Guía de Seguridad en Protocolos Industriales
Smart Grid

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
incibe cert_

Mayo 2020

INCIBE-CERT_GUIA_PROTOCOLOS_SMART_GRID_2017_v2

La presente publicación pertenece a INCIBE (Instituto Nacional de Ciberseguridad) y está bajo una licencia Reconocimiento-No comercial 3.0 España de Creative Commons. Por esta razón, está permitido copiar, distribuir y comunicar públicamente esta obra bajo las siguientes condiciones:

- Reconocimiento. El contenido de este informe se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a INCIBE o INCIBE-CERT como a su sitio web: https://www.incibe.es/. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- Uso No Comercial. El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE-CERT como titular de los derechos de autor. Texto completo de la licencia: https://creativecommons.org/licenses/by-nc-sa/3.0/es/.

Índice

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. Sobre esta guía

Siguiendo con la línea del estudio publicado por INCIBE "*Protocolos y Seguridad de red en infraestructuras SCI*"[1], donde se ofrece una visión de los protocolos más representativos en sistemas de control, se presenta este documento que pretende profundizar en los protocolos utilizados en las redes inteligentes.

Este estudio, de carácter técnico, se centra en las comunicaciones de las redes inteligentes, y pretende ofrecer una visión sobre los protocolos más utilizados en España y Europa, mostrando sus funcionalidades, medidas de seguridad ofrecidas y problemas a los que se enfrentan. Así mismo, se indican una serie de recomendaciones en cada uno de ellos con el fin de mejorar la seguridad de las instalaciones que los tengan implementados.

[1] https://www.incibe-cert.es/guias-y-estudios/guias/protocolos-y-seguridad-sci

2. Introducción y situación actual

Desde hace unos años la red eléctrica está sufriendo una gran transformación promovida sobre todo a nivel europeo por el "objetivo 20-20-20"[2]. La base de la modificación de la red eléctrica surge con la comunicación COM (2006) 786 "On a European Programme for Critical Infrastructure Protection"[3] de la Comisión Europea, donde se definen los aspectos principales del programa europeo de protección de infraestructuras críticas (EPCIP, European Programme for Critical Infrastructures Protection); y tiene su punto álgido con la publicación por parte de Comisión Europea de la comunicación COM (2011) 202, "Smart Grids: from innovation to deployment"[4].

Este hecho también ha afectado a las comunicaciones, creando nuevas redes y apareciendo nuevos protocolos específicos para este sector. Ciertas tareas, ahora demandadas, requieren del uso de comunicaciones bidireccionales entre el tramo final de la distribución eléctrica, también llamado última milla, la cual abarca desde los centros de transformación hasta el contador situado en la casa/comunidad del cliente; y los centros de control, bien para pasarle información al cliente final, bien para gestionar la producción y demanda de energía, tal y como se puede ver en el esquema de la Figura 1.

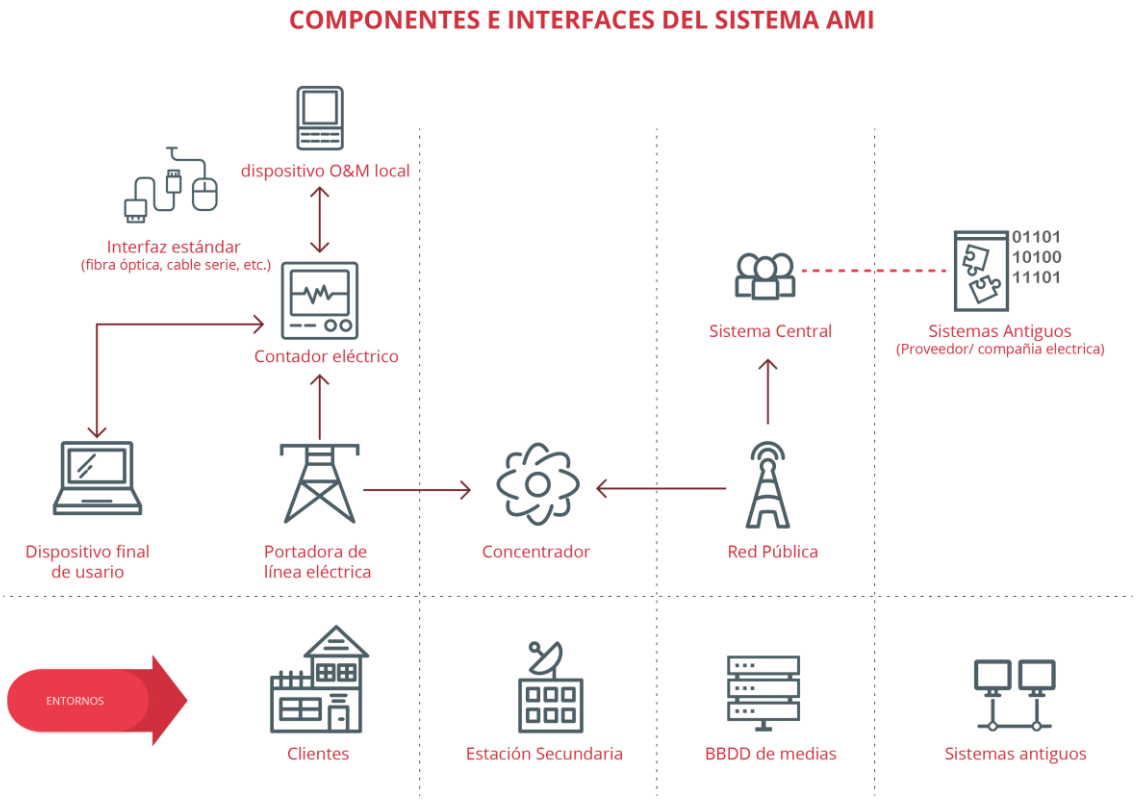

Figura 1 Componentes principales de la infraestructura de medida avanzada (AMI). Fuente: METERS AND MORE

[2] http://ec.europa.eu/clima/policies/strategies/2020/index_es.htm

[3] http://www.iserd.org.il/_Uploads/dbsAttachedFiles/com2006_0786en01.pdf

[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0202:FIN:EN:PDF

3. Protocolos y puntos de análisis

3.1. Protocolos a analizar

Gracias la unión y estandarización establecida entre distribuidores de energía, fabricantes y desarrolladores, la existencia de protocolos relacionados con las redes inteligentes no es tan profusa como en otros entornos de la industria. De entre los protocolos salidos de esta unión y estandarización se analizan aquellos cuyo uso es más común en el territorio español y aquellos que son usados ampliamente a lo largo del territorio europeo.

Los protocolos seleccionados son los siguientes:

- PRIME
- Meters and More
- DLMS/COSEM
- G3-PLC
- OSGP

3.2. Capas de actuación de los protocolos

Los protocolos de las redes industriales son de nueva generación en su mayoría, lo que implica una separación de funciones en su especificación que se ajustan con los niveles del esquema OSI, a diferencia de los antiguos protocolos de los sistemas de control que presentaban fronteras difusas.

A lo largo de este estudio se va a referenciar en varias ocasiones el modelo de capas definido en OSI para explicar con cuales de ellas interactúa cada protocolo. Los protocolos utilizados para el control de la distribución y el consumo eléctrico suelen tener más de una definición de la capa 1 o física, debido a la variedad de comunicaciones disponibles en los dispositivos.

3.3. Elementos de seguridad y recomendaciones

Para cada uno de los protocolos seleccionados se hace una descripción del mismo, indicando sus fortalezas y debilidades a nivel de seguridad. Para terminar, se exponen una serie de recomendaciones a aplicar para utilizar las mejores características de seguridad en cada uso del protocolo.

4. Análisis de los protocolos de comunicación en las redes inteligentes

4.1. PRIME

4.1.1. Descripción

PRIME (PoweRline Intelligent Metering Evolution) es un protocolo de nueva generación regido por la PRIME Alliance[5], que implementa los dos primeros niveles del modelo OSI, la capa física y la capa de enlace.

A nivel físico, PRIME utiliza la tecnología PLC (Power Line Communications)[6], originalmente en la banda CENELEN-A (3-95 KHz) pero se extiende a los 500 KHz en la última versión del estándar (PRIME Versión 1.4[7]), siempre utilizando una modulación OFDM (Multiplexación por División de Frecuencias Ortogonales)[8].

A nivel de enlace define una capa de acceso al medio donde conforma una estructura de red en árbol con dos tipos diferentes de nodos para la red, tal como muestra la Figura 2:

- Nodo base: Elemento correspondiente con la raíz del árbol y actúa como maestro de la comunicación. Solamente existe un nodo base en cada subred. Inicialmente él conforma toda la subred hasta que diferentes nodos de servicio se van asociando a la misma.
- Nodo de servicio: Elemento que se encuentra inicialmente en estado desconectado y necesita pasar un proceso de registro para unirse a la red. Los nodos de servicio tienen dos funciones: mantener la conexión en la subred para la capa de aplicación y hacer de enrutador de la conexión para los datos de otros nodos de servicio. Existen tres diferentes estados para un nodo de servicio:
  - Desconectado: El nodo no se encuentra conectado a la subred.
  - Terminal: El nodo se encuentra conectado a la subred pero no ejerce tareas de enrutamiento. Se comporta como un nodo hoja del árbol.
  - Switch: El nodo de servicio se encuentra conectado a la red y además realiza funciones de enrutamiento de la subred. Se comporta como un nodo rama del árbol.

[5] http://www.prime-alliance.org/

[6] http://es.wikipedia.org/wiki/Power_Line_Communications

[7] http://www.prime-alliance.org/wp-content/uploads/2014/10/PRIME-Spec_v1.4-20141031.pdf

[8] http://es.wikipedia.org/wiki/Acceso_m%C3%BAltiple_por_divisi%C3%B3n_de_frecuencias_ortogonales

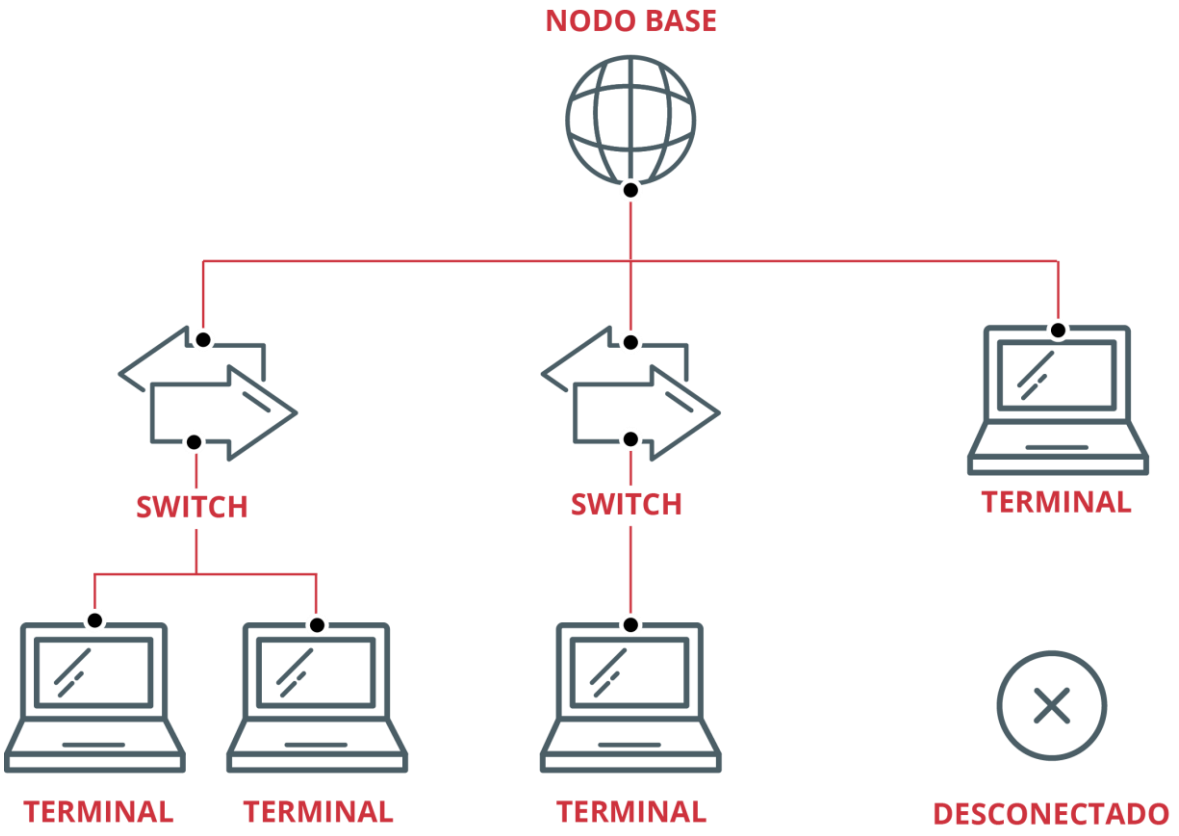

Figura 2. Topología PRIME

PRIME se utiliza principalmente en Europa, siendo España uno de los países con mayor implantación gracias a las compañías Iberdrola (principal fundador e impulsor de la alianza) y Gas Natural Fenosa, aunque su uso también se ha expandido a otras partes del mundo como puede verse en la Figura 3.

Figura 3. Área de uso del protocolo PRIME. Fuente: PRIME ALLIANCE

El despliegue de dispositivos con tecnología PRIME supera los 10 millones de equipos alrededor del mundo.

4.1.2. Seguridad

A nivel de seguridad, PRIME define 3 perfiles diferentes, a nivel de capa MAC o capa de nivel 2:

- Perfil de seguridad 0: no aporta cifrado y la protección queda relegada al nivel de seguridad que aporten las capas superiores.
- Perfil de seguridad 1 y 2: Aportan cifrado. El perfil 2 aparece con en la especificación 1.4 del protocolo y se diferencia del perfil 1 en que cifra más tipos de paquetes, basándose para ello en primitivas criptográficas y utilizando AES128.

  Las ventajas que aporta el cifrado son:

  - Confidencialidad, autenticidad e integridad de paquetes garantizada por el uso de un algoritmo de cifrado a nivel de capa de enlace.
  - Autenticación garantizada porque cada nodo posee su propia clave única, conocida solo por el propio nodo y el nodo base, y que se establece en la fabricación del dispositivo.
  - Prevención de ataques por repetición mediante el uso de un campo de 4 bytes para el contador de paquetes.

Los mecanismos de seguridad propuestos en los perfiles de seguridad no protegen frente a ataques al medio (ataques temporizados, ataques eléctricos o electromagnéticos, ruido en el canal, etc.).

4.1.3. Recomendaciones de seguridad

Las comunicaciones PRIME son accesibles a cualquier usuario con acceso a la red eléctrica en la que se encuentran los dispositivos que utilizan este protocolo.

Para proteger las comunicaciones usando el protocolo PRIME es aconsejable utilizar el perfil de seguridad 2, ya que aportan cifrado. Hay que tener en cuenta que PRIME solo actúa en los niveles inferiores del modelo OSI y el protocolo que se utilice en los niveles superiores puede ya aportar seguridad a los mensajes, pudiendo en estos casos utilizar el perfil 0, asumiendo que la comunicación PRIME puede ser observada al no llevar cifrado aplicado.

El perfil de seguridad 0 sólo debería utilizarse en entornos totalmente controlados y donde no exista la posibilidad de acceso no autorizado; o donde los datos transmitidos sean de uso público y por lo tanto no sean críticos para sistema.

4.2. Meters and More

4.2.1. Descripción

Meters and More[9] es la evolución del protocolo propietario de telegestión de la compañía energética italiana ENEL, que se ha desplegado en España gracias a su compra de la compañía ENDESA. Actualmente se ha creado una alianza para promocionar el uso del protocolo de forma abierta con otros competidores y fabricantes.

El protocolo *Meters and More* cubre la pila completa del modelo OSI, desde el nivel físico hasta el de aplicación, permitiendo su utilización sobre diversos medios de transmisión:

- Perfil PLC. Para la comunicación entre los contadores inteligentes y los concentradores.

[9] http://www.metersandmore.com/

- Perfil IP. Para las comunicaciones a través de redes públicas entre el sistema central y el concentrador.
- Perfil IEC62056-21[10]. Para el acceso local a través del puerto óptico de comunicaciones.
- Perfil DLMS/COSEM (ver apartado 4.5). Para comunicaciones PLC realizando un intercambio de objetos COSEM, como alternativa al perfil PLC.

La Figura 4 muestra el diagrama de capas de cada una de las variantes del protocolo.

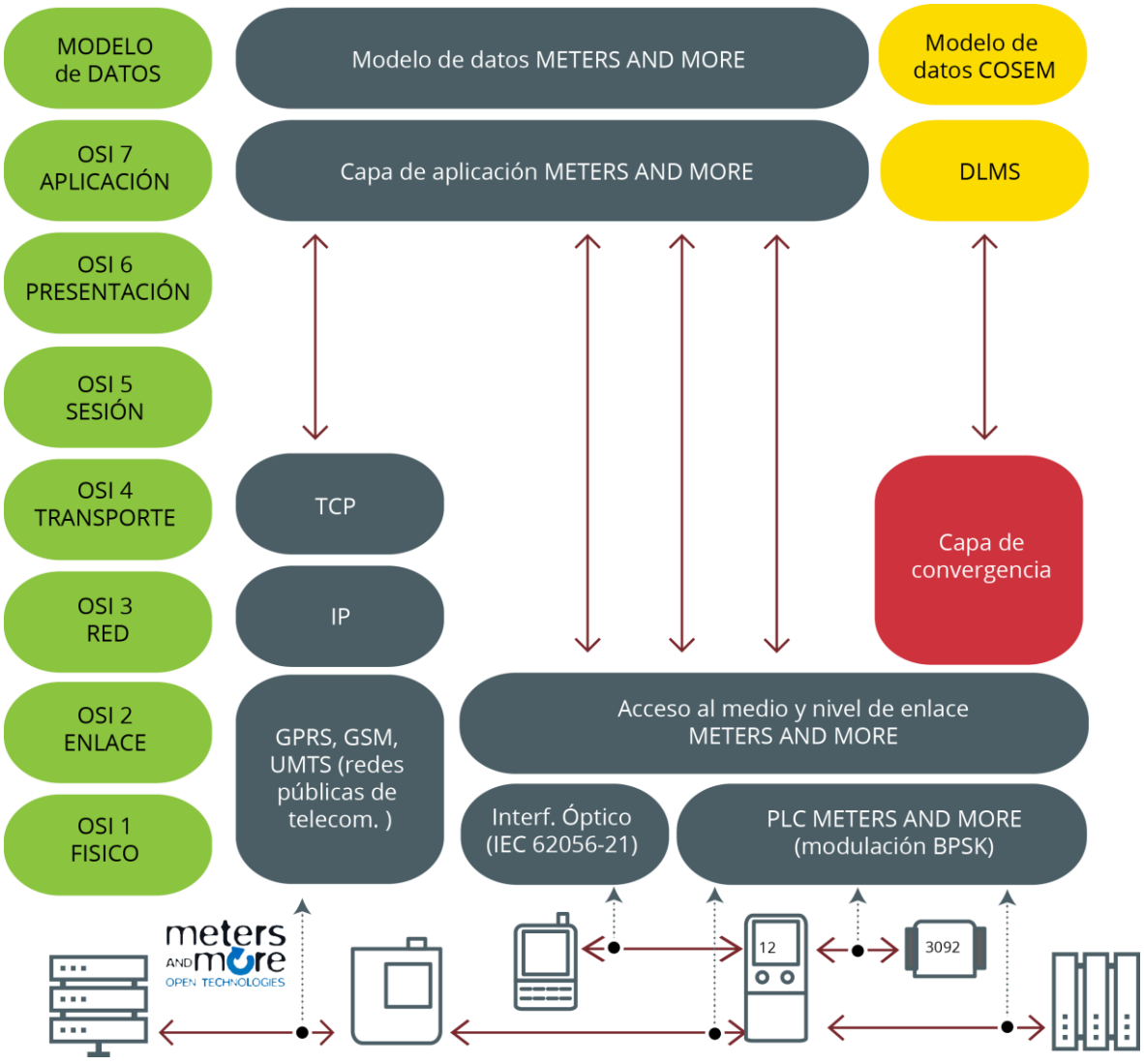

Figura 4. Arquitectura Meters and More. Fuente: Enginyers Industrials de Catalunya

En Italia ya existen más de 35 millones de dispositivos desplegados utilizando este protocolo y se espera que en España se instalen otros 15 millones antes de 2018 sólo en el ámbito de ENEL – ENDESA.

4.2.2. Seguridad

[10] http://en.wikipedia.org/wiki/IEC_62056

A nivel de seguridad, el protocolo *Meters and More* presenta las siguientes características dentro de la capa de acceso al medio o capa 2 del modelo OSI:

- Cifrado mediante claves AES de 128 bits.
- Autenticación en base a claves simétricas.
- Protección frente a ataques de retransmisión.
- Comprobación de integridad de mensaje.
- Claves individuales para cada contador, con control de acceso (lectura/escritura).
- Protección extremo-extremo.

Los mensajes se cifran y autentican mediante la misma clave.

4.2.3. Recomendaciones de seguridad

El protocolo *Meters and More* incorpora características de seguridad en su diseño, por lo que su utilización es recomendable siempre y cuando se utilicen dichas características de forma adecuada.

Centrándonos en la utilización conjunta de *Meters and More* con DLMS/COSEM, no se debe dejar toda la seguridad sobre este segundo protocolo y deben aplicarse también las medias de seguridad propias de *Meters and More*.

En entornos mixtos donde se utilicen de forma conjunta los protocolos comentados, es recomendable aplicar todas las medidas de seguridad propias de *Meters and More* a aquellas características de seguridad adicionales aportadas por DLMS/COSEM (ver apartado 4.5.2 y apartado 4.5.3).

4.3. G3-PLC

4.3.1. Descripción

G3-PLC[11] es un protocolo estándar internacional abierto desarrollado específicamente para las redes inteligentes por Sagem[12], ERDF[13] y Maxim[14]; que trabaja a baja frecuencia, por debajo de los 500 kHz, promoviendo la interoperabilidad entre los 10 kHz y los 490 kHz en su comunicación. Soporta diferentes modulaciones de OFDM y se trata de un protocolo con comunicación bidireccional, de gran fiabilidad. La especificación G3-PLC incluye las capas física y de enlace (MAC), donde se apoya en OFDM, y una capa de adaptación 6LoWPAN[15] para transmitir paquetes IPv6 por la red. Estas características hacen que este protocolo esté pensado para infraestructuras que poseen multitud de nodos a gran escala.

El protocolo está impulsado por el gestor de redes de distribución francés (ERDF).

Algunas de las características que posee este protocolo son las siguientes:

[11] http://www.g3-plc.com/

[12] http://www.sagem.com/

[13] http://www.erdf.fr/

[14] http://www.maximintegrated.com/

[15] https://es.wikipedia.org/wiki/6LoWPAN

- Robustez y amplio rango de frecuencias de comunicación que proporcionan una gran ventaja a la hora de instalar dispositivos inteligentes que envíen datos a los concentradores.
- Diseño que permite la comunicación punto a punto mediante IPv6.
- Utiliza las bandas definidas por CENELEC[16], FCC[17] y ARIB[18]:
    - La sección 15 de FCC define que la frecuencia de la banda para PLC en Norte América ha de estar entre 10 y 490 kHz.
    - ARIB define que la frecuencia de la banda para PLC en Asia ha de estar entre 10 y 450 kHz.
    - CENELEC EN50065-1 define el rango para bandas de baja frecuencia para PLC en Europa:

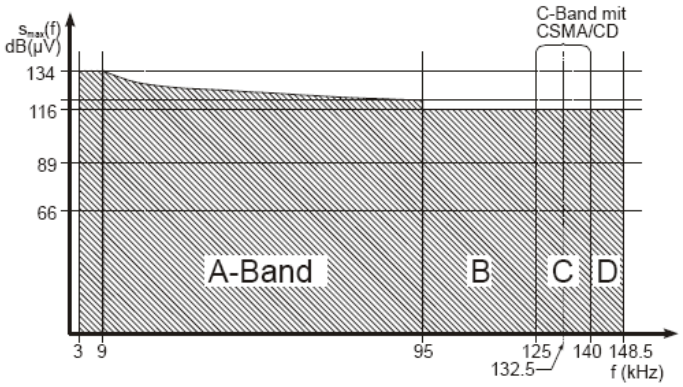

Figura 5. Bandas de frecuencia definidas por CENELEC.

        - Banda A (3-95 kHz): Las frecuencias en esta banda sólo se utilizan para la monitorización o control de la parte de baja tensión de la red de distribución, incluyendo la información de consumos energéticos de los equipos e instalaciones conectados.
        - Banda B (95-125 kHz): Puede usarse para todo tipo de aplicaciones.
        - Banda C (125-140 kHz): Para los sistemas de redes domésticas.
        - Banda D (140-148.5 kHz): específico para alarmas y sistemas de seguridad.
- Se trata de una tecnología nueva, pero comprometida con los ajustes y objetivos finales que marca el “objetivo 20-20-20” a las redes inteligentes.

Para poder entender el funcionamiento del protocolo G3-PLC en profundidad, es necesario ver una descripción detallada de las capas donde se encuentra presente.

[16] http://www.cenelec.eu/

[17] https://www.fcc.gov/

[18] http://www.arib.or.jp/english/index.html

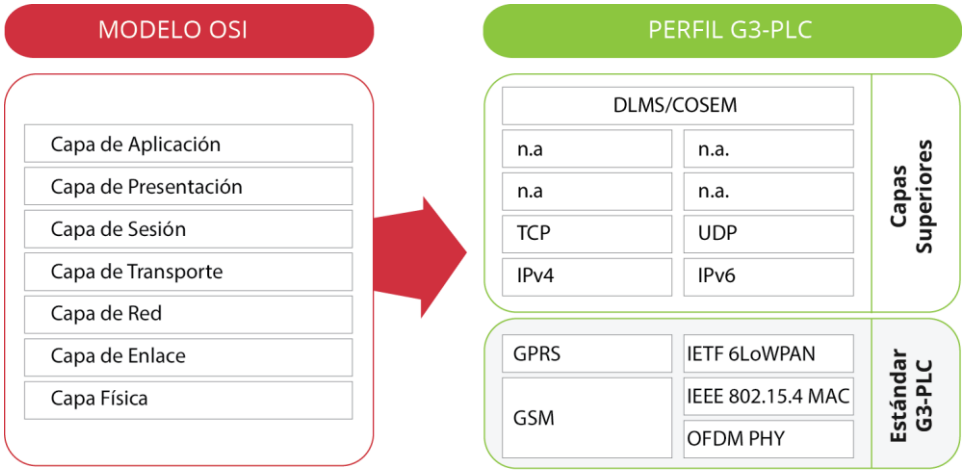

Figura 6. Muestra del protocolo G3-PLC y el modelo OSI

El encapsulamiento de los datos del protocolo G3-PLC a través de las diferentes capas en las que posee presencia este protocolo, se resume en la Figura 7.

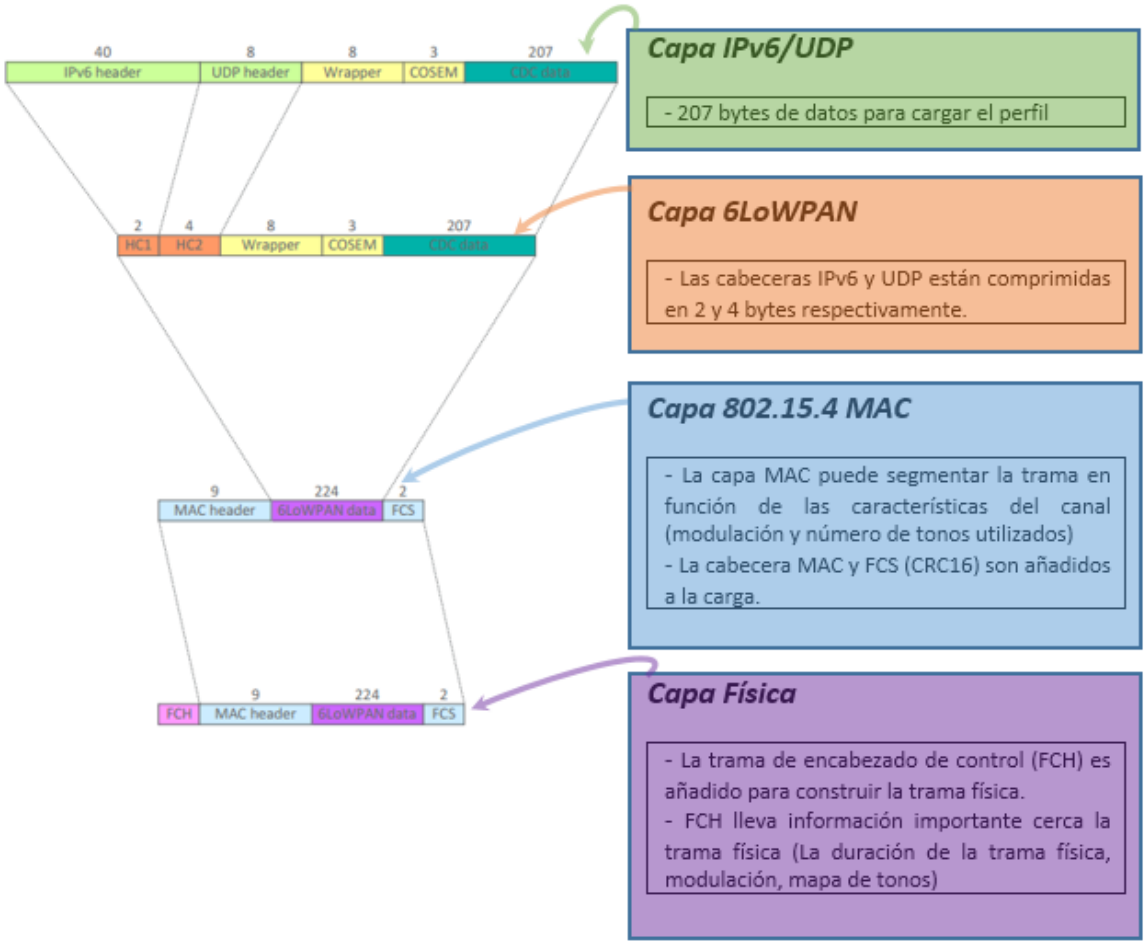

Figura 7. Viaje de los datos en el protocolo 3G-PLC.

El mapa de la Figura 8, muestra los países que usan actualmente el protocolo G3-PLC y los órganos que regulan las frecuencias a las que pueden trabajar los dispositivos que

implementen este protocolo en cada zona. Se espera que para el año 2018 están implantados 35 millones de dispositivos usando este protocolo sólo en Francia.

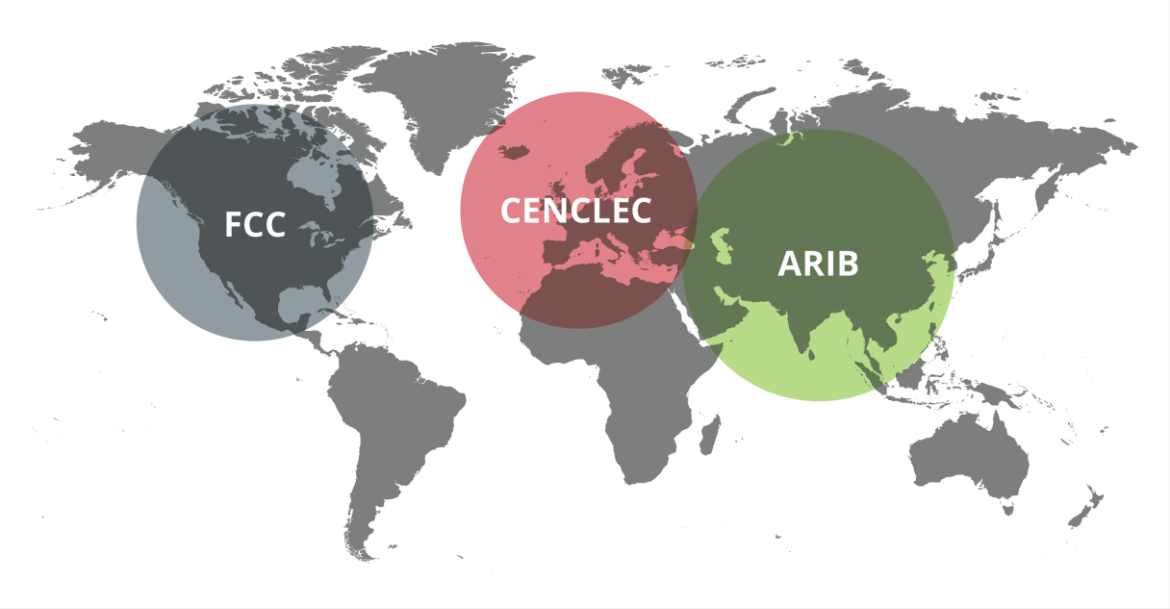

Figura 8. Zonas donde se utiliza el protocolo G3-PLC. Fuente: G3-PLC Alliance

4.3.2. Seguridad

El método G3-PLC adoptado para la implementación de la seguridad a nivel físico por G3-PLC consiste en un cifrado AES-128 a nivel de capa de control de acceso al medio (MAC), correspondiente con la capa 2 del modelo OSI, que posee las siguientes características:

- Simplicidad: Se basa en una sola credencial (una clave de 128 bits pre-compartida) y un único algoritmo de cifrado (AES-128).
- Seguridad: Tiene un diseño bien conocido y mejorado de esquemas criptográficos.
- Extensibilidad: En el caso de OFDM sobre PLC, se puede ampliar fácilmente para apoyar la distribución de la clave de grupo.

La confidencialidad e integridad están asegurados a nivel de MAC. Como se define en IEEE 802.15.4, un tipo de cifrado CCM[19] se entrega a cada trama transmitida entre los nodos de la red. El modo de cifrado CCM es utilizado en la capa MAC, y previene de accesos indebidos de dispositivos a la red que realizan acciones maliciosas en la misma y en otros procesos de capas inferiores. Las tramas MAC se cifran y descifran en cada salto. Las únicas excepciones son algunas tramas en las primeras etapas del proceso de arranque[20]. Para apoyar este servicio, todos los nodos de la red reciben la misma clave de

[19] El cifrado CCM proporciona cifrado de datos mediante clave de 128 bits y un código de autenticación de mensaje (MAC) a modo de firma del paquete.

[20] https://es.wikipedia.org/wiki/Bootstrapping_(inform%C3%A1tica)

sesión de grupo (GMK). Esta GMK se distribuye de forma individual y de forma segura a cada nodo mediante el canal seguro EAP-PSK.

Por otra parte, G3-PLC presenta dos arquitecturas de autenticación diferentes:

- La función de servidor de autenticación esta soportada directamente por un LBS (LoWPAN BootStrapping Server)[21]. En este caso todo el material de autenticación (credenciales, listas de acceso, etc.) se debe cargar en los LBS. El LBS contiene toda la información base de cada uno de los dispositivos activos.
- El servidor de autenticación está soportado por un servidor AAA (autenticación, autorización y contabilización) remoto. En este caso, el LBS sólo es responsable de la transmisión de los mensajes EAP al servidor AAA través de un protocolo AAA estándar como es RADIUS[22].

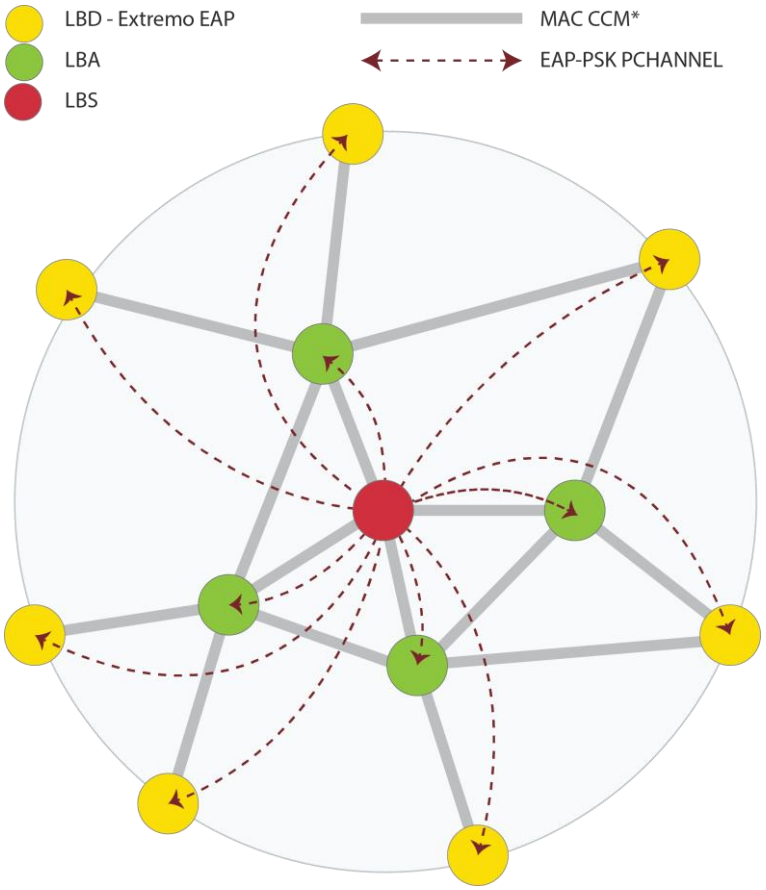

Figura 9. Confidencialidad y seguridad gracias a la comunicación cifrada en G3-PLC. Fuente: Enedis

4.3.3. Recomendaciones de seguridad

Como protocolo de comunicaciones, G3-PLC no dispone de opciones de seguridad que puedan ser habilitadas/deshabilitadas o configuradas según las necesidades. Todas las medidas están siempre activadas para su uso. La única opción parametrizable es la autenticación, donde se recomienda usar el protocolo RADIUS para establecer la autenticación entre el cliente y el servidor AAA.

[21] https://tools.ietf.org/html/draft-daniel-6lowpan-commissioning-02

[22] https://tools.ietf.org/html/rfc2865

Fuera del propio protocolo se recomienda realizar un correcto filtrado de la información que llega a través de las redes PLC.

Como G3-PLC solo implementa los niveles bajos del modelo OSI se debe utilizar algún otro protocolo en los niveles superiores. Estos protocolos de niveles superiores también deben tener habilitadas las características de seguridad que tengan disponible.

4.4. OSGP

4.4.1. Descripción

El protocolo abierto de Smart Grid (OSGP) se aplica actualmente en varios países en proyectos de *Smart Metering* a gran escala. Fue desarrollado por OSGP Alliance[23] y publicado como un estándar por el Instituto Europeo de Estándares y Telecomunicaciones (ETSI). Es uno de los protocolos más utilizados y probados en el campo de los contadores y redes inteligentes y en la actualidad existen más de 100 millones de dispositivos que lo soportan desplegados por todo el mundo.

OSGP sigue un enfoque moderno basado en el modelo OSI y la frecuencia a la que trabajan los dispositivos que lo utilizan se encuentra en un rango entre 9 kHz y 95 kHz. OSGP especifica una capa de control independiente del medio para la comunicación segura entre medidores y nodos de control.

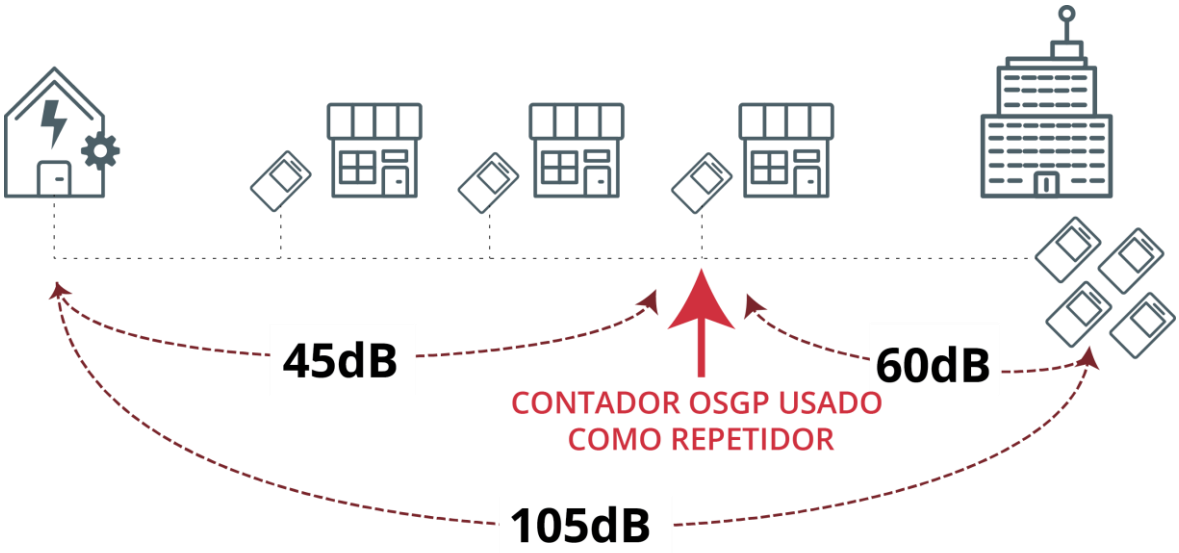

Figura 10. Intensidades a las que trabajan los dispositivos que usan el protocolo OSGP. Fuente: ESNA

OSGP se basa en los siguientes estándares abiertos:

- ETSI TS 104 001 (Capa de aplicación).
- ISO/IEC 14908-1 (Capa de transporte).
- ETSI TS 103 908 (Capa física).

4.4.2. Seguridad

[23] http://www.osgp.org/

El protocolo OSGP requiere que se utilice un protocolo de seguridad de transporte obligatorio llamado OSGP-AES-128-PSK o, abreviado, OSGP-AES. Esto significa que no es posible deshabilitar la seguridad.

El OSGP-AES proporciona un canal de comunicación bidireccional protegido entre un cliente (por ejemplo, un concentrador de datos) y un contador. El canal seguro garantiza la confidencialidad de los datos, a través del cifrado AES-128-CCM, integridad de datos y origen, a través de la autenticación, y protección frente al ataque de repetición mediante números secuenciales. El OSGP-AES asegura los mensajes, tanto *unicast*, como *broadcast*.

Todos los mensajes OSGP se envían dentro del canal seguro establecido por el OSGP-AES. Entre ellos, se incluye la lectura de datos de contadores personales, como el consumo de energía, así como funciones críticas de seguridad, como cambiar la configuración del contador. No hay excepciones, todas las comunicaciones están protegidas y todos los mensajes intercambiados se someten a cifrado, autenticación mutua y protección ante ataques de repetición. Esto contrasta con DLMS y otros estándares que permiten que se deshabiliten o se disminuyan las propiedades de seguridad, dando lugar a configuraciones inseguras.

El OSGP-AES está diseñado para un uso en claves únicas de dispositivo. Esto significa que si la clave de un contador se ve comprometida, las otras claves siguen siendo seguras.

El OSGP-AES está específicamente diseñado para redes limitadas de dispositivos integrados de baja gama y antiguos. Su uso principal es en redes de comunicaciones mediante líneas de potencia (PLC, por sus siglas en inglés). Por lo tanto, proporciona un alto rendimiento, a la vez que mantiene la seguridad.

Como ocurre con el resto de los OSGP, la especificación del protocolo de seguridad OSGP-AES es abierta, estandarizada y de acceso libre. El protocolo de seguridad OSGP-AES fue sometido a una revisión independiente de un tercero por parte de un experto en seguridad. El informe que se obtuvo, que puede solicitarse contactando con el OSGP Alliance, concluyó que:

En general, el protocolo es seguro, está bien diseñado y se basa en primitivas criptográficas establecidas (AES, CMAC y CCM) con parámetros razonables. Estas primitivas criptográficas se usan de modos que no deberían dar lugar a los ataques actualmente conocidos.

El protocolo OSGP también incluye un protocolo de seguridad más antiguo denominado OSGP-RC4.

No obstante, en 2015, el OSGP Alliance estableció que el OSGP-RC4 estaba obsoleto, ya que contenía numerosos problemas de seguridad.

4.4.3. Recomendaciones de seguridad

El OSGP Alliance recomienda utilizar siempre el OSGP-AES como protocolo de seguridad OSGP. El OSGP-AES tiene los mismos requisitos de recursos de hardware y de red y cuenta con un rendimiento de comunicación comparable al antiguo y obsoleto protocolo de seguridad. De hecho, el OSGP-AES es en algunos casos más rápido, lo que significa que no hay limitaciones de rendimiento para utilizarlo.

Todas las primitivas criptográficas usadas por OSGP están estandarizadas y su uso está aprobado por organizaciones de normalización, entre las que se incluye el Instituto Nacional de Estándares y Tecnología Estadounidense. Específicamente, OSGP-AES utiliza las siguientes primitivas criptográficas.

- AES-128: la variante de clave de 128 bits del algoritmo de cifrado por bloques simétricos con autorización FIPS, tal como se especifica en el FIPS PUB 197.
- CCM: contador con CBC-MAC (CCM) según se especifica en la Publicación Especial NIST 800-38C.
- CMAC: código de autenticación de mensaje basado en cifras (CMAC) según se especifica en la Publicación Especial NIST 800-38B.

Como es imposible desactivar la seguridad, garantiza la confianza de que el cifrado y la autenticación proporcionan la protección de la privacidad y la seguridad necesarias para las comunicaciones de la red inteligente.

4.5. DLMS/COSEM

4.5.1. Descripción

DLMS/COSEM[24] es un protocolo de nivel de aplicación que define desde la capa 4 hasta la capa 7 del modelo OSI. El significado de las siglas que dan nombre al protocolo es el siguiente

- DLMS: "*Device Language Message Specification*", un concepto generalizado para un modelo abstracto de entidades de comunicación.
- COSEM: "*COmpanion Specification for Energy Metering*", fija las reglas, basadas en estándares, para el intercambio de información con los contadores de energía.

Este protocolo está regulado por la norma IEC 62056[25].

[24] http://www.dlms.com/

[25] http://www.dlms.com/documentation/dlmscosemspecification/iecstandardsforelectricitymetering.html

Figura 11. Modelo de capas de DLMS/COSEM

El protocolo DLMS/COSEM se desarrolló para ser utilizado conjuntamente al protocolo PRIME, el cual actúa en los niveles inferiores del modelo OSI, o a protocolos de nivel de red (IPv4/IPv6). De esta forma se permiten comunicaciones con dispositivos de bajo nivel, como los contadores inteligentes, y las comunicaciones con sistemas con más recursos, como los equipos de los centros de control. También es posible utilizar este protocolo conjuntamente con el protocolo "Meters and More".

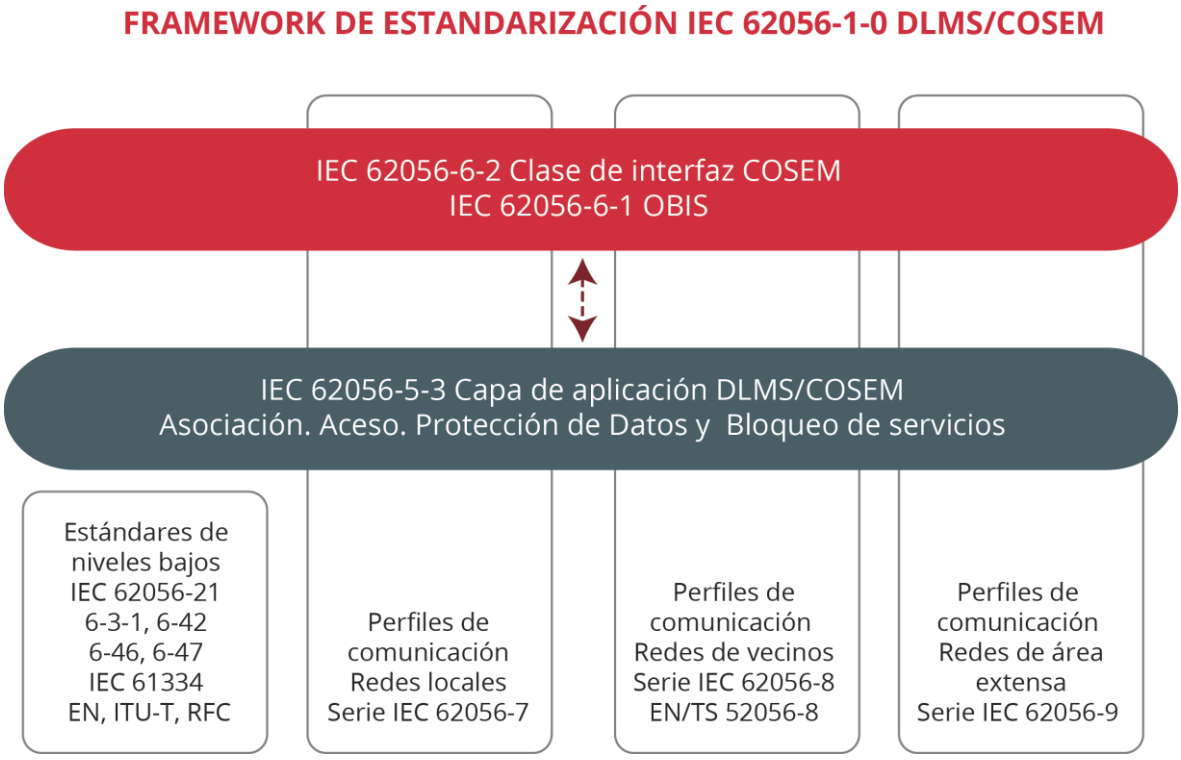

Figura 12. Arquitectura DLMS/COSEM. Fuente: DLMS

4.5.2. Seguridad

La seguridad en el protocolo DLMS/COSEM se clasifica en tres niveles de seguridad diferentes:

- *Lowest level security*: Este nivel no aporta ningún tipo de seguridad a la comunicación DLMS/COSEM.
- *Low Level security*: La seguridad de la comunicación DLMS/COSEM está basada en el uso de credenciales. El cliente ha de disponer de una contraseña para poder realizar la comunicación.
- *High Level security*: Es el máximo nivel de seguridad permitido. El cliente y el servidor han de realizar un método de autenticación mutua utilizando un proceso de cuatro pasos.

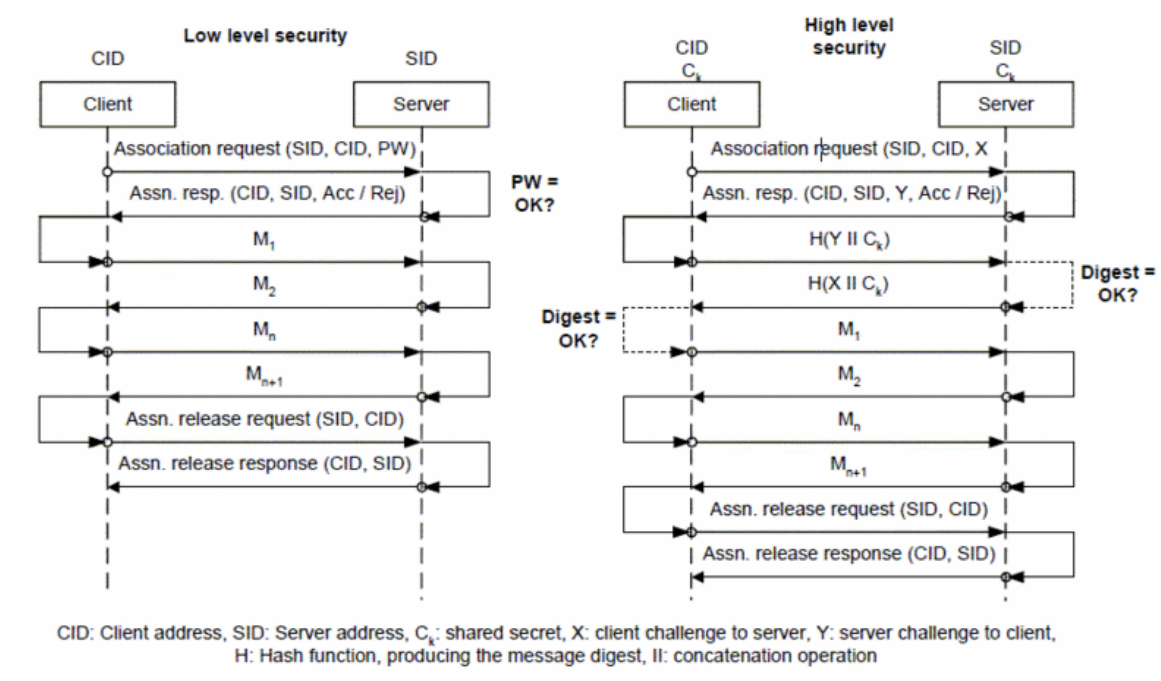

Figura 13. Autenticación en DLMS/COSEM

El contexto de seguridad define atributos de seguridad relevantes para transformaciones criptográficas e incluye los siguientes elementos:

- Suite de seguridad: Determina el algoritmo de seguridad utilizado y el uso de cifrado (AES 128).
- Política de seguridad: Determina el tipo de protección que es aplicado a los paquetes del protocolo.
- Material de seguridad: Es información relevante para el algoritmo de seguridad, incluye claves de seguridad, vectores de inicialización, certificados de clave pública, etc. El material de seguridad es específico para cada algoritmo.

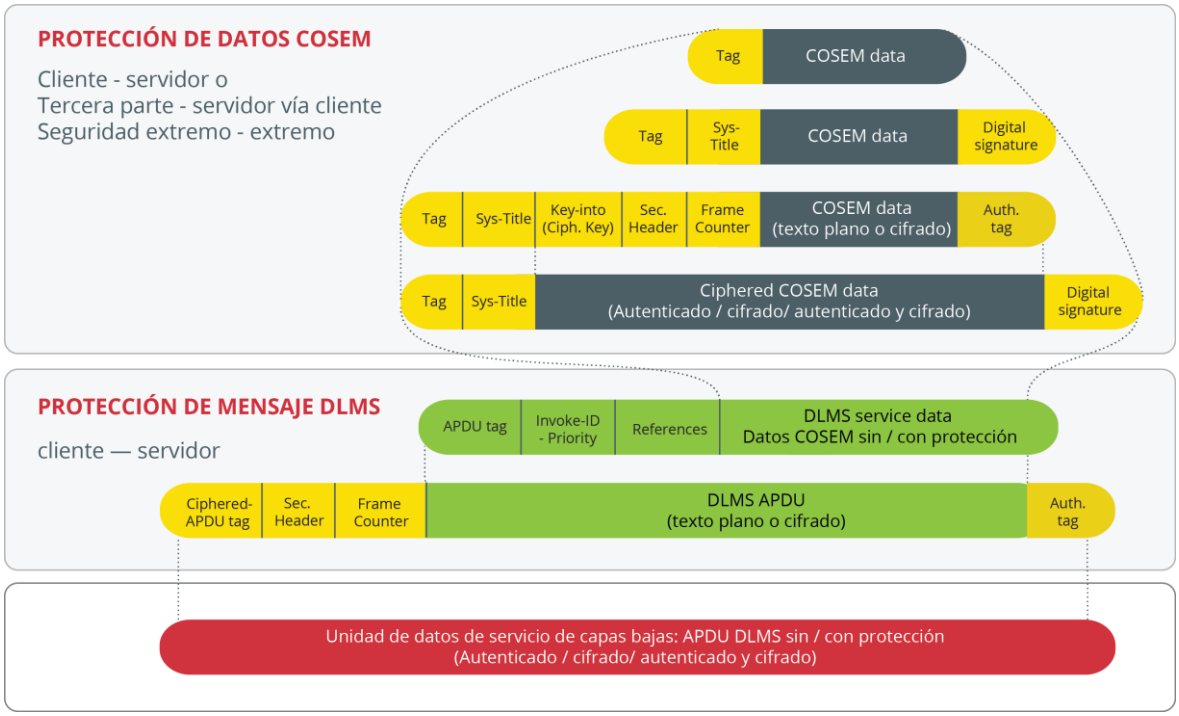

Figura 14. Seguridad en los paquetes DLMS/COSEM. Fuente: DLMS

4.5.3. Recomendaciones de seguridad

El protocolo DLMS/COSEM es un protocolo de alto nivel con presencia en la capa de aplicación. Este hecho permite el uso de otros protocolos para reforzar la seguridad en capas inferiores donde existe un transporte de datos (cifrado), lo que a su vez aporta un nivel extra de seguridad no presente en otros protocolos. Además, al poder utilizar diferentes protocolos en los niveles inferiores, que pueden o no tener activadas algunas funciones de seguridad, para proteger el envío de información entre cliente y servidor independientemente del medio utilizado.

Siempre que sea posible es recomendable utilizar el perfil "*High Level security*", el nivel más alto de seguridad que proporciona el protocolo. Además, para añadir mayor nivel de seguridad se recomienda la utilización de certificados digitales junto a una infraestructura de PKI para realizar la autenticación de los dispositivos en la comunicación.

Cuando se utiliza DLMS/COSEM sobre TCP/IP es posible utilizar herramientas de comunicaciones de seguridad como cortafuegos y dispositivos IDS/IPS. El puerto utilizado por defecto es el 4059, por lo que es recomendable monitorizar el tráfico asociado con dicho puerto.

4.6. IEEE 1901

4.6.1. Descripción

La norma IEEE 1901-2010 define un estándar de comunicación de alta velocidad, hasta 500 Mb/s en la capa física, de banda ancha a través de líneas eléctricas (*Broadband over Power Lines*, BPL). Este estándar utiliza frecuencias de transmisión por debajo de 100 MHz. Todos los tipos de dispositivos BPL pueden usar este estándar, incluso los que se

usan para conexiones a menos de 1500 metros de las instalaciones a los servicios de acceso a Internet. El estándar define las capas físicas (PHY) y de enlace (MAC).

El estándar IEEE 1901 puede incluir dos capas físicas diferentes, ambas basadas en la modulación mediante multiplexación por división de frecuencia ortogonal (*Orthogonal Frequency-Division Multiplexing*, OFDM): una es FFT (*Fast Fourier Transform*) OFDM, y la otra es Waveet OFDM. Cada capa física es opcional, por lo que no es obligatorio implementar ambas especificaciones simultáneamente. FFT se deriva de la tecnología HomePlug AV y se implementa en productos basados en HomePlug, mientras que Wavelet se deriva de la tecnología HD-PLC (*High Definition - Power Line Comunication*) y se implementa en productos basados en esta tecnología.

En el modelo FFT OFDM, que permite el intercambio de datos a velocidades de hasta 400 Mbps con anchos de banda de hasta 50 MHz, es necesario tener un intervalo de guardia para asegurarse de que no interfieren las diferentes transmisiones, y así conseguir mantener la ortogonalidad y redundancia. De esta manera, se consigue una rectificación de señal óptima en la transmisión.

La tecnología Wavelet OFDM proporciona una transmisión eficiente y puede coexistir con los sistemas existentes (emisiones de onda corta y de radioaficionados). La velocidad de la capa física es de aproximadamente 240 Mbps y se alcanza con un ancho de banda de 26 MHz. Además, se logran comunicaciones de alta calidad y confiabilidad, incluso en rutas de transmisión de energía doméstica, donde el medio físico es de mala calidad, mediante el uso de una codificación de corrección de errores sólida y un modo de diversidad.

En general, tanto FFT como Wavelet son muy parecidas en sus características, exceptuando algunos puntos:

- Prioridad de acceso, donde Wavelet tiene la prioridad más alta.
- En la seguridad, FFT puede usar DSNA/RSNA (asociación de redes de seguridad basada en dispositivos / asociación de redes de seguridad robusta) mientras que Wavelet usa PSNA/RSNA (asociación de redes de seguridad en pares / asociación de redes de seguridad robusta).
- Las operaciones en modo ráfaga pueden ser unidireccionales o bidireccionales en FFT, mientras que Wavelet no lo soporta.
- Utilizan acceso múltiple por detección de portadora y prevención de colisiones (CSMA/CA, *Carrier Sense Multiple Access with Collision Avoidance*) como esquema base de contención. También es posible la utilización de acceso múltiple por división de tiempo (TDMA, *Time Division Multiple Access*) como esquema libre de contención.

Característica y tecnología		IEEE 1901	
		FFT-PHY	Wavelet-PHY
Acceso al canal	Tecnología fundamental	CSMA/CA	
	Esquema base de contención	CSMA/CA	
	Prioridades de acceso	4	8
	Detección de portadora virtual	Sí	
	Esquema libre de contención	TDMA	
	Acceso persistente	Sí	
	Administración de acceso	Basado en Beacon	
Seguridad	Marco de seguridad	DNSA/RSNA	PNSA/RSNA
	Protocolo de cifrado	CCMP	
Operación en modo ráfaga	Operación en modo ráfaga	Uni/bidireccional	No soportado
Esquema de direcciones	Modos	Unicast, multicast y broadcast	
	Espacio (por dominio)	8 bit	
Tramas	Agregación, fragmentación y reensamblado	Soportado	

Figura 15. Comparativa entre las dos versiones de capa física de IEEE 1901. Fuente: ResearchGate[26].

4.6.2. Seguridad

A nivel de seguridad, el protocolo IEEE 1901 presenta las siguientes características dentro de la capa de enlace:

- Cifrado mediante claves AES de 128 bits.
- Protección extremo-extremo.
- Control de acceso.

El estándar IEEE 1901 utiliza el marco de seguridad en IEEE 802.1X, junto con el protocolo CCMP (encadenamiento de bloques de cifrado de MAC en modo contador). El grupo de trabajo del IEEE 1901 se basó en el estándar 802.11[27] para la seguridad en redes inalámbricas, que se basa en el concepto de RSNA que se encuentra en 802.1X y CCMP. La RSNA define una serie de características de seguridad:

- Mecanismos de autenticación mejorados para estaciones.
- Un conjunto de algoritmos de gestión de claves.
- Establecimiento de claves criptográficas.

[26] Medium Access Control for Power Line Communications: An Overview of the IEEE 1901 and ITU-T G.hn Standards

[27] https://standards.ieee.org/standard/802_11-2016.html

- Mecanismo de encapsulado criptográfico de datos mejorado, llamado modo contador con CCMP.

4.6.3. Recomendaciones de seguridad

La seguridad de IEEE 1901 se basa en el marco IEEE 802.1X de forma general, utilizando el estándar IEEE 802.1i sobre seguridad en redes inalámbricas como pilar principal.

El estándar IEEE 1901 incorpora características de seguridad en la capa 2 del modelo OSI, incluyendo cifrado y mecanismos de autenticación, que deberían utilizarse en todos los escenarios en los que sea posible. También implementa una serie de recomendaciones adicionales, recogidas en varios informes de la ITU (*International Telecommunication Union*), donde se especifican varios consejos de seguridad en la capa 2 del modelo OSI, como son el cifrado, la autenticación y procedimientos de gestión de claves.

Además, como medida adicional de protección, utiliza el estándar IEEE 802.11 de seguridad, que es específico para las capas de enlace y física. De esta forma, la seguridad del mismo no solo depende del propio protocolo IEEE 1901. Entre las características de seguridad que aporta IEEE 802.11 se encuentra el control de autenticación y codificación o identificación de dispositivos en la red.

5. Cuadro comparativo resumen

	Protocolo	PRIME	DLMS/COSEM	Meters and More	G3-PLC	OSGP	IEEE 1901
Aspectos generales	Tipo de estándar	Abierto	Abierto	Propietario	Abierto	Abierto	Abierto
	Medio de transmisión	PLC	Ethernet	PLC Ethernet Serie	PLC Ethernet	PLC Ethernet	PLC Ethernet
	Región de uso	España	España	Italia España	Francia	Norte de Europa	España
	Compatibilidad	DLMS/COSEM	PRIME M&M G3-PLC OSGP	DLMS/COSEM	DLMS/COSEM	DLMS/COSEM G3-PLC	802.1X
Seguridad	Cifrado	Perfiles 1 y 2	Niveles Low y High	SI	SI	SI	SI
	Autenticación	Perfiles 1 y 2	Niveles Low y High	SI	SI	SI	SI
Capas implementadas por el protocolo (nivel OSI)	1	X		X	X	X	X
	2	X		X	X	X	X
	3			X	X	X	
	4		X	X	X	X	
	5		X		X	X	
	6		X		X	X	
	7		X	X	X	X	
Recomendaciones de seguridad		Utilizar el perfil de seguridad 2	Utilizar High Level security Sobre TCP/IP realizar filtrado en el puerto 4059	En despliegues conjuntos con DLMS/COSEM aplicar la seguridad en ambos protocolos	Utilizar autenticación vía RADIUS	Utilizar OSGP-AES	Utilizar el estándar IEEE 802.11

Tabla 1: Cuadro resumen de protocolos de las redes inteligentes.

incibe cert_

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD