las acciones, la ejecución de macros también es posible:

- Mediante teclado (usando la combinación numérica B + NN + ENTER)

- Mediante SMS (usando el formato de mensaje #F NN#), en el que NN es el número de macro
- Mediante Bidireccionalidad desde la CRA.
- Mediante asociación de las mismas tanto a parámetros (internos o aplicables a zonas) como a apertura de zonas.

Como consecuencia, los códigos de origen pueden ser los mismos que los indicados en la acciones.

Asimismo se podrá definir el permiso de forma individual para cada una de ellas salvo en el caso de Bidireccionalidad donde se podrá ejecutar cualquier macro sin restricción.

7.11 GSM/GPRS

La central de alarmas integra los siguientes módem GSM/GPRS para poder tener una comunicación Ethernet alternativa e incluso poder modificar su estado por medio del Servicio de Mensajes Cortos:

- MC55i-w de Cinterion
- MC55i de Cinterion

El primero es un módulo integrado en la propia circuitería de la tarjeta y el segundo es un módulo externo independiente pero ambos usan el puerto serie RS-232 de la tarjeta.

> *IMPORTANTE: El uso del módulo GSM / GPRS externo no se incluye en la certificación Grado 4.*

Si se quiere usar cualquiera de ellos será necesario indicar el Operador de la tarjeta SIM y la velocidad con la que se realizará la comunicación entre la central y

el módem. Además es necesario indicar en la programación el tipo de modem utilizado (interno o externo) usando el parámetro adecuado[17].

7.12 COMANDOS SMS

Existen una serie de comandos que permiten interactuar con la Central de Alarmas utilizando mensajes cortos de texto (SMS). Si se habilita este tipo de control por SMS, además de requerir una correcta sintaxis, la Central de Alarmas filtra la entrada de mensajes de texto bien por número de teléfono, por clave o por cualquiera de los dos, teléfono o clave. Para poder realizar estos filtros, la Central de Alarmas admite órdenes de hasta 8 números de teléfono distintos así como un máximo de 8 claves diferentes.

Estos mismos números de teléfono son los que en apartados anteriores se indicaba que pueden utilizarse como los destinatarios de las incidencias programadas con envío de SMS (parámetros internos de la Central, parámetros relativos a la alarma de zonas o alarmas de zonas).

Hay un tercer filtro que la central aplica a los SMS. Este filtro es temporal y consiste en que la central de alarmas no tendrá en consideración los SMS recibidos salvo que estos tengan una fecha y hora que coincida con la de la central con un margen de 15 minutos.

Los comandos han de tener el siguiente formato:

[Clave]#Orden<Espacio>Parámetros#[ACK]

Si se recibe clave, se compara. Si no, comprueba que el nº de teléfono es uno de los autorizados, es decir, uno de los definidos en el sistema por el servicio técnico.

Los comandos no distinguen entre mayúsculas y minúsculas.

[17] Lo que hay que indicar es si se usa el Relé 2 de la central para Módem/GSM exterior o no.

Al final de cada mensaje es obligatorio poner siempre el símbolo '#'. Por ello, el mensaje no puede contener el símbolo "#".

Las diferentes opciones de mensaje se muestran a continuación:

Mensaje	Descripción
#C (1-96)#	Ejecutar la acción NN, si ésta tiene permiso sms.
#F (1-12)#	Ejecutar la macro NN, si ésta tiene permiso sms.
#A T#	Armado Total
#A (1-5)#	Armar partición. Sólo si como mínimo existen 2 particiones.
#D T#	Desarmado Total
#D (1-5)#	Desarmado Parcial. Sólo si como mínimo existen 2 particiones.
#M Mensaje#	Enviar un mensaje para poder ser visualizado por el display
#E 0#	Informa del estado actual de la Central y de los últimos 5 eventos. Devuelve siempre confirmación en sms.
#E (1-209)#	Informa al usuario si una zona tiene o no programado el envío de SMS ante alarma. Devuelve siempre confirmación por sms.
#R (1-209)#	Reactiva el envío de SMS ante una alarma de la zona indicada. Devuelve siempre confirmación por sms.
#I (1-209)#	Anula el envío de SMS ante una alarma de la zona indicada. Devuelve siempre confirmación por sms.

ACK: S = SMS o ACK:E=E-Mail

Por otro lado, para mayor seguridad ante el control por SMS, se puede pedir confirmación de la acción realizada. Esta confirmación podrá ser en el teléfono de origen del comando si se indica al final la letra "S" o "s" o en un mail si es que se indica la letra "E" o "e" y el teléfono o clave tiene una dirección de correo asociada[18].

En caso de que el usuario solicite confirmación y el mensaje llegue fuera de tiempo, la central contestara con un SMS o un mail indicándoselo.

[18] En caso de tener habilitado como Filtro Clave o Teléfono (no solo clave o solo teléfono) lo primero que se atiende es a la clave, por lo que si se pide confirmación a Email se tomará el mail asociado a la clave .

7.13 CORREO ELECTRÓNICO

Al igual que la central de alarmas puede informar de sus incidencias mediante mensajes cortos de texto o SMS, también puede utilizar un servidor SMTP para informar de estas incidencias mediante mensajes de correo electrónico[19].

La Central de Alarmas permite editar una lista de 8 direcciones de correo electrónico como máximo.

Además, también podrán usarse como destinatarios de las respuestas a comandos SMS. Para ello se permite asociar una dirección de correo a cada uno de los teléfonos y a cada una de las claves definidas.

7.14 MENSAJES

La Central de alarmas puede albergar hasta 10 mensajes de texto recibidos bien desde un mensaje corto de texto (SMS) o bien usando bidireccionalidad.

Cada vez que la central reciba un mensaje avisará de forma acústica y lo mostrará en el display de todos los teclados de la instalación instando al usuario a entrar en el menú de mensajes. Desde este menú se podrá visualizar y/o borrar cada mensaje de forma individual.

Debido a que los mensajes recibidos pueden tener una longitud mayor que las líneas del display de los teclados ICPA se mostrará cada mensaje usando un modo “cortina” que irá refrescando el contenido del mismo a intervalos de medio segundo.

Si se recibe más de 10 mensajes se eliminarán de forma automática los mensajes más antiguos no pudiendo ser leídos.

[19] Actualmente solo se ofrece la posibilidad de usar un único servidor SMTP propio de IC debido a no estar implementado la característica de correo con Autentificación necesaria para la mayoría de los servidores.

7.15 HISTORIAL DE EVENTOS

La central Atenea G4 cuenta con dos historiales de eventos. El primero de ellos tendrá una capacidad de 1.000 eventos y sólo almacenará los incidentes que marca el estándar EN50131-3 como obligatorios.

El segundo, al que llamamos historial auxiliar, tendrá una capacidad de 256 eventos. En este, se registrarán todas las incidencias que se producen en el sistema, tanto las obligatorias como las opcionales.

Para cada evento almacenado se asocia la fecha/hora de la incidencia y los datos auxiliares.

El listado de eventos se podrá visualizar por medio de las siguientes opciones:

- El Menú de Eventos
- El Software de Configuración ProgG4
- El programa de gestión y control de alarmas

Ambos historiales de eventos se almacenan en una memoria EEPROM, lo que garantiza mantenerlos después de un fallo de alimentación en el sistema. (Serial EEPROM 24LC512, Conservación de los datos> 200 años)

7.16 GESTIONES INTERNAS

7.16.1 Alertas

En los display de los teclados se presentará de forma permanente, en la primera fila de caracteres información relativa a la fecha y hora del sistema de alarma y en la segunda la versión del sistema (Si un fallo de microprocesador está presente en el sistema, en la segunda línea del teclado se muestra el mensaje "ICPA Versión XX".). En caso de haber avisos relativos al estado y/o funcionamiento de la Central de Alarmas se mostrará el mensaje de 'HAY ALERTAS' junto con la versión del

sistema de forma rotativa cada 2 segundos. Este mensaje ira acompañado de un aviso acústico cada 3 minutos aproximadamente.

IMPORTANTE: El mensaje 'HAY ALERTAS' y el aviso acústico permanecerán hasta que haya desaparecido la causa que lo ha producido y las alertas hayan sido consultadas después por el usuario desde el menú de alertas.

Para consultar el menú de Alertas, presione la tecla A seguido de uno de los 32 códigos de usuario autorizado y la tecla ENTER:

A + CCCCCC + ENTER

A continuación se enumeran las diferentes alertas de las que puede informar la Central de Alarmas así como de su interpretación.

Alerta	Descripción
Estado del sistema de seguridad	Indica el estado del sistema: Armado o Desarmado. Si hay particiones, también puede aparecer "Arm. Parc" y una lista de las particiones armadas.
RESET WATCHDOG	Indica que la central se ha reseteado por algún fallo de funcionamiento en micro.
ALARMA ZONA XXX	Indica que ha habido una nueva alarma en la zona que muestra.
FALLO COM PIC	Mal funcionamiento del equipo.
FALLO COM. CON ETDS, COM. 485	Hay algún problema con los módulos expansores o teclados conectados a la central y éstos no se comunican con la central.
FALLO TX CON MODULO GPRS	Indica que ha habido un problema en la transmisión vía GPRS. Si el fallo persiste este puede ser debido a un problema con el módulo GPRS o la tarjeta SIM.
FALLO TX CON MODULO ETH	Indica que ha habido un problema en la transmisión vía Ethernet. Si el fallo persiste compruebe el correcto funcionamiento del router y que tenga correctamente configurados los puertos.
FALLO 220 ALIM. CENTRAL	Indica que ha habido un corte en el suministro eléctrico.

Alerta	Descripción
FALLO BATERIA ALIM. SECUNDARIA	Cada día el sistema realiza una prueba de batería para comprobar que está en buen estado. Si aparece este mensaje, significa que se ha detectado un problema con la batería, y posiblemente haya que sustituirla por una nueva.
FALLO SALIDA ALIMENTACION	Este fallo aparece cuando hay algún problema en la fuente de alimentación (Ejemplo: la fuente de alimentación no pueda carga correctamente la batería)
XXX Zonas ANULADAS TEMP.	Indica que hay XXX zonas anuladas por un armado forzado o por petición desde el Menú de Usuario.
HAY FALLOS INHIBIDOS	Indica que en el último armado, los fallos existentes fueron anulados para poder llevarlo a cabo.

7.16.2 Bidireccionalidad

La Central de alarmas tiene bidireccionalidad absoluta y desde ella se pueden realizar las siguientes tareas:

Orden	Descripción
Descargar eventos	Descarga todos los eventos almacenados en la memoria de la central.
Comprobar actividad de la Central	Ver los distintos eventos ocurridos
Consultar estado de las zonas	La Central informa del estado actual de todas sus zonas así como de su máscara de vigilancia actual[20].
Armar/Desarmar[21] el Sistema	Se puede realizar un armado/desarmado total o parcial remoto y conocer el estado de cada una de las particiones del sistema en cada momento.
Activar/Desactivar una zona[22]	Añadir/Eliminar del mapa lógico de la Central una zona.
Activar/Desactivar una salida	Poner a on/off o temporizar cualquiera de las salidas[23] del sistema.

[20] Se informa de si la zona está activa o no, si está en estado de alarma o reposo y si está vigilada o no. La no vigilancia puede deberse a no estar armadas sus particiones o a estar anulada temporalmente. Y si la zona está inactiva se mostrará siempre en reposo.
[21] Este Armado Remoto será siempre forzado.
[22] Solución provisional usada en caso de averías con detectores. En cuanto el Servicio Técnico solucione el problema deberá reactivarse dicha zona.

Orden	Descripción
Ejecutar Acción/Macro	Ejecutar remotamente cualquiera de las acciones o macros.
Enviar un mensaje	Enviar un mensaje que será visualizado en los displays de los teclados.
Forzar conexión con receptora MST-1	Forzar a la Central a que envíe petición de conexión (abonado nuevo) a la/s receptora/s MST-1 programada/s.
Solicitar envío de Test periódico	Pedir a la Central que envíe un evento de "Test periódico" al margen de su periodicidad diaria.
Petición de información de sistema	Solicitar información referente a tipo de Central y versiones de programa.
Leer/Escribir Fecha/Hora	Consultar/Modificar la Fecha/Hora del Sistema.
Petición de Reset	Ordena a la Central que se resetee.
Autotest Detectores	Ejecuta un test remoto a los sensores
Test de Batería	Ejecuta un test remoto a la batería.

7.16.3 Test periódico

La Central de Alarmas envía el evento "Test periódico" a los 5 minutos de haber sido programada o reseteada, y a partir de ese instante y mientras no se reprograme, se enviará de forma periódica cada 24 horas.

7.16.4 Polling - Conexión Ethernet/GPRS

Otra característica es el polling. Este es la comunicación que se mantiene con la Receptora cada 10 segundos o el tiempo elegido por el usuario para asegurar la integridad del sistema.

IMPORTANTE: Aunque el sistema le permite establecer un tiempo de muestreo superior a 10 segundos, el grado 4 sólo se garantiza si se utiliza la opción de los 10 segundos. De lo contrario el sistema será de grado 3

[23] Salidas de zumbador de los teclados ICPA, salidas de relé on board y salidas de relé de las demás etds expansoras.

Habitualmente la vía principal de comunicación es por ADSL y respaldo vía GPRS. En este caso, si la comunicación por la vía principal no es posible, la central conmuta automáticamente a GPRS comprobando cada 5 minutos si es posible volver a comunicar por ADSL. Cuando éste se restaura, la central cierra la comunicación GPRS y retorna a la vía principal.

La detección del fallo de la conexión con la receptora se hace en menos de 20 segundos tanto para Ethernet como para GPRS, cuando se utiliza un tiempo de muestreo de 10 segundos.

7.16.5 Estado de la fuente de alimentación principal y auxiliar

La central de alarmas está supervisando de forma constante tanto la alimentación principal como la salida de 12Vdc y la carga de batería. En el caso de que hubiera un corte en el suministro eléctrico, la central registrará el fallo automáticamente pero no lo reportara a la receptora hasta que no hayan pasado 10 minutos sin la alimentación principal.

De igual forma si hubiera cualquier problema en el circuito de la fuente de alimentación y ésta no proporcionara la tensión adecuada o no fuera capaz de cargar la batería, la central registrará y reportará de forma automática un fallo en la fuente de alimentación.

La Central de Alarmas realiza una prueba de batería de forma automática todos los días a las 12 a todas las baterías del sistema, siempre y cuando lleve más de una hora en marcha. En caso de no poder terminar la prueba de batería (bien porque ésta tiene un nivel muy bajo de tensión, es decir, está descargada, o porque la central no tenga conectada ninguna batería) se reportará el evento de fallo de batería.

7.16.6 Modo IP por defecto

Este es el modo que se usa cuando no hay datos de configuración en la central y con la única finalidad de poder cargar datos válidos.

La dirección IP por defecto es 10.0.0.10.

Para ponerle en este modo se pondrá el puente IP-DEF.

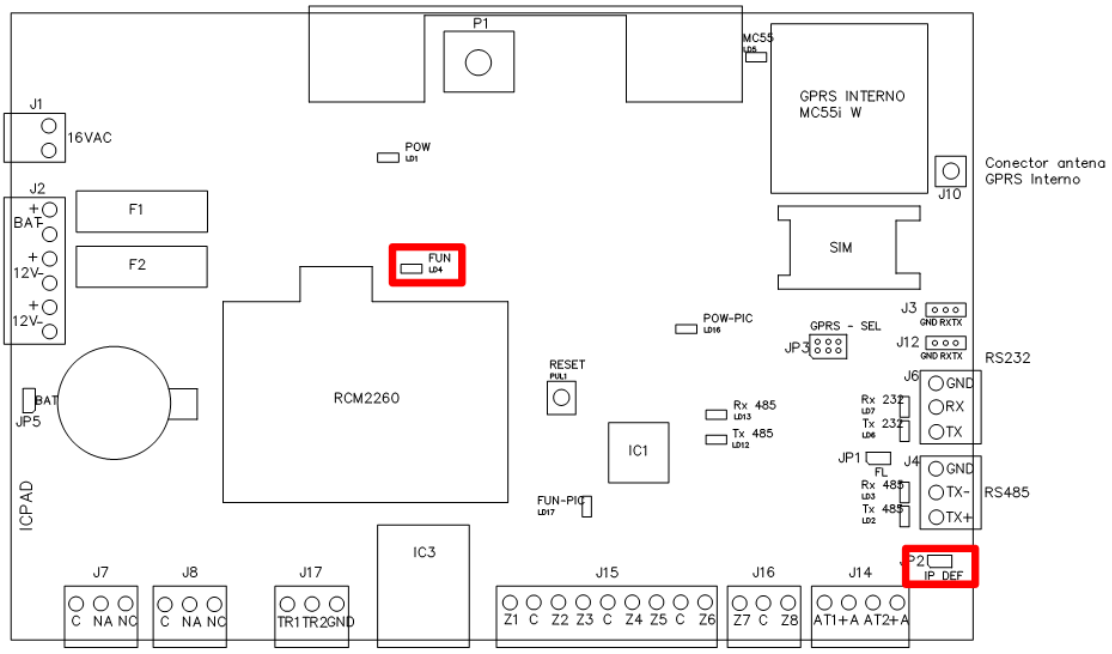
Una vez cargados los datos de una programación se debe sacar a la central de este modo, aunque se quisiera usar la IP por defecto, para que todo funcione correctamente[24].

El piloto de funcionamiento de la tarjeta ICPAD parpadeará de forma distinta para indicarnos que la central se encuentra en modo IP por defecto (2 segundos ON, 2 segundos OFF).

Nota: Estando en este modo no es necesaria ni la clave de servicio técnico, ni la autorización del usuario para acceder a la programación de la central mediante el software ProgG4

En el esquema siguiente se indica la ubicación del puente usado para poner o quitar a la central del modo IP por defecto y la ubicación del led de funcionamiento:

[24] En modo IP por defecto SOLO se habilita las funciones mínimas para poder obtener datos correctos



Tener en cuenta que además de poner o quitar el puente es necesario resetear la central pulsando el pulsador de reset para que el cambio tenga efecto.

7.16.7 Puesta en hora

Si la Central de Alarmas está conectada a receptora, la central mantendrá la hora sincronizada permanentemente con la hora de esta.

8 MENU DE SERVICIO TÉCNICO

El menú de Servicio Técnico está pensado para realizar operaciones de supervisión y/o mantenimiento del Sistema de Seguridad.

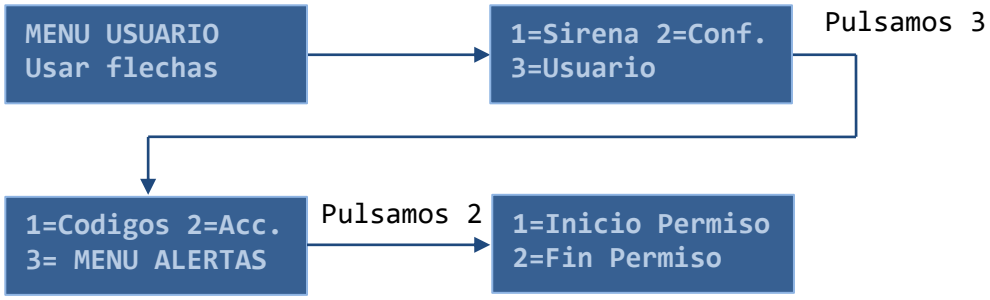
Para poder acceder al menú de Servicio Técnico el instalador ha de solicitar que un usuario le dé permiso.

Este permiso se habilita entrando en el menú Acc (opción 3.2) del menú de usuario. En este menú el usuario podrá habilitar o denegar el permiso de acceso al servicio técnico (una vez autorizado, el permiso permanece hasta que el usuario lo deniegue).

Ejemplo de la operación a realizar por el usuario:

Pulsar la tecla B seguida de uno de los 32 códigos de usuario autorizados y de la tecla ENTER

B + CCCCCC + ENTER



Una vez obtenido el permiso para acceder al menú de Servicio Técnico, el instalador debe pulsar CHIME seguido de los 6 dígitos del código autorizado de servicio técnico y de la tecla ENTER.

CHIME + CCCCCC+ENTER

Aparece el siguiente menú:

Las teclas para moverse por los distintos menús son:

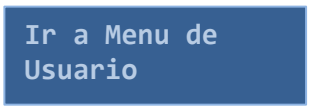
- **ENTER para aceptar**
- **PROG para salir de subpantallas o del menú principal**
- **y las flechas para avanzar y retroceder**

8.1 OPCIONES DEL MENU DE SERVICIO TÉCNICO

8.1.1 Ir al Menú de Usuario

Esta es la forma en la que el instalador accede al menú de Usuario para realizar alguna tarea perteneciente al mismo (por ejemplo la prueba de batería o el test de zonas) sin necesidad de conocer los códigos de acceso del usuario final.

Desde el menú anterior pulsar Avance y aparecerá:



Pulsando ENTER entraremos en el menú de usuario

8.1.2 Ver Historial de eventos

Si en vez de pulsar “ENTER” se sigue avanzando; aparece la opción “Ver Historial de eventos”.

Pulsando ENTER entraremos en el historial de eventos.

La central Atenea G4 cuenta con dos historiales de eventos. El primero de ellos tiene una capacidad de 1.000 eventos y sólo almacena los eventos que marca el estándar EN50131-3 como obligatorios. Para acceder a él, pulse el '1'.

El segundo, al que llamamos "Historial auxiliar", tiene una capacidad de 256 eventos. En este segundo historial se registran todas las incidencias que se producen en el sistema, tanto las obligatorias como las opcionales. Para acceder a él, pulse el '2'.

En ambos historiales, pulsando la tecla de avance, se mostrará la información relativa a cada evento (fecha / hora, eventos y datos auxiliares). Con la tecla de retroceso se puede ir en la dirección opuesta.

El desplazamiento de avance y retroceso se realiza también con las teclas: → y ←.

Para salir del menú en cualquier momento, pulse la tecla PROG.

El instalador visualizará los mismos eventos que visualizaría el usuario. Para acceder a mayor información con respecto a los eventos sería necesario descargarse los eventos del sistema desde el ProgG4 en un PC.

A continuación se muestra un resumen de los eventos más habituales que pueden aparecer en este historial:

Evento	Descripción
Armado	Se ha realizado una maniobra de Armado, Desarmado, o Armado Forzado. En el display aparecerá el número del código o de la llave con que se ha realizado la misma.
Desarmad	
ArmKey	
DesarKey	
ArmForza	
Fallo220	Ha habido un fallo en el suministro eléctrico de 220v durante más de 10 minutos.
Rest.220	Se ha restaurado el suministro eléctrico de 220v.
Fbateria	La última prueba de batería realizada dio como resultado un nivel bajo de la batería. Avisar al Servicio Técnico.
Ffuente	Hay un fallo en la fuente de alimentación del sistema Avisar al Servicio Técnico
Av.Perif	Se ha perdido la comunicación con una ETD del sistema (expansor o teclado). Es un problema de funcionamiento interno llamar al Servicio Técnico.
RestPeri	Se ha recuperado la comunicación con una ETD del sistema.
PrgCentr	Se ha cambiado la programación interna de la Central de Alarmas.
Pánico	Ha habido una alarma de Pánico o Coacción. En el display aparecerá el número de zona en que ha ocurrido.
Coacción	
BypassZ	Se ha anulado una zona desde el menú de Usuario o por un Armado Forzado.
Bpas24H	Se ha anulado una zona de tipo 24 horas desde el menú de Usuario o por un Armado Forzado
RBypassZ	Se ha restaurado la zona indicada desde el menú de Usuario.
RBpas24H	Se ha restaurado la zona 24 horas indicada desde el menú de Usuario.
Robo, Sabotaje…	Se ha producido una alarma de la zona indicada.

8.1.3 .Ir al menú de alertas

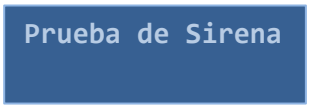
Esta es la forma en la que el instalador acceder al menú de alertas sin tener que utilizar los códigos de acceso del usuario final.

En el menú anterior, presione hacia adelante y aparecerá lo siguiente:

Presionando ENTER entrará en el menú de alertas

8.1.4 Prueba de Sirena

Con esta opción se temporizan durante 10 segundos todas las salidas configuradas como sirena en el sistema.



8.1.5 Monitor de ETDS

Con esta opción, es posible comprobar el estado de las comunicaciones con todas las ETDs del sistema (máximo 21).

Una vez estamos en la pantalla anterior, pulsamos ENTER para acceder al Monitor de ETDs

La información se muestra de forma individual para cada uno de los periféricos (ETDs) instalados y dados de alta en el sistema. Utilizaremos las flechas para avanzar e ir viendo la información de cada uno de ellos.

Los parámetros sobre los que se muestra información son:

- El número de ETD o periférico (ETD).
- El estado de la comunicación con la central.
- El estado de la alimentación principal (220).
- El estado de la batería del mismo (BAT).
- El estado de la fuente de alimentación (FAL).

Para cada uno de estos valores la central utilizará las siguientes abreviaturas:

- 'V' si el parámetro sobre el que se muestra la información esta correcto.
- '*' si hay algún problema en el parámetros sobre el que se muestra la información.

Ejemplo:

```
ETD  220 BAT FAL
00 V  V   V   V
```

Hay que tener en cuenta que si el periférico es un teclado ICPA, tan solo se mostrará información sobre el estado de comunicaciones ya que el resto carece de sentido.

Además en el caso de que un periférico no comunique, el resto de información no tendrá relevancia alguna.

8.1.6 Autotest de los detectores

Con esta opción se activan durante 10 segundos todas las salidas programadas como auto-test.

8.1.7 Test de comunicaciones

Esta opción le permite realizar una prueba de comunicación para cada una de las vías de transmisión de las que se disponga y con cada una de las receptoras programadas de una manera simple.

Sin presionar cualquier tecla, se muestra un mensaje directamente como el de la siguiente figura:

Una vez en la pantalla anterior, pulse ENTER para realizar la prueba. Se enviará una señal de “test” a todas las CRA programadas en el sistema por cada una de las vías de transmisión que esten disponibles.

Momentáneamente aparecerá una pantalla con el siguiente texto:

Después muestra la siguiente pantalla para dar el resultado:

La primera línea muestra las diferentes receptoras y vías de transmisión que se pueden programar en el sistema. De izquierda a derecha:

- ' R ' = Receptora Principal, 'E ' = Ethernet, 'G ' = GPRS
- ' E1 ' = ECO1 , 'E ' = Ethernet, 'G ' = GPRS
- ' E2 ' = ECO2 , 'E ' = Ethernet, 'G ' = GPRS '

La segunda línea indica el estado de conexión de la central con las diferentes receptoras IP (MST-1) y vías programadas en el sistema. Los valores posibles que cada una de las conexiones puede tomar son:

- - = La central Atenea G4 no tiene ninguna receptora IP de este tipo configurada.
- S = Se ha conectado correctamente con la receptora IP .
- N = No se pudo establecer una conexión.
- ? = Intentando conectar.

8.1.8 Versión Sistema

Seleccionando esta opción con la tecla ENTER se muestra información referente a la versión del sistema (firmware de la central), la versión del software de programación y la versión del PIC.

9 MENU DE INGENIERO

El menú de Ingeniero está dirigido a realizar operaciones de supervisión y/o mantenimiento del Sistema de Seguridad con más amplitud.

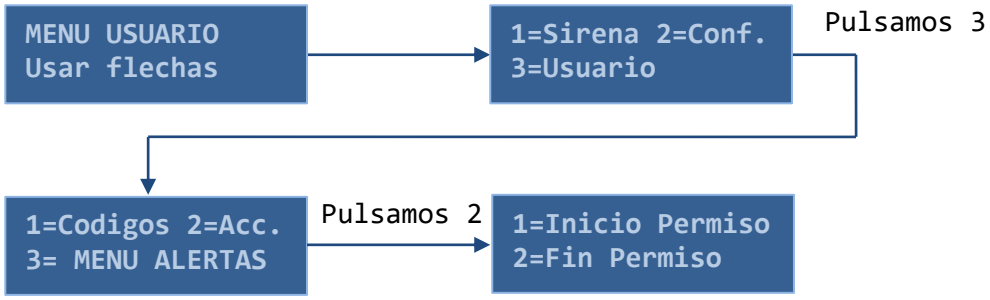
Para poder acceder al menú de ingeniero el instalador ha de solicitar que un usuario le dé permiso de igual forma que se hacía para el menú de servicio técnico.

Este permiso se habilita entrando en el menú Acc (opción 3.2) del menú de usuario. En este menú el usuario podrá habilitar o denegar el permiso de acceso al servicio técnico (una vez autorizado, el permiso permanece hasta que el usuario lo deniegue).

Ejemplo de la operación a realizar por el usuario:

Pulsar la tecla B seguida de uno de los 32 códigos de usuario autorizados y de la tecla ENTER

B + CCCCCC + ENTER



Una vez obtenido el permiso para acceder al menú de Ingeniero, el instalador debe pulsar CONTROL seguido de los 6 dígitos del código autorizado de servicio técnico y de la tecla ENTER.

CONTROL + CCCCCC+ENTER

Aparece el siguiente menú:

Las teclas para moverse por los distintos menús son:

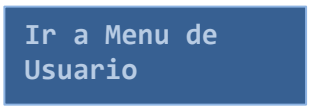
- **ENTER para aceptar**
- **PROG para salir de subpantallas o del menú principal**
- **y las flechas para avanzar y retroceder**

9.1 OPCIONES DEL MENU DE INGENIERO

9.1.1 Ir al Menú de Usuario

Esta es la forma en la que el instalador accede al menú de Usuario para realizar alguna tarea perteneciente al mismo (por ejemplo la prueba de batería o el test de zonas) sin necesidad de conocer los códigos de acceso del usuario final.

Desde el menú anterior pulsar Avance y aparecerá:



Pulsando ENTER entraremos en el menú de usuario

9.1.2 Ir al Menú del Servicio Técnico

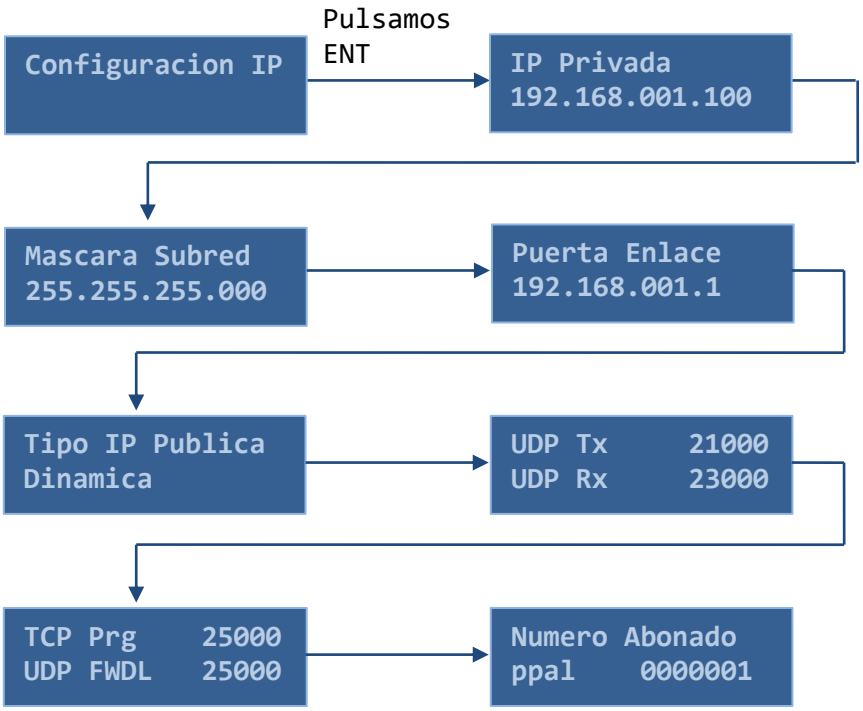
Con esta opción, se puede acceder al menú de Servicio Técnico, sin necesidad de salir y volver a teclear el código de Servicio Técnico.

9.1.3 Ver Config IP

Desde esta opción se pueden consultar los valores de configuración Ethernet.

Pulsando la tecla ENTER y utilizando las flechas para avanzar se mostrarán distintas pantallas con el valor de la direccione IP de la central, Máscara de Subred y Puerta de Enlace del Sistema.

Además, se especificará si la IP Pública es Estática o Dinámica y qué puertos se utilizan para la transmisión de eventos a la Receptora, recepción de los ACKs por parte de la Receptora y para la bidireccionalidad, y como dato útil también se indica el número del abonado principal si es que lo hay.



9.1.4 Conexión IP + Calidad Señal GSM/GPRS

Sin necesidad de pulsar ninguna tecla, se muestra directamente un mensaje como el de la figura.

La primera línea, indica el estado de conexión de la Central con las distintas receptoras IP (MST-1). De izquierda a derecha son:

- Estado conexión con Receptora Principal
- Estado conexión con ECO1

- Estado conexión con ECO2.

Los posibles valores que puede tomar cada una de las conexiones son:

- 0 = La Central no tiene configurada ninguna receptora IP de este tipo.
- S = Se ha conectado con éxito con la receptora IP.
- N = No se ha conseguido establecer la conexión.
- ? = Intentando conectar.

Esta opción sólo se utiliza cuando el sistema esta conectado a alguna receptora, y sirve para reiniciar la conexión con la receptora IP. Para ello, y sin salirse de esta pantalla, hay que pulsar la tecla ENTER (según se indica al final de la segunda línea). La central intentará conectarse de nuevo con todas las receptoras IP.

Momentáneamente aparecerá una pantalla con el texto:

Acto seguido se volverá a mostrar la misma pantalla para poder ver el resultado.

El proceso de conexión puede durar un tiempo, sobre todo si alguna de las vías de transmisión es GPRS, y finalizará cuando todas las receptoras tengan un valor distinto de “?”.

NOTA: La conexión con la receptora principal se puede realizar a través de ambas vías de transmisión.

En la misma pantalla, en la segunda línea, se puede comprobar la calidad de la señal recibida por el GSM/GPRS (en caso de que se utilice para transmisión GPRS o envío/recepción de SMS).

- Para poder usar SMS, el valor debe ser al menos del 38%.
- Para poder usar GPRS, el valor debe ser al menos del 48%.

Si no se consiguen dichos valores, el instalador debe probar a colocar el modem o la antena en otro sitio y permanecer en esta pantalla mientras busca otra ubicación (el valor se actualiza automáticamente en poco segundos).

Estos valores son sólo indicativos, dependen del operador, la saturación de líneas del momento, etc. Es por ello que en determinados momentos, el modem pueda funcionar con valores inferiores, y no hacerlo con otros muy superiores de cobertura.

Otra información que puede aparecer en esta pantalla, en la misma posición donde se refleja la cobertura del modem, es:

- NO CFG : se está configurando el modem.
- -OCUP- : no muestra la cobertura porque el modem está realizando otras tareas (SMS, GPRS).
- _____ : la central no tiene modem.

9.1.5 CHEKSUM Sistema

Esta opción permite comprobar la integridad del software del sistema, realizando un Checksum.

Tras pulsar ENTER, el sistema empezará a calcular el Checksum, lo que le llevará unos pocos segundos.

Para información relativa al Checksum del sistema consulte a su Proveedor.

10 ANEXOS

10.1 CONFIGURACIONES QUE INCUMPLEN EL ESTANDAR EN50131-3

- El Grado 4 solo está garantizado si se utilizan sensores Grado 4 con conexión a bus. De lo contrario el sistema será Grado 3.
- El Grado 4 solo está garantizado si se utiliza un tiempo de polling de 10 segundos. De lo contrario el sistema será Grado 3.
- No deberán asociarse relés que controlen dispositivos de aviso (sirenas, flashes, etc…) a los eventos de Tamper (sabotaje), fallo de interconexión (Avería periférico) o fallo de batería. Si estos eventos son asociados con un dispositivo de aviso (Señalización, indicación y/o salidas), el sistema no cumplirá con el estándar EN50131-3.
- El evento ”TAMPER” no deberá ser asociado a los relés que controlan dispositivos de aviso externos (sirenas exteriores), abarcando este evento las siguientes señales:
    - Tamper
    - Tamper sensor
    - Mascara sensor
    - Cortocircuito
    - Reducción de alcance
    - Sustitución sensor
    - Modulo añadido
    - 24 horas
    - Tamper módulo expansión

- Los eventos “fallo” no deberán ser asociados a los reles que controlan dispositivos de aviso externos (sirenas exteriores), abarcando este evento las siguientes señales:
    - Fallo report
    - Avería periférico
    - Fallo 220v
    - Fallo batería
    - Fallo fuente alimentación
    - Fallo sensor
    - Fallo dispositivo de aviso
- El evento “Atraco” (pánico o pánico silencioso) no deberá ser asociado a los relés que controlan dispositivos de aviso externos (sirenas exteriores)

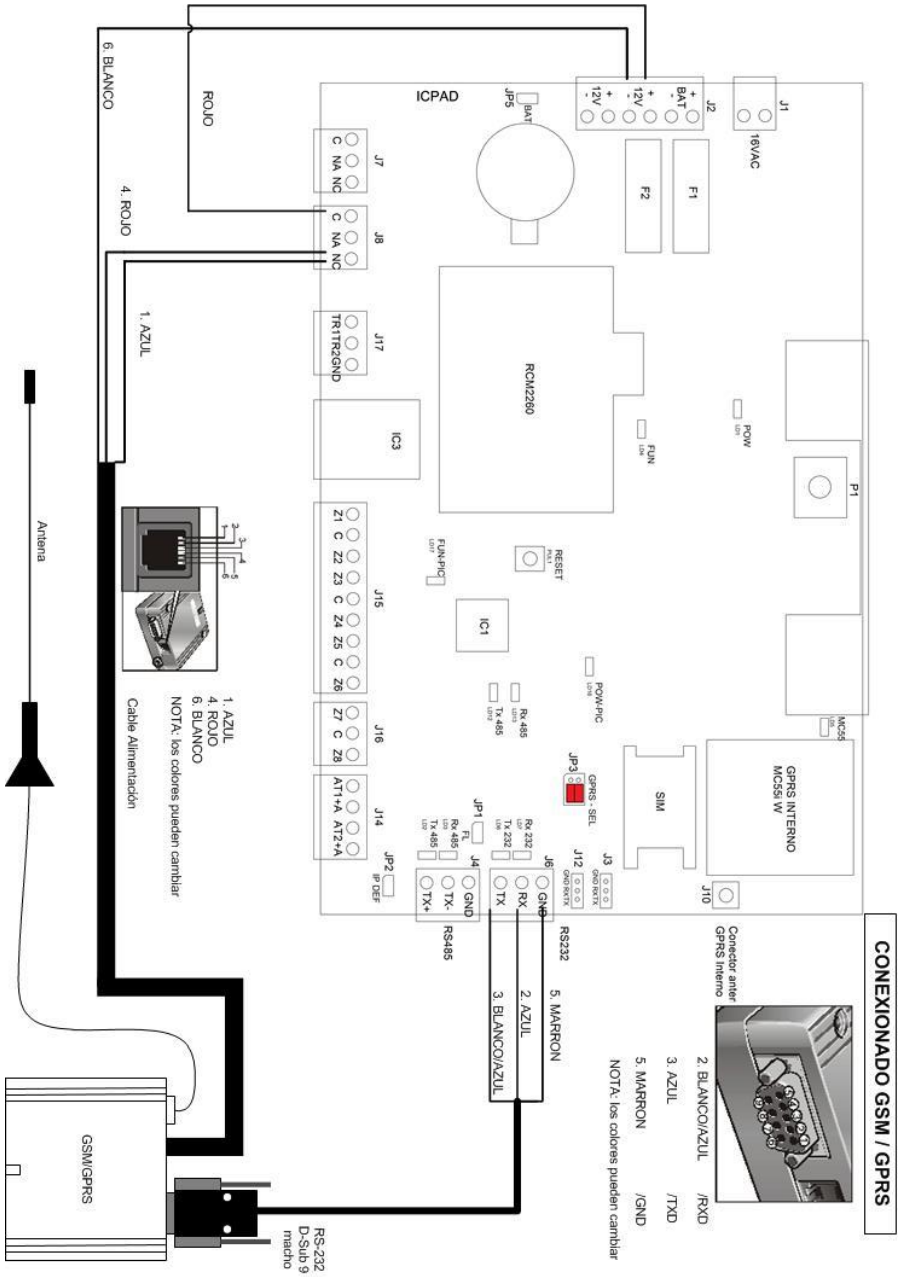
- El uso de parámetros técnicos, tales como gas o fuego no están cubiertos por la norma, aunque no suponen la pérdida del Grado 4 si su uso no interfiere en el resto de funciones del sistema.
- El uso del modem/GPRS externo no está incluido en la configuración certificada como Grado 4.
- El estándar no permite que los teclados muestren el estado del sistema (armado/desarmado) de la instalación de forma permanente.
- El estándar indica que la señalización acústica de los teclados es necesaria.
- El Grado 4 solo está garantizado si se utilizan comunicaciones RS485 cifradas.

10.2 PARÁMETROS TÉCNICOS

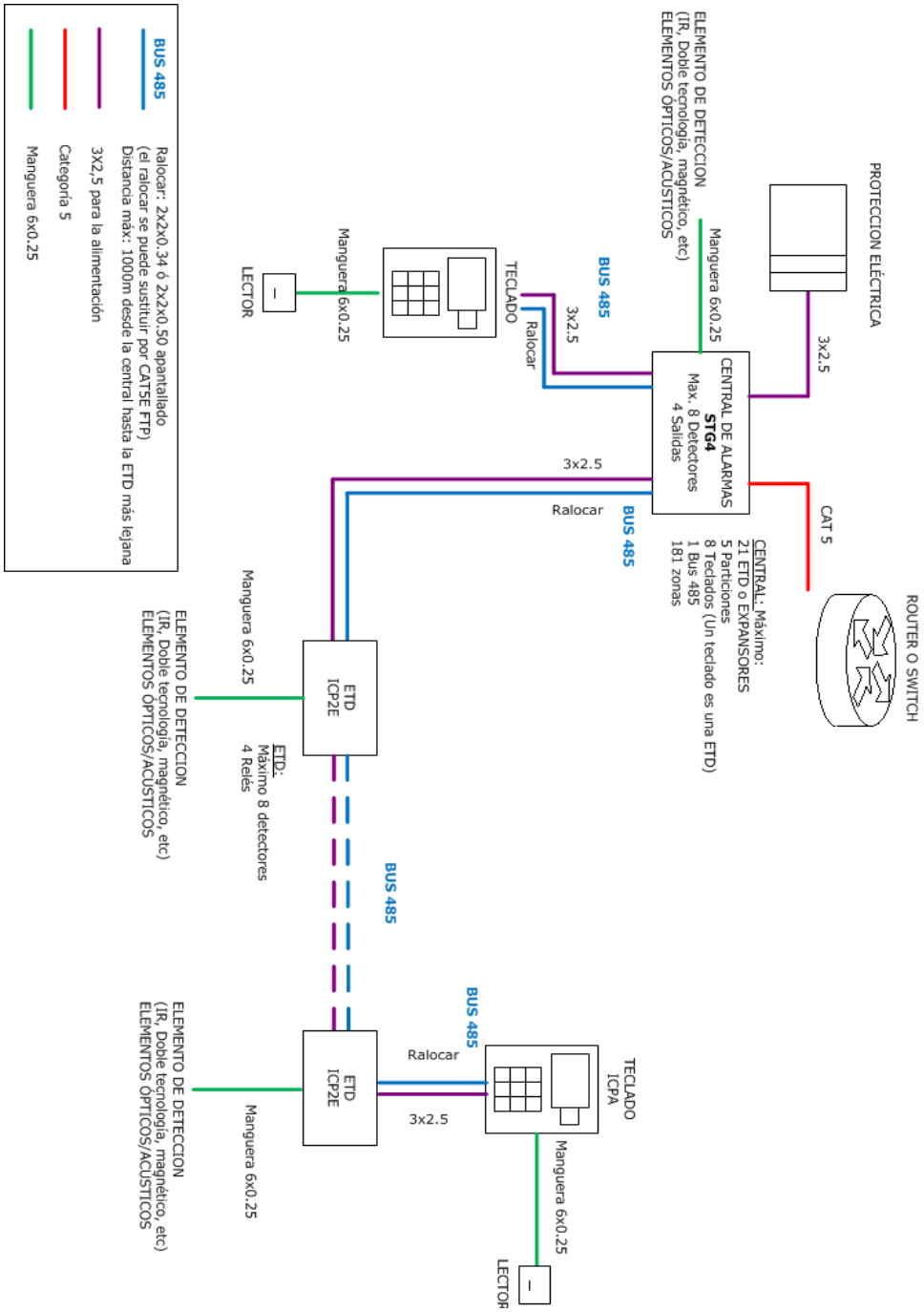
El uso de los parámetros técnicos no está cubierto por la norma, aunque se permite su uso y este no anula la certificación mientras no interfieran en ninguna de las otras funciones del sistema. A continuación se da una lista de todos estos parámetros:

- Fuego
- Emergencia Médica
- Emergencia personal
- Inactividad de anciano
- Alarma general
- Alerta de mantenimiento
- Avería sistema
- Sistema calefacción
- Inundación
- Detector de humo
- Combustión
- Alta temperatura
- Baja temperatura
- Fuego supervisado
- Avería de fuego
- Fallo bomba
- Bajo CO2
- Refrigeración
- Gas detectado
- Modo test andando

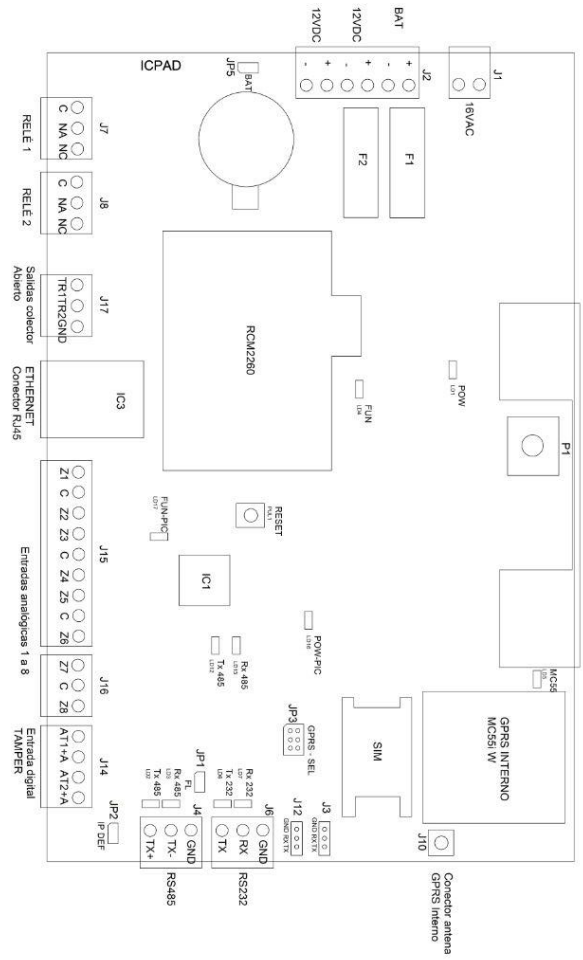
10.3 CONEXIONADO GSM/GPRS EXTERNO



10.4 EJEMPLO INSTALACION ATENEA G4



10.5 CONFIGURACIÓN PUENTES ATENEA G4



CONFIGURACIÓN DE PUENTES:

JP3 GPRS - SEL
(1-2) y (5-6) SELECCIÓN MODEM INTERNO

JP3 GPRS - SEL
(2-3) y (4-5) SELECCIÓN MODEM EXTERNO
CLEMA J6 HABILITADA

JP2 IP DEF
FUNCIONAMIENTO EN MODO IP POR DEFECTO

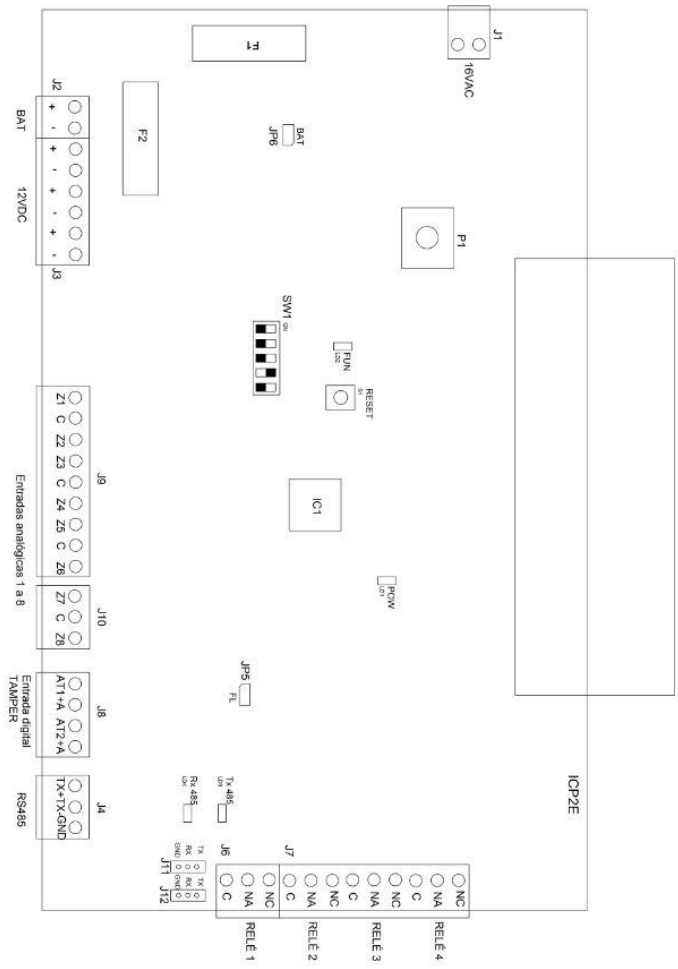
JP1 FL
HABILITACIÓN DE LA RESISTENCIA FINAL DE LÍNEA

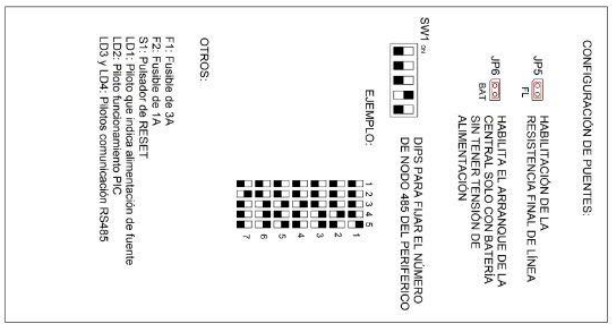
JP5 BAT
HABILITA EL ARRANQUE DE LA CENTRAL SOLO CON BATERÍA SIN TENER TENSIÓN DE ALIMENTACIÓN

OTROS:

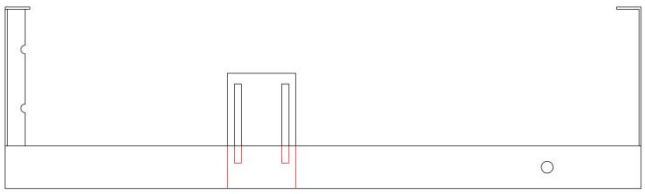
F1: Fusible de 3A
F2: Fusible de 1A
PUL1: Pulsador de RESET
LD1: Piloto que indica alimentación de fuente
LD3 y LD2: Pilotos comunicación RS485
LD4: Piloto funcionamiento ROM2260
LD5 (MC55):Piloto funcionamiento MC55i-W (GPRS/GSM)
LD6 y LD7: Pilotos comunicación RS232
LD13 y LD12: Pilotos comunicación RS485 PIC Central (ETD 0)
LD16: Piloto que indica alimentación ETD 0
LD17: Piloto funcionamiento PIC Central (ETD 0)

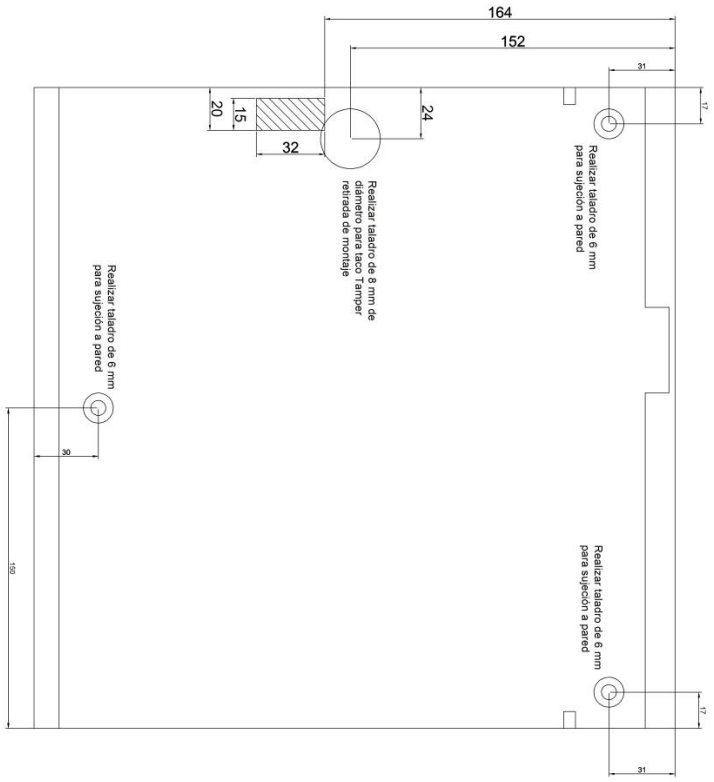
10.6 CONFIGURACIÓN PUENTES ICP2E-G4



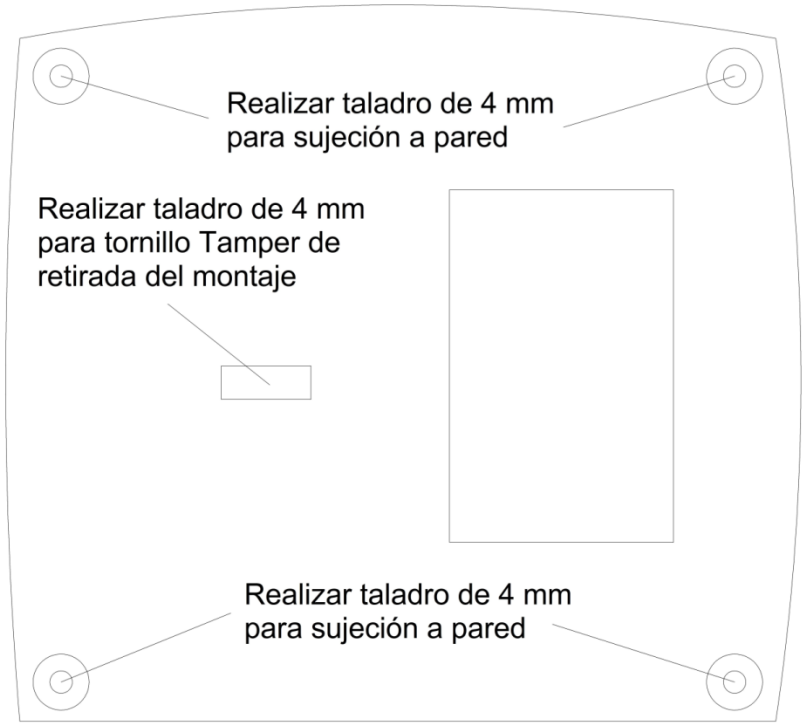


10.7 TALADROS CENTRAL ATENEA G4 Y PERIFERICO ICP2E-G4





10.8 TALADROS TECLADO ICPA



10.9 . NIVELES DE ACCESO

De acuerdo con la norma EN50131-3:2009 hay 4 niveles de acceso de usuarios, clasificando por categorías la capacidad de los usuarios para acceder a los componentes y funciones del sistema.

Nivel 1: Acceso para cualquier persona.

Nivel 2: Acceso para un operador.

Nivel 3: Acceso para un operador maestro o para el personal de la empresa de seguridad.

Nivel 4: Acceso para los fabricantes del equipo.

Nivel 2:

Un usuario de nivel 2 puede armar y desarmar el sistema, resetearlo, verificar sus funciones, inhibir zonas, modificar su propio código y borrar el código de cualquier otro usuario de nivel 2. Puede además anular algunas condiciones de las que impiden armar el sistema, tales como:

- Zona de robo o atraco abierta.
- Detector enmascarado o con reducción de alcance.
- Detector con fallo sensor.
- Fallo de alimentación principal.

Las alertas originadas por eventos tipo Tamper, FALLO COM. CON ETDS, COM. 485 o Fallo Batería, no pueden ser restauradas por usuarios de nivel 2, solo podrán hacerlo usuarios de nivel 3.

Nivel 3 (operador maestro):

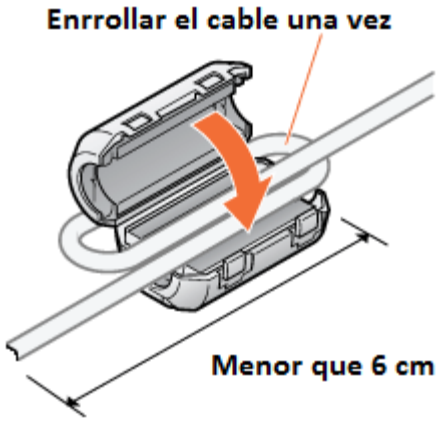
Un usuario de nivel 3 (operador maestro) tiene acceso a las mismas funciones que un usuario de nivel 2, pero además puede anular cualquiera de las condiciones que impidan realizar el armado del Sistema y puede restaurar todas las alertas.

Nivel 3 (servicio técnico):

Un usuario de nivel 3 (servicio técnico) puede acceder a las funciones de verificación del sistema y puede además modificar su configuración y programación. Para que este tipo de usuarios pueda acceder a sus funciones, previamente deberá haber sido autorizado por un usuario de nivel 2 o por un usuario de nivel 3 del tipo operador maestro.

10.10 INSTALACIÓN DE LA FERRITA:

La instalación de la ferrita (Z 119Ω or Z 89Ω) en el bus ha de hacerse tal y como se muestra en la siguiente figura:



La ferrita ha de instalarse en cada entrada/salida de bus. Si se tiene más de una salida de bus en el mismo equipo, se ha de instalar una ferrita en cada salida de bus adicional.

Ejemplo: