Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1331

(03/2018)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Aplicaciones y servicios con seguridad (2) – Seguridad en sistemas eléctricos inteligentes

Directrices de seguridad para dispositivos de redes domésticas (HAN) en sistemas eléctricos inteligentes

Recomendación UIT-T X.1331

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1319
Seguridad en sistemas eléctricos inteligentes	**X.1330–X.1339**
Correo certificado	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistema de transporte inteligente (ITS)	X.1370–X.1389
Seguridad de la tecnología de registros distribuidos	X.1400–X.1429
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1331

Directrices de seguridad para dispositivos de redes domésticas (HAN) en sistemas eléctricos inteligentes

Resumen

Una red doméstica (HAN) en el contexto de sistemas eléctricos inteligentes es una red en los locales del cliente. Se diferencia de la red doméstica tradicional en que la HAN en las redes inteligentes incluye dispositivos eléctricos inteligentes, como recursos de energía distribuidos (DER), cargador de vehículos eléctricos (EV), sistema de gestión de energía doméstica (HEMS) y pantalla de energía del cliente (CED). Las cargas eléctricas y los DER del cliente están conectados a la HAN, de modo que el cliente puede apagarlos o encenderlos basándose en la información del proveedor a fin de utilizar la electricidad del modo más eficiente posible. La HAN suele estar conectada a Internet, por lo que los agresores pueden atacar fácilmente a la HAN y dispositivos HAN. Por consiguiente, los dispositivos HAN deben disponer de capacidades que impidan a los agresores poner en peligro la HAN y sus dispositivos. El proyecto de Recomendación UIT-T X.1331 presenta un análisis de las amenazas a la HAN en las redes inteligentes, los requisitos de seguridad y las funciones de seguridad. Dado que cada dispositivo HAN desempeña una función y un papel diferentes, se facilitan los requisitos de seguridad y las funciones de seguridad para cada tipo de dispositivo.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1331	29-03-2018	17	11.1002/1000/13405

Palabras clave

Red doméstica, directrices de seguridad, requisitos de seguridad, red eléctrica inteligente.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1331

Directrices de seguridad para dispositivos de redes domésticas (HAN) en sistemas eléctricos inteligentes

1 Alcance

En la presente Recomendación se describen las directrices de seguridad para dispositivos de redes domésticas (HAN) en sistemas eléctricos inteligentes. La presente Recomendación abarca:

– riesgos de seguridad de los dispositivos y comunicaciones en la HAN;

– requisitos de seguridad para los dispositivos y comunicaciones en la HAN;

– funciones de seguridad de los dispositivos y comunicaciones en la HAN.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otros textos

En la presente Recomendación se utilizan los siguientes términos definidos en otros textos:

3.1.1 interfaz de servicios energéticos (ESI) [b-UIT-T Y.2071]: Conjunto de funciones que consiste en funciones de pasarela y funciones para aplicaciones en las redes eléctricas inteligentes destinadas a controlar y gestionar los servicios eléctricos inteligentes en los locales del cliente.

3.1.2 sistema de almacenamiento de energía (ESS) [b-UIT-T L.1430]: Unidad o componente físico con capacidad para almacenar o acumular la energía producida por un generador o adquirida por el consumidor de energía.

NOTA – El ESS ofrece funciones de almacenamiento de electricidad utilizando diversos tipos de baterías. Un ejemplo de aplicación del almacenamiento de energía consiste en responder eficazmente a un mecanismo de precios dinámico desde la red del servicio público. La energía eléctrica se almacena durante un periodo en el que el coste es relativamente bajo y, cuando el precio sube, se utiliza para reemplazar la procedente de la red del servicio de suministro.

3.1.3 red doméstica (HAN) [b-UIT-T G.9959]: Red capaz de conectar los dispositivos en el ámbito doméstico.

3.1.4 sistema de gestión de energía doméstica (HEMS) [b-UIT-T Y.4409]: Sistema informático que consta de una plataforma software que ofrece servicios básicos y un conjunto de aplicaciones con la funcionalidad necesaria para la utilización eficaz del equipo doméstico, como electrodomésticos y baterías recargables, a fin de garantizar una seguridad adecuada del suministro eléctrico a un coste mínimo.

NOTA – El HEMS se denomina HAN en una red eléctrica inteligente.

3.1.5 pantalla doméstica (IHD) [b-UIT-T Y.4409]: Pantalla del usuario donde se muestra información sobre el consumo energético en el hogar. Los usuarios tienen la opción de controlar sus dispositivos domésticos a través de su interfaz de usuario.

NOTA – En el entorno del sistema de comunicación de la HAN se transfiere información de control y utilización. La pantalla del usuario puede ser también un móvil o teléfono inteligente, un televisor (protocolo Internet), videoteléfono Internet, computador personal, tableta o una pantalla mural.

3.1.6 red de área extensa (WAN) [b-UIT-T Y.4409]: Red de comunicación IP que abarca una zona geográfica extensa que incorpora Internet y dispositivos redes de área local.

3.2 Términos definidos en esta Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 vehículo eléctrico (EV): Vehículo motorizado que se recarga con una fuente de electricidad externa y que, a su vez, puede actuar de sistema de suministro eléctrico.

Ejemplos son todo tipo de vehículos eléctricos, EV de batería, EV híbridos enchufables y conversiones enchufables de EV híbridos. Los EV enchufables se denominan a veces vehículo con conexión a la red eléctrica o vehículo recargable con electricidad.

3.2.2 red de vecindad (NAN): Red de acceso que permite a la conexión de dispositivos finales de red eléctrica inteligente y de redes domésticas a una red de área extensa (WAN).

NOTA – Adaptado de [b-Smart-O-33].

3.2.3 contador inteligente: Dispositivo instalado en los locales para supervisar y controlar el consumo eléctrico de los dispositivos domésticos inteligentes basado en su información de respuesta a la demanda.

NOTA – Adaptado de [b-UIT-T Y.4409].

4 Abreviaturas y acrónimos

Esta Recomendación hace uso de las siguientes abreviaturas y acrónimos:

AMI Infraestructura de medición avanzada (*Advanced Metering Infrastructure*)

CED Pantalla de energía del cliente (*Customer Energy Display*)

DER Recurso eléctrico distribuido (*Distributed Electricity Resource*)

DG Generador distribuido (*Distributed Generator*)

DoS Denegación del servicio (*Denial of Service*)

DTLS Seguridad de la capa de transporte de datagramas (*Datagram Transport Layer Security*)

ESI Interfaz de servicios energéticos (*Energy Services Interface*)

ESS Sistema de almacenamiento de energía (*Energy Storage System*)

EV Vehículo eléctrico (*Electric Vehicle*)

G/W Pasarela (*Gateway*)

HAN Red doméstica (*Home Area Network*)

HEMS Sistema de gestión de la energía doméstica (*Home Energy Management System*)

HMAC Código de autentificación de mensajes basado en número generador (*Hash-based Message Authentication Code*)

ID Identificador (*Identifier*)

IP Protocolo Internet (*Internet Protocol*)

IHD Pantalla doméstica (*In-Home Display*)

NAN Red de vecindad (*Neighbourhood Area Network*)

TLS Seguridad de la capa de transporte (*Transport Layer Security*)

WAN Red de área extensa (*Wide Area Network*)

WPA Acceso Wi-Fi protegido (*Wi-Fi Protected Access*)

5 Convenios

Ninguno.

6 Modelo general de la red doméstica en una red eléctrica inteligente

Una red eléctrica inteligente es una red de distribución de electricidad equipada con tecnologías de la información y la comunicación. En una red eléctrica inteligente el servicio de suministro eléctrico puede estimar la demanda de electricidad a partir de la información sobre el consumo eléctrico del cliente recabada mediante contadores inteligentes. Por consiguiente, el servicio de suministro puede controlar los periodos de carga máxima basándose en dicha estimación. Antes de entrar en un periodo de carga máxima, el servicio de suministro reduce el consumo del cliente o lo hace conmutar a fuentes alternativas generadas mediante un recurso eléctrico distribuido (DER) en los locales del cliente, como dispositivos fotovoltaicos en el tejado, acumuladores de electricidad y vehículos eléctricos (EV). Asimismo, el cliente puede retrasar o adelantar el consumo eléctrico en función de la información sobre los periodos de máxima carga comunicada por el servicio de suministro.

A fin de intercambiar información entre el servicio de suministro y el cliente, el sistema de gestión de estimaciones o de la demanda del servicio de suministro debe conectarse a los dispositivos en los locales del cliente, por ejemplo un sistema de gestión de energía doméstica (HEMS) o una pantalla de energía del cliente (CED). En la Figura 6-1 se ilustran varias redes en un entorno de red eléctrica inteligente. Como se muestra en la Figura, la conexión puede establecerse por varias redes, como la HAN, la red de acceso [también denominada red de vecindad (NAN)] o la red de área extensa (WAN).

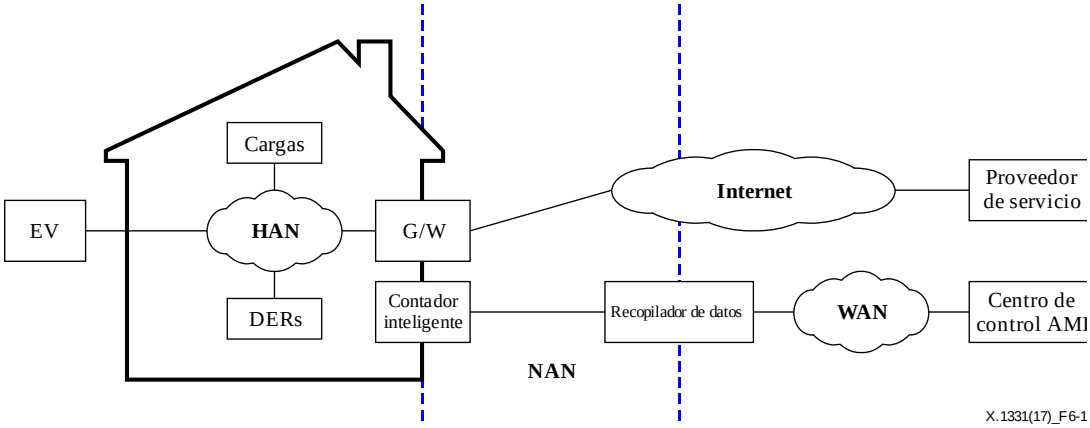

Figura 6-1 – Diversos tipos de redes en una red eléctrica inteligente

La HAN relaciona la carga eléctrica y los recursos eléctricos presentes en los locales del cliente. Toda la información procedente de los dispositivos HAN debe transferirse en primer lugar a un sistema de control del servicio de suministro, como el centro de control de la infraestructura de medición avanzada (AMI), desde la HAN, mientras que toda la información procedente del servicio de suministro debe transmitirse a los dispositivos cliente a través de la HAN.

Dado que la HAN suele estar conectada a Internet, la HAN es accesible desde Internet. Una vez que el usuario malicioso accede a la HAN, los dispositivos conectados a ésta pueden quedar en peligro y el agresor puede alterar deliberadamente la información, como la relativa a la carga eléctrica. Llegada esta situación, el agresor puede controlar los dispositivos HAN a su voluntad. Por consiguiente, se deben tomar medidas de seguridad en los dispositivos conectados a la HAC y en sus intercomunicaciones.

Antes de pasar a describir las amenazas, los requisitos y las tecnologías de seguridad, cabe formular un modelo general de HAN en la red eléctrica inteligente. El modelo general debe identificar todas las entidades e interfaces de comunicación conexas con el fin de aclarar sus interrelaciones.

En la Figura 6-2 se muestra el modelo general de HAN en una red eléctrica inteligente. En esta HAN, existen muchos elementos, como la carga eléctrica, un DER, un HEMS, una CED [también denominada pantalla doméstica (IHD)], una interfaz de servicios energéticos (ESI) y un contador inteligente.

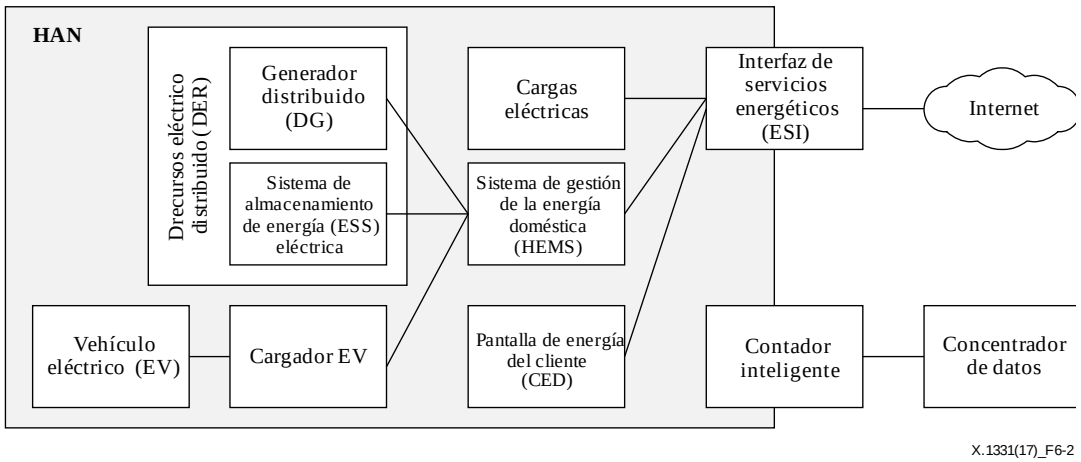

Figura 6-2 – Modelo general de la red doméstica en una red eléctrica inteligente

- Las cargas eléctricas son el resultado del consumo eléctrico de los dispositivos, como electrodomésticos, aparatos de aire acondicionado y bombas de agua. Las cargas suelen ser de dos tipos: inteligentes y tradicionales. Las cargas inteligentes incluyen funciones de comunicación y medición que no existían en las cargas tradicionales. Sin embargo, el consumo eléctrico resultante de las cargas tradicionales puede controlarse mediante un HEMS si el dispositivo se conecta al enchufe mediante una clavija inteligente, que disponga de funciones de comunicación y conmutación. Por consiguiente, en el presente proyecto de Recomendación se consideran cargas eléctricas tanto las cargas inteligentes como las clavijas inteligentes.
- Los recursos DER, entre los que se cuentan los generadores distribuidos (DG) y los sistemas de almacenamiento de energía eléctrica (ESS), son dispositivos que suministran electricidad a las cargas. Las fuentes fotovoltaicas son DG muy utilizados en las HAN.
- El EV puede actuar como carga y como DER. Cuando se está cargando, el EV constituye una carga para la HAN, mientras que cuando funciona como DER suministra electricidad a los electrodomésticos.
- El HEMS controla las capacidades de las cargas y los DER en función de lo programado por el cliente registrado o de las condiciones predefinidas. Los principales criterios son el precio de la electricidad y la señal de respuesta a la demanda.
- La pantalla CED muestra estadísticas de utilización de energía eléctrica e información sobre precios, de modo que el cliente puede reducir su consumo eléctrico o variar su horario de actividades que consumen energía.

7 Amenazas a la seguridad contra la red doméstica

En esta cláusula se enumeran las principales amenazas a la HAN. Obsérvese que no se pretende en esta cláusula definir una taxonomía de las amenazas, sino informar de las amenazas a la HAN que los operadores deben tener en cuenta como mínimo.

7.1 Filtración de datos

Una de las amenazas contra las redes o dispositivos más ampliamente detectadas es la filtración de datos almacenados o comunicados. El agresor puede espiar los datos transmitidos o acceder

físicamente a un dispositivo con el fin de obtener datos de su memoria. Si los datos no están protegidos, el agresor puede filtrarlos.

Dado que en las HAN se utiliza sobremanera la comunicación inalámbrica, resulta fácil espiar desde dentro o fuera de la HAN. Por otra parte, dado que las entidades en la HAN suelen estar conectadas a Internet, también son accesibles por entidades a distancia. Por consiguiente, en un entorno HAN resulta posible que agresores no autorizados accedan a los datos comunicados y almacenados.

El sistema HEMS, la CED y el contador inteligente de la HAN almacenan diversos tipos de datos relacionados con la privacidad, como información sobre el consumo eléctrico, sobre facturación y el plan de utilización de electricidad. Estos datos privados circulan por el HEMS y la CED a través de la interfaz ESI. La filtración de datos puede tener graves consecuencias negativas para la privacidad del cliente, por cuanto el agresor conocerá las costumbres cotidianas del mismo.

Por otra parte, también circulan por el HEMS y la CED, a través de la red de comunicación, instrucciones que controlan el funcionamiento de la carga, los DER o los cargadores de EV. Al acceder a estos datos, el agresor puede determinar cómo controlar la carga y los DER en la HAN. Este conocimiento constituye otra amenaza, como por ejemplo la de introducir datos maliciosos, como se describe en la cláusula 7.2.

7.2 Falsificación de datos o introducción de datos maliciosos

El agresor no autorizado puede insertar, modificar o suprimir información que se transmite entre entidades en la HAN o que está almacenada en una entidad de la HAN. El agresor puede ser una persona, un programa o una entidad de la HAN. Una vez se produce una amenaza de este tipo, la integridad de los datos queda menoscabada. Además, los daños causados a la integridad de los datos pueden dar lugar a una disfunción del dispositivo.

Dado que cualquier entidad anónima puede acceder a las redes de comunicaciones inalámbricas, toda entidad anónima puede enviar datos maliciosos a las entidades HAN. Por otra parte, el agresor puede añadir datos a una conexión existente fin el fin de piratear la conexión o enviar datos con fines maliciosos. Además, el agresor puede acceder a la memora de la entidad HAN, por ejemplo a un HEMS, y cambiar los datos almacenados o insertar datos maliciosos en la memoria.

Si se modifica más arriba la señal que contiene información sobre el precio de la electricidad, el HEMS puede reducir el consumo eléctrico en contra de la voluntad del cliente. Asimismo, el agresor puede enviar un mensaje de control para descargar un EV o un ESS. Otros ejemplos son enviar muchísimas solicitudes a una entidad, produciéndose una denegación del servicio (DoS) para dicha entidad, cambiar los valores en un fichero de datos o modificar un programa para alterar el funcionamiento de la entidad HAN.

7.3 Interrupción de la comunicación

Una forma de interrumpir la comunicación consiste en interferirla, que se produce cuando la señal interferente deliberada (*jamming*) o no prevalece en potencia sobre la señal del emisor o receptor en un enlace de comunicación, causando que este enlace resulte inservible. Otro ejemplo de interrupción consiste en consumir en exceso el ancho de banda de la comunicación, enviando ingentes volúmenes de datos.

El HEMS de la HAN debe recabar información sobre el estado de las cargas y de los DER en cuanto al consumo eléctrico, así como las señales de control y precio procedentes del servicio de suministro eléctrico o del proveedor del servicio, a fin de responder a los ajustes de la demanda solicitados. Por ende, para que la HAN funcione adecuadamente es necesario preservar sus capacidades de comunicación.

7.4 Acceso no autorizado

El acceso no autorizado se produce cuando el agresor consigue acceder a entidades tales como los DER, los HEMS o las CED, haciéndose pasar por un usuario real. Una vez que la tentativa de acceso no autorizado resulta fructuosa, el agresor podrá acceder también a otros dispositivos.

Para lograr dicho acceso, el agresor debe ser identificado y autentificado. A tal efecto, el agresor puede iniciar un ataque por barrido de puertos, que consiste en comprobar qué puertos vulnerables del dispositivo HAN están abiertos. Si hay puertos vulnerables abiertos, el agresor puede explotar dicha vulnerabilidad del dispositivo HAN. Asimismo, el agresor puede obtener acceso no autorizado al servicio "invulnerable" por medio de un ataque destinado a acertar la contraseña.

El malware constituye otra de las principales amenazas, por cuanto puede infectar un dispositivo HAN, por ejemplo una CED, por correo electrónico o servicio web, que luego se propaga a otros dispositivos en la HAN. Una vez se ha instalado malware en un dispositivo HAN, éste podrá obtener acceso no autorizado a los recursos del dispositivo, resultando posiblemente en una disfunción, deterioro o alteración del dispositivo.

7.5 Repudio

Esta amenaza se produce cuando el agresor, ya sea remitente o receptor, niega haber transmitido o recibido un mensaje. Esto no produce el deterioro o la disfunción de los dispositivos en la HAN, pero puede generar un conflicto. En función de la naturaleza del conflicto, es posible que el servicio deje de funcionar o funcione erróneamente al no haber sido correctamente identificado.

7.6 Relación entre amenazas de seguridad y la red doméstica

Las amenazas de seguridad descritas en las cláusulas 7.1 a 7.5 se producen en una entidad o comunicación determinada en el modelo general de HAN. En el Cuadro 7-1 se muestran las relaciones entre las amenazas de seguridad y las entidades HAN; el círculo indica que la amenaza del caso existe para la entidad indicada.

Cuadro 7-1 – Relaciones entre las amenazas de seguridad y la red doméstica

Entidad	Revelación		Modificación/ introducción		Interrupción	Acceso no autorizado	Repudio
	Datos almac.	Datos comunic.	Datos almac.	Datos comunic.			
Carga		○		○	○		
DER		○		○	○	○	○
Cargador EV		○		○	○		○
HEMS	○	○	○	○	○	○	○
CED	○	○	○	○	○	○	○
ESI					○	○	
Comunicación		○		○	○		

8 Requisitos de seguridad de la red doméstica

En esta cláusula se describen los requisitos generales de seguridad desde los principales cuatro aspectos de la seguridad, a saber, disponibilidad, confidencialidad, integridad y no repudio.

8.1 Disponibilidad

La disponibilidad garantiza que no se rechaza el acceso autorizado a los elementos de red, la información almacenada, los flujos de información, los servicios y a las aplicaciones debido a eventos que repercuten en la red. Es decir, si una entidad en la HAN desea obtener información sobre otro dispositivo y tiene permiso para ello, debe poder acceder al dispositivo inmediatamente.

Toda HAN en una red eléctrica inteligente debe poder controlar la utilización de las cargas, la generación y el almacenamiento de electricidad por los DER en función de la demanda de la red. Cuando el servicio de suministro estima que hay un pico de demanda, se debe transferir al HEMS o a la CED una solicitud de reducción del consumo o una señal con el nuevo precio, de modo que puedan gestionar la demanda de electricidad de los dispositivos del cliente. Se puede determinar si la solicitud ha sido aceptada a partir de los requisitos registrados por el cliente.

En cualquier caso, se debe garantizar en primer lugar la disponibilidad de la red y la funcionalidad de las entidades de la HAN. Si la red HAN no está disponible cuando se produce el pico de demanda, es posible que el HEMS no reciba señal alguna del servicio de suministro, dando lugar mayores costes para el cliente.

8.2 Confidencialidad

La confidencialidad garantiza que los datos contenidos no pueden ser leídos por entidades no autorizadas. Aun en el caso de incidentes donde se hayan interceptado datos espiando las comunicaciones inalámbricas, se puede garantizar la confidencialidad siempre que el agresor no pueda revelarlos.

La confidencialidad es imprescindible para entidades y datos de comunicación sensibles, ya se trate de almacenamiento o transmisión. Los datos sensibles en la HAN son, entre otros, la información del contador de consumo eléctrico, las instrucciones que controlan el funcionamiento de las cargas y de los DER, las señales de precios o las solicitudes de ajuste de la demanda procedentes del servicio de suministro y la información personal almacenada en la CED.

8.3 Integridad

La integridad garantiza que los datos, una vez transferidos, no difieren de los enviados en el origen. Últimamente se ha ampliado el significado de integridad para incluir el estado de un sistema o dispositivo, que no debe variar respecto de la configuración básica. Análogamente, los datos originales almacenados no deben alterarse tras una manipulación autorizada.

Por otra parte, debe garantizarse la integridad de las instrucciones de control y de la información de estado transferida entre un HEMS y otras entidades, ya sean cargas o DER. Además, debe protegerse la integridad de los datos enviados o recibidos por la CED. A fin de garantizar la funcionalidad, también debe protegerse la integridad de la lista de programas instalados en cada dispositivo HAN así como la de los programas propiamente dichos.

8.4 No repudio

El no repudio impide que una persona o entidad niegue haber realizado una determinada acción relacionada con los datos, mediante la puesta a disposición de pruebas digitales de la acción.

En una HAN, entre las acciones que posiblemente dan lugar a conflictos se cuentan el control de los DER y las cargas, la recepción de señales de precios y solicitudes de ajuste de la demanda, así como el registro del horario de utilización de electricidad por medio de la CED. Así, las entidades de la HAN relacionadas con estas acciones deben satisfacer el requisito de no repudio. No obstante, en el caso de las cargas el no repudio quizá no sea posible debido su forma de funcionar. Por ejemplo, un enchufe inteligente es un dispositivo limitado que no dispone de suficiente memoria ni capacidad de cálculo.

8.5 Relación entre requisitos de seguridad y la red doméstica

En el Cuadro 8-1 se muestra la relación entre los requisitos de seguridad y las amenazas de seguridad; el círculo indica que el requisito de seguridad del caso debe satisfacerse para eliminar o mitigar la amenaza considerada.

Cuadro 8-1 – Relación entre requisitos y amenazas de seguridad

			Amenazas de seguridad						
			Revelación		**Modificación /introducción**		**Interrupción**	**Acceso no autorizado**	**Repudio**
			Datos almac.	**Datos comunic.**	**Datos almac.**	**Datos comunic.**			
Requisitos de seguridad	**Confiden-cialidad**	**Datos almc.**	○						
		Datos comun.		○					
	Integridad	**Datos almc.**			○			○	
		Datos comun.				○		○	
	Disponibilidad						○		
	No repudio								○

Como las amenazas para cada entidad en la HAN se enumeran en el Cuadro 7-1 y los requisitos para cada amenaza en el Cuadro 8-1, es posible indicar los requisitos de seguridad para cada entidad en la HAN mediante la correlación de estos dos cuadros. En el Cuadro 8-2 se muestra la atribución de requisitos de seguridad a las entidades en la HAN, en el que el círculo significa que cada entidad debe satisfacer el requisito de seguridad del caso a fin de eliminar o reducir la amenaza considerada.

Cuadro 8-2 – Atribución de requisitos de seguridad a entidades en la red doméstica

		Requisitos de seguridad					
		Disponi-bilidad	**Confidencialidad**		**Integridad**		**No repudio**
			Datos almac.	**Datos comunic.**	**Datos almac.**	**Datos comunic.**	
Entidad	**Carga**	○		○		○	
	DER	○		○		○	○
	Cargador EV	○		○		○	○
	CED	○	○	○	○	○	○
	HEMS	○	○	○	○	○	○
	ESI	○				○	
	Comunicación	○		○		○	

9 Relación entre requisitos de seguridad y funciones de seguridad

A fin de satisfacer los requisitos de seguridad de la HAN y sus dispositivos, se deben aplicar funciones de seguridad, como por ejemplo cifrado y descifrado, firma digital, autentificación de mensajes y de entidades, autorización, control de acceso, medidas contra ataques DoS, auditoría y seguridad física.

En el Cuadro 9-1 se describe cómo pueden satisfacerse los requisitos de seguridad mediante funciones de seguridad. El círculo indica que puede recurrirse a la función de seguridad del caso para satisfacer el requisito de seguridad considerado. Obsérvese que en la cláusula 10 se describen cada una de las funciones de seguridad indicadas en el Cuadro 9-1.

Cuadro 9-1 – Relación entre los requisitos y las funciones de seguridad

			Funciones de seguridad							
			Cif./ Desc.	Firma digital	Autentificación		Control de acceso	Anti-DoS	Audi-toría	Seguridad física
					Msg.	Entidad				
Requisitos de seguridad	Confiden-cialidad	Datos almc.	○							
		Datos comn.	○							
	Integridad	Datos almc.		○	○		○			
		Datos comn.		○	○		○			
	Disponibilidad					○		○	○	○
	No repudio			○					○	○

10 Directrices de seguridad para dispositivos de red doméstica en sistemas de red eléctrica inteligente

10.1 Funciones de seguridad para cargas

En el Cuadro 10-1 se enumeran las funciones de seguridad para cargas en la HAN. Muestra la relación entre los requisitos de seguridad y las funciones de seguridad y describe en detalle las capacidades necesarias para implementar las funciones de seguridad.

Cuadro 10-1 – Funciones de seguridad para las cargas en la red doméstica

Requisitos de seguridad	Funciones de seguridad	Descripción
Disponibilidad	Medidas contra DoS	Capacidad para detectar y mitigar ataques DoS.
	Seguridad física	Capacidad para evitar el acceso físico no autorizado a fin de impedir a los usuarios no autorizados que manipulen o configuren las cargas.
Integridad	Autentificación de mensajes	Capacidad para generar y verificar datos de integridad criptográfica a fin de garantizar la integridad de notificaciones y de instrucciones de control. Los datos de integridad criptográfica pueden generarse mediante mecanismos HMAC (código de autentificación de mensajes basado en número generador).
Confidencialidad	Cifrado y descifrado	Capacidad para descifrar las instrucciones cifradas procedentes del HEMS.

10.2 Funciones de seguridad para recursos de energía distribuidos

En el Cuadro 10-2 se enumeran las funciones de seguridad de DER en la HAN. Muestra la relación entre los requisitos de seguridad y las funciones de seguridad y describe en detalle las capacidades necesarias para implementar las funciones de seguridad.

Cuadro 10-2 – Funciones de seguridad para recursos de energía distribuidos en la red doméstica

Requisitos de seguridad	Funciones de seguridad	Descripción
Disponibilidad	Medidas contra DoS	Capacidad para detectar y mitigar ataques DoS.
	Seguridad física	Capacidad para evitar el acceso físico no autorizado a fin de impedir a los usuarios no autorizados que manipulen o configuren las cargas.
Integridad	Autentificación de mensajes	Capacidad para generar y verificar datos de integridad criptográfica a fin de garantizar la integridad de notificaciones y de instrucciones de control. Los datos de integridad criptográfica pueden generarse mediante mecanismos HMAC o de firma digital.
	Autentificación de entidades	• Capacidad para autentificar terminales remotos, que envían instrucciones de control. La verificación de credenciales criptográficas o certificados puede considerarse un método de autentificación. • Capacidad para autentificar usuarios que tratan de configurar o manipular DER. La verificación por contraseña es una forma típica de autentificación de usuarios. Alternativas son la autentificación biométrica, como huellas digitales.
	Control de acceso	Capacidad para permitir que sólo los usuarios autorizados puedan modificar y manipular la configuración del DER.
Confidencialidad	Cifrado y descifrado	Capacidad para cifrar y descifrar instrucciones procedentes del HEMS.
No repudio	Firma digital	Capacidad para verificar la firma digital incluida en las instrucciones de control.
	Auditoría	Capacidad para crear y mantener registros de auditoría a fin de garantizar la responsabilidad. La carga y descarga de ESS es una acción importante que debe registrarse.

10.3 Funciones de seguridad para cargadores de vehículos eléctricos

En el Cuadro 10-3 se enumeran las funciones de seguridad de los cargadores EV en la HAN. Muestra la relación entre los requisitos de seguridad y las funciones de seguridad y describe en detalle las capacidades necesarias para implementar las funciones de seguridad.

Cuadro 10-3 – Funciones de seguridad para cargadores de vehículos eléctricos en la red doméstica

Requisitos de seguridad	Funciones de seguridad	Descripción
Disponibilidad	Medidas contra DoS	Capacidad para detectar y mitigar ataques DoS.
	Seguridad física	Capacidad para evitar el acceso físico no autorizado a fin de impedir a los usuarios no autorizados que manipulen o configuren las cargas.
Integridad	Autentificación de mensajes	Capacidad para generar y verificar datos de integridad criptográfica a fin de garantizar la integridad de notificaciones y de instrucciones

Cuadro 10-3 – Funciones de seguridad para cargadores de vehículos eléctricos en la red doméstica

Requisitos de seguridad	Funciones de seguridad	Descripción
		de control. Los datos de integridad criptográfica pueden generarse mediante mecanismos HMAC o de firma digital.
	Autentificación de entidades	• Capacidad para autentificar terminales remotos, que envían instrucciones de control. La verificación de credenciales criptográficas o certificados puede considerarse un método de autentificación. • Capacidad para autentificar usuarios que tratan de configurar o manipular cargadores. La verificación mediante contraseña es una forma típica de autentificación de usuarios. Una alternativa es la autentificación biométrica, como huellas digitales.
	Control de acceso	Capacidad para permitir que sólo los usuarios autorizados puedan modificar y manipular la configuración del cargador.
Confidencialidad	Cifrado y descifrado	Capacidad para descifrar las instrucciones cifradas procedentes del HEMS.
No repudio	Firma digital	Capacidad para verificar la firma digital incluida en una instrucción de control.
	Auditoría	Capacidad para crear y mantener registros de auditoría a fin de garantizar la responsabilidad. El inicio o fin de la carga es una acción importante que debe registrarse.

10.4 Funciones de seguridad para la pantalla de energía del cliente

En el Cuadro 10-4 se enumeran las funciones de seguridad de las CED en la HAN. Muestra la relación entre los requisitos de seguridad y las funciones de seguridad y describe en detalle las capacidades necesarias para implementar las funciones de seguridad.

Cuadro 10-4 – Funciones de seguridad para las pantalla de energía del cliente en la red doméstica

Requisitos de seguridad	Funciones de seguridad	Descripción
Disponibilidad	Seguridad física	Capacidad para impedir el acceso físico no autorizado a fin de impedir a los usuarios no autorizados que utilicen las CED.
Integridad	Autentificación de mensajes	Capacidad para generar y verificar datos de integridad criptográfica a fin de garantizar la integridad de la información de estado procedente del HEMS y de las instrucciones de control que se envía al HEMS. Los datos de integridad criptográfica pueden generarse mediante mecanismos HMAC o de firma digital.
	Autentificación de entidades	• Capacidad para autentificar el HEMS. La verificación de un certificado puede considerarse un método de autentificación. • Capacidad para autentificar usuarios que tratan de utilizar las CED. La verificación mediante contraseña es una forma típica de autentificación de usuarios. Una alternativa es la autentificación biométrica, como huellas digitales.
	Control de acceso	Capacidad para permitir que sólo los usuarios autorizados puedan modificar la configuración de la CED o utilizar sus funciones.

Cuadro 10-4 – Funciones de seguridad para las pantalla de energía del cliente en la red doméstica

Requisitos de seguridad	Funciones de seguridad	Descripción
	Integridad de las aplicaciones	Capacidad para garantizar la integridad de las aplicaciones a fin de detectar las que estén infectadas por malware o modificadas por agresores. Los agresores pueden modificar o suprimir deliberadamente ficheros ejecutables o bibliotecas, causando que la aplicación sea inestable. Esta capacidad permite a los dispositivos HAN determinar que la aplicación no ha sido modificada. Como método de ejemplo puede citarse verificar el código de integridad criptográfica de una aplicación, que se genera cuando ésta se instala o actualiza.
Confidencialidad	Cifrado y descifrado	• Capacidad para cifrar y descifrar mensajes enviados o recibidos por el HEMS a fin de proteger las instrucciones y otros mensajes que incluyan información de identificación personal. • Capacidad para cifrar y descifrar datos almacenados en una CED a fin de proteger la información de identificación personal en la CED.
No repudio	Firma digital	Capacidad para verificar la firma digital incluida en instrucciones de control.
	Auditoría	Capacidad para crear y mantener registros de auditoría a fin de garantizar la responsabilidad.

10.5 Funciones de seguridad para el sistema de gestión de energía doméstica

En el Cuadro 10-5 se enumeran las funciones de seguridad de un HEMS en la HAN. Muestra la relación entre los requisitos de seguridad y las funciones de seguridad y describe en detalle las capacidades necesarias para implementar las funciones de seguridad.

Cuadro 10-5 – Funciones de seguridad para el sistema de gestión de energía doméstica en la red doméstica

Requisitos de seguridad	Funciones de seguridad	Descripción
Disponibilidad	Medidas contra DoS	Capacidad para detectar y mitigar ataques DoS. En particular, deben protegerse contra ataques DoS los servicios que utilizan los clientes para controlar cargas y DER.
	Seguridad física	Capacidad para impedir el acceso físico no autorizado a fin de impedir a los usuarios no autorizados que manipulen o configuren el HEMS.
Integridad	Autentificación de mensajes	Capacidad para generar y verificar datos de integridad criptográfica a fin de garantizar la integridad de la información de estado procedente de otros dispositivos (cargas, DER y cargadores EV) e instrucciones de control que se envían a otros dispositivos (cargas, DER y cargadores EV). Los datos de integridad criptográfica pueden generarse mediante mecanismos HMAC o de firma digital.

Cuadro 10-5 – Funciones de seguridad para el sistema de gestión de energía doméstica en la red doméstica

Requisitos de seguridad	Funciones de seguridad	Descripción
	Autentificación de entidades	• Capacidad para autentificar terminales remotos. La verificación de un certificado puede considerarse un método de autentificación. Para cargas con poca potencia de cálculo, la autentificación puede lograrse verificando las credenciales generadas mediante un secreto compartido previamente. • Capacidad para autentificar usuarios que tratan de utilizar el HEMS. La verificación mediante contraseña es una forma típica de autentificación de usuarios. Una alternativa es la autentificación biométrica, como huellas digitales.
	Control de acceso	Capacidad para permitir que sólo los usuarios autorizados puedan modificar la configuración del HEMS o utilizar sus funciones. Deben mantenerse separadas las cuentas de administrador y de usuario general. Se deben crear y utilizar cuentas separadas para cada función, de modo que el agresor tenga acceso limitado a información sensible, funciones y a otras cuentas, si una cuenta ha sido pirateada.
	Integridad de las aplicaciones	Capacidad para garantizar la integridad de las aplicaciones a fin de detectar las que estén infectadas por malware o modificadas por agresores. Los agresores pueden modificar o suprimir deliberadamente ficheros ejecutables o bibliotecas, causando que la aplicación sea inestable. Esta capacidad permite a los dispositivos HAN determinar que la aplicación no ha sido modificada. Como método de ejemplo puede citarse verificar el código de integridad criptográfica de una aplicación, que se genera cuando ésta se instala o actualiza.
Confidencialidad	Cifrado y descifrado	• Capacidad para cifrar y descifrar mensajes enviados o recibidos por otra entidad en la HAN a fin de proteger las instrucciones y otros mensajes que incluyan información de identificación personal. • Capacidad para cifrar y descifrar datos almacenados en el HEMS a fin de proteger la eventual información de identificación personal en la HEMS.
No repudio	Firma digital	Capacidad para verificar la firma digital incluida en instrucciones de control.
	Auditoría	Capacidad para crear y mantener registros de auditoría a fin de garantizar la responsabilidad.

10.6 Funciones de seguridad para la interfaz de servicios energéticos

En el Cuadro 10-6 se enumeran las funciones de seguridad para un ESI en la HAN. Muestra la relación entre los requisitos de seguridad y las funciones de seguridad y describe en detalle las capacidades necesarias para implementar las funciones de seguridad.

Cuadro 10-6 – Funciones de seguridad para la interfaz de servicios energéticos en la red doméstica

Requisitos de seguridad	Funciones de seguridad	Descripción
Disponibilidad	Seguridad física	Capacidad para impedir el acceso físico no autorizado a fin de impedir a los usuarios no autorizados que utilicen la ESI.
Integridad	Control de acceso	• Capacidad para que solamente los dispositivos locales puedan acceder a la HAN. El punto de acceso Wi-Fi debe estar protegido por WPA II (acceso Wi-Fi protegido), con una contraseña compleja para evitar ataques por acierto de contraseña. Además, debe desactivarse la función de difusión del SSID (identificador (ID) de secuencia del servicio). Los puntos de acceso ZigBee o Bluetooth deben estar plenamente protegidos por funciones de seguridad de cada protocolo a fin que cumplir los requisitos de seguridad. • Capacidad para bloquear tráfico no autorizado basada en ID únicos. Como ID único puede recurrirse a la dirección MAC (control de acceso a los medios) o a la dirección IP (Protocolo Internet) del dispositivo.
	Integridad de la aplicación	Capacidad para garantizar la integridad de las aplicaciones a fin de detectar las que estén infectadas por malware o modificadas por agresores. Los agresores pueden modificar o suprimir deliberadamente ficheros ejecutables o bibliotecas, causando que la aplicación sea inestable. Esta capacidad permite a los dispositivos HAN determinar que la aplicación no ha sido modificada. Como método de ejemplo puede citarse verificar el código de integridad criptográfica de una aplicación, que se genera cuando ésta se instala o actualiza.

10.7 Funciones de seguridad para la comunicación

En el Cuadro 10-7 se enumeran las funciones de seguridad para la comunicación en la HAN. Muestra la relación entre los requisitos de seguridad y las funciones de seguridad y describe en detalle las capacidades necesarias para implementar las funciones de seguridad.

Cuadro 10-7 – Funciones de seguridad para la comunicación en la red doméstica

Requisitos de seguridad	Funciones de seguridad	Descripción
Disponibilidad	Medidas contra DoS	Capacidad para detectar y mitigar ataques DoS.
Integridad	Autentificación de mensajes y entidades	Capacidad para la autentificación mutua de entidades comunicantes y de los mensajes a fin de garantizar la integridad de los datos en la comunicación. Una opción adecuada sería la seguridad de la capa de transporte (TLS) o la seguridad de la capa de transporte de datagramas (DTLS) utilizando certificados. Debe seleccionarse un algoritmo criptográfico seguro para TLS o DTLS.

Cuadro 10-7 – Funciones de seguridad para la comunicación en la red doméstica

Requisitos de seguridad	Funciones de seguridad	Descripción
	Control de acceso	• Capacidad para que sólo los dispositivos locales autorizados puedan acceder a la HAN. • Capacidad para bloquear tráfico no autorizado basada en ID únicos. Como ID único puede recurrirse a la dirección MAC o la dirección IP del dispositivo.
Confidencialidad	Cifrado y descifrado	Capacidad para cifrar y descifrar datos almacenados en el HEMS a fin de proteger la eventual información de identificación personal en la HEMS.

Bibliografía

[b-UIT-T G.9959] Recomendación UIT-T G.9959 (2015), *Transceptores de radiocomunicación digital de corto alcance y banda estrecha – Especificaciones de las capas PHY, MAC, SAR y LLC*.

[b-UIT-T L.1430] Recomendación UIT-T L.1430 (2013), *Método para la evaluación de los efectos medioambientales de los gases de efecto invernadero de las tecnologías de la información y la comunicación y los proyectos de energía*.

[b-UIT-T Y.2071] Recomendación UIT-T Y.2071 (2015), *Marco para una microrred eléctrica*.

[b-UIT-T Y.4409] Recomendación UIT-T Y.4409/Y.2070 (2015), *Requisitos y arquitectura del sistema de gestión energética doméstica y de los servicios de red doméstica*.

[b-UIT-T Smart-O-33] UIT-T FG-Smart Grid: Smart-O-33Rev.6 (2011) *Smart Grid Architecture*; http://www.itu.int/en/ITU-T/focusgroups/smart/Documents/smart-o-0033r6_architecture_deliverable.doc

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de la próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2019