Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1373

(03/2017)

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

Capacidad de actualización segura de software en dispositivos de comunicación de sistemas de transporte inteligente

Recomendación UIT-T X.1373

Unión Internacional de Telecomunicaciones

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 (1)	
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 (1)	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
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	**X.1370–X.1379**
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.1373

Capacidad de actualización segura de software en dispositivos de **comunicación de sistemas de transporte inteligente**

Resumen

La mejora de las tecnologías de los sistemas de transporte inteligente (ITS) ha permitido que sea habitual la comunicación entre vehículos y otras entidades, ya sean otros vehículos (comunicaciones vehículo a vehículo, V2V) o infraestructura (comunicaciones vehículo a infraestructura, V2I). Los dispositivos electrónicos integrados en los vehículos, como las unidades de control electrónicas (ECU), los sistemas electrónicos de pago de peaje (ETC) y los sistemas de navegación, son cada vez más sofisticados. Como resultado, los módulos software de dichos dispositivos electrónicos deben actualizarse adecuadamente para subsanar errores del software y mejorar la calidad de funcionamiento y la seguridad, con el fin de evitar accidentes.

Con el objetivo de cumplir los requisitos mencionados, la Recomendación UIT-T X.1373 proporciona procedimientos de actualización segura de software que se ejecutan entre el servidor de actualización de software y los vehículos, en los que se aplican controles de seguridad adecuados con el fin de satisfacer esos requisitos. Esta Recomendación puede ser de utilidad para fabricantes de automóviles y para industrias relacionadas con los ITS, como conjunto de capacidades normalizadas para el desarrollo de prácticas idóneas.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1373	2017-03-30	17	11.1002/1000/13197

Palabras clave

Análisis de riesgos, ataque de denegación de servicio, comunicaciones inalámbricas, dispositivos de comunicación, DoS, HSM, ITS, módulo hardware de seguridad, privacidad, sistema de transporte inteligente, sistema integrado, software malicioso, V2I, V2V, vehículo a infraestructura, vehículo a vehículo, vehículo a X (vehículo/infraestructura) (V2X).

* 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 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.1373

Capacidad de actualización segura de software en dispositivos de **comunicación de sistemas de transporte inteligente**

1 Alcance

En el contexto de las actualizaciones de los módulos software de dispositivos electrónicos de vehículos en el entorno de las comunicaciones de sistemas de transporte inteligente (ITS), esta Recomendación tiene por objeto proporcionar un procedimiento seguro de actualización de software de la capa de aplicación en dispositivos de comunicaciones ITS a fin de prevenir amenazas tales como la manipulación e intrusión maliciosa en los dispositivos de comunicación a bordo de vehículos. Se incluye un modelo básico de actualización de software, controles de seguridad para la actualización de software y una especificación del formato de datos abstracto del módulo del software de actualización.

El procedimiento asociado a la comunicación en el interior del vehículo queda fuera del alcance de esta Recomendación. El procedimiento utilizado en el interior del vehículo que se recoge en esta Recomendación tiene carácter informativo.

El procedimiento tiene por objeto ser aplicado a dispositivos de comunicación en vehículos dotados de ITS en el entorno de la comunicación vehículo a infraestructura (V2I) mediante Internet y/o redes dedicadas para ITS. El procedimiento comprende una serie de pautas técnicas, carece de requisitos en materia de cumplimiento y puede ser utilizado por fabricantes de automóviles y por la industria relacionada con los ITS como un conjunto de procedimientos protegidos y controles de seguridad.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[UIT-T X.509] Recomendación UIT-T X.509 (2012) | ISO/CEI 9594-8:2014, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos*.

[UIT-T X.1521] Recomendación UIT-T X.1521 (2011), *Sistema común de puntuación de vulnerabilidades*.

[ISO/CEI 15408-1] ISO/CEI 15408:2009, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*.

[ISO/CEI 27000] ISO/CEI 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 amenaza [ISO/CEI 27000]: causa potencial de un incidente indeseado, que puede infringir daño a un sistema u organización.

3.2 Términos definidos en esta Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 puntuación del riesgo: puntuación calculada mediante un método de análisis del riesgo para cada amenaza.

3.2.2 pasarela móvil de vehículo (**VMG**, *vehicle mobile gateway*): módulo que proporciona la comunicación entre las unidades de control electrónicas (ECU) situadas en la red de área del controlador (CAN) (buses del vehículo) y las entidades exteriores del sistema de transporte inteligente (ITS) situadas en la red externa.

4 Siglas y acrónimos

En la presente Recomendación se utilizan las siguientes siglas y acrónimos:

CA Autoridad de certificación (*certification authority*)

CAN Red de área del controlador (*controller area network*)

CD Disco compacto (*compact disc*)

CRSS Sistema de puntuación del riesgo basado en CVSS (*CVSS based risk scoring system*)

CVSS Sistema común de puntuación de la vulnerabilidad (*common vulnerability scoring system*)

DoS Denegación de servicio (*denial of service*)

DVD Disco digital versátil (*digital versatile disc*)

ECU Unidad de control electrónica (*electronic control unit*)

ETC Pago electrónico de peaje (*electronic toll collection*)

FT Árbol de fallos (*fault tree*)

GPS Sistema mundial de determinación de posición (*global positioning system*)

GUID Identificador global de usuario (*global user ID*)

HSM Módulo hardware de seguridad (*hardware security module*)

HTTP Protocolo de transferencia de hipertexto (*hypertext transfer protocol*)

HTTPS Protocolo seguro de transferencia de hipertexto (*hypertext transfer protocol secure*)

ID Identificador (*identifier*)

ITS Sistema de transporte inteligente (*intelligent transportation system*)

LIN Red de interconexión local (*local interconnect network*)

MAC Código de autenticación de mensaje (*message authentication code*)

MOST Transporte de sistemas orientados a los medios (*media oriented systems transport*)

OBD Diagnosis a bordo (*on-board diagnostics*)

OEM Fabricante de equipo original (*original equipment manufacturer*)

PC Computadora personal (*personal computer*)

RPM Revoluciones por minuto (*revolutions per minute*)

RSS Sistema de puntuación del riesgo (*risk scoring system*)

SD Seguridad digital (*secure digital*)

SHA Algoritmo de troceo (*hash*) seguro (*secure hash algorithm*)

SSL Capa de zócalo segura (*secure socket layer*)

TI Tecnología de la información (*information technology*)

TLS Seguridad de la capa de transporte (*transport layer security*)

TOE Objetivo de la evaluación (*target of evaluation*)

TPM Módulo de plataforma de confianza (*trusted platform module*)

TV Televisión (*television*)

UI Interfaz de usuario (*user interface*)

URL Localizador uniforme de recursos (*uniform resource locator*)

USB Bus serie universal (*universal serial bus*)

Usvr Servidor de actualización (*update server*)

V2I Vehículo a infraestructura (*vehicle-to-infrastructure*)

V2V Vehículo a vehículo (*vehicle-to-vehicle)*

V2X Vehículo a X (vehículo/infraestructura) (*vehicle-to-X (vehicle/infrastructure)*)

VMG Pasarela móvil de vehículo (*vehicle mobile gateway*)

WiFi Fidelidad inalámbrica (*wireless-fidelity*)

XML Lenguaje de marcación eXtendida (*extended mark-up language*)

5 Convenios

Ninguno.

6 Modelo básico de actualización de software a distancia

A efectos de la realización práctica de una arquitectura de seguridad, este apartado presenta un modelo básico de arquitectura convencional para la actualización de software que incluye la definición de módulos principales y de procesos típicos de actualización de software.

6.1 Módulos del entorno ITS para la actualización de software

En la Figura 1 se presenta la visión general de los principales módulos de un vehículo para la actualización de software a distancia en el entorno de comunicación de los ITS. Los principales módulos son dispositivos de información, unidades de control electrónicas (ECU), una pasarela móvil de vehículo (VMG) a bordo del vehículo, el servidor de actualización (Usvr) y la base de datos de registro del fabricante del vehículo y del proveedor. Los procedimientos asociados a las comunicaciones en el interior del vehículo (por ejemplo entre la ECU y la pasarela móvil de vehículo) quedan fuera del alcance de esta Recomendación. Los módulos utilizados para la comunicación dentro el vehículo (como la "interfaz de usuario" y las "ECU") se describen más adelante con carácter informativo.

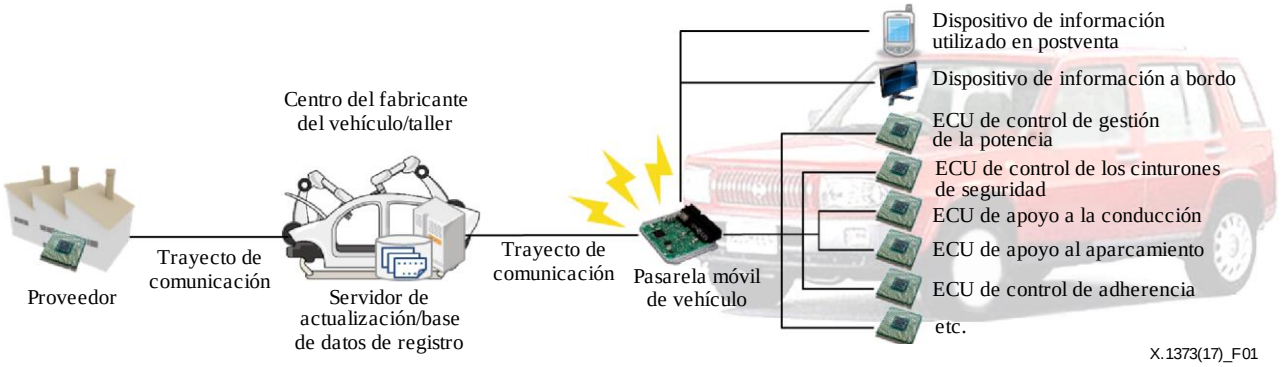

Figura 1 – Módulos principales en el entorno de un vehículo

6.1.1 Interfaz de usuario (informativo)

La interfaz de usuario (UI) es, por lo general, un dispositivo a bordo del vehículo o del que dispone el servicio de mantenimiento que tiene una pantalla y dispositivos de entrada. El dispositivo está directamente conectado a otros dispositivos del vehículo (por ejemplo, a la VMG o a las ECU (véase la cláusula 6.1.2)) de forma que puede obtener datos e informar sobre la situación de diversos parámetros del vehículo, como la velocidad, las revoluciones por minuto, el nivel de combustible y otros. En particular, en esta Recomendación se utiliza una interfaz de usuario para notificar a los conductores la necesidad de actualizaciones.

6.1.2 Unidad de control electrónica (ECU) (informativo)

ECU es un término genérico que hace referencia a computadoras que controlan diversos tipos de dispositivos en un vehículo. En los primeros años de existencia de las ECU, éstas realizaban funciones de control de aspectos tales como el encendido, la inyección, el ajuste del ralentí y actuaban como limitadores del motor para mejorar la eficiencia de uso del combustible y reducir las emisiones de gases. Conforme se han incorporado nuevos elementos informáticos en los vehículos, las ECU ha ido ampliando su campo de aplicación a diversos tipos de funciones, como la gestión de la potencia, el control de los cinturones de seguridad, los asistentes a la conducción, los asistentes de aparcamiento, el control de adherencia, la transmisión automática, etc. En los últimos años, el número de ECU de un vehículo ha aumentado de 50 a 100 y su importancia para el control de la seguridad y las comunicaciones es cada vez mayor. Sin embargo, dado que el desarrollo de las ECU conlleva implementaciones sofisticadas de software, este aumento del número de ECU en los vehículos supone un sobrecoste muy importante para los fabricantes de automóviles.

6.1.3 Pasarela móvil de vehículo

La pasarela móvil de vehículo es un módulo cuya función es interaccionar con el "servidor de actualizaciones" (véase la cláusula 6.1.4) para la actualización de software del vehículo. El proceso de actualización de software del vehículo que se desarrolla en el interior del mismo queda fuera del alcance de esta Recomendación. La VMG puede ser una entidad conceptual que en la práctica se implementa en un conjunto de componentes. Por ejemplo, la entidad de gestión de la conexión (también conocida como "pasarela central", "unidad de cabecera", "unidad de cabecera de comunicación" o "pasarela de vehículo (VG)") puede utilizarse en este contexto para la función de VMG, pudiendo utilizarse también otros dispositivos para la actualización de software. El trayecto de comunicación entre la pasarela móvil de vehículo y las entidades externas de los ITS utiliza una red celular (red móvil) y una red fija con acceso inalámbrico.

6.1.4 Servidor de actualización y base de datos de registro

Los servidores de actualización se instalan en centros de fabricantes de automóviles o en talleres con el fin de recopilar información sobre el estado de los módulos software de los vehículos y distribuir módulos de actualización de software a los mismos. Asimismo, en las computadoras en red más recientes, como computadoras personales y teléfonos inteligentes, una de las funciones más

importantes del servidor de actualización es la gestión y el control integral del software de los vehículos. A fin de gestionar de forma automática la situación del software de cada vehículo, el servidor de actualización debe trabajar con una base de datos de registro que almacene información que refleje la situación real del software del vehículo. Nótese que un servidor de actualización puede instalarse no sólo en un centro de un fabricante de automóviles, sino también de un proveedor o de un tercero.

6.1.5 Proveedor

Un vehículo se compone de miles de componentes suministrados por numerosos proveedores del sector del automóvil. Los dispositivos de comunicación a bordo y las ECU son suministrados por proveedores especializados y son ensamblados por los fabricantes de automóviles teniendo en cuenta las dependencias entre los diversos dispositivos. Por tanto, y en general, los módulos de actualización de dispositivos de comunicación a bordo no son producidos previamente por el fabricante del automóvil, sino por uno de sus proveedores. El fabricante instala en los vehículos los módulos actualizados suministrados tras un una cuidadosa prueba y evaluación por su parte.

6.2 Modelo del procedimiento de actualización de software

6.2.1 Procedimiento general de actualización

La Figura 2 muestra un modelo típico de procedimiento de actualización de software que inicia la pasarela móvil de vehículo al verificar que existen nuevas actualizaciones. Dado que las comunicaciones en el interior del vehículo están fuera del alcance de esta Recomendación, los pasos asociados a las comunicaciones en el interior del vehículo de la Figura 2 sólo tienen carácter informativo a los que se hace referencia para facilitar la implementación práctica de un procedimiento seguro de actualización.

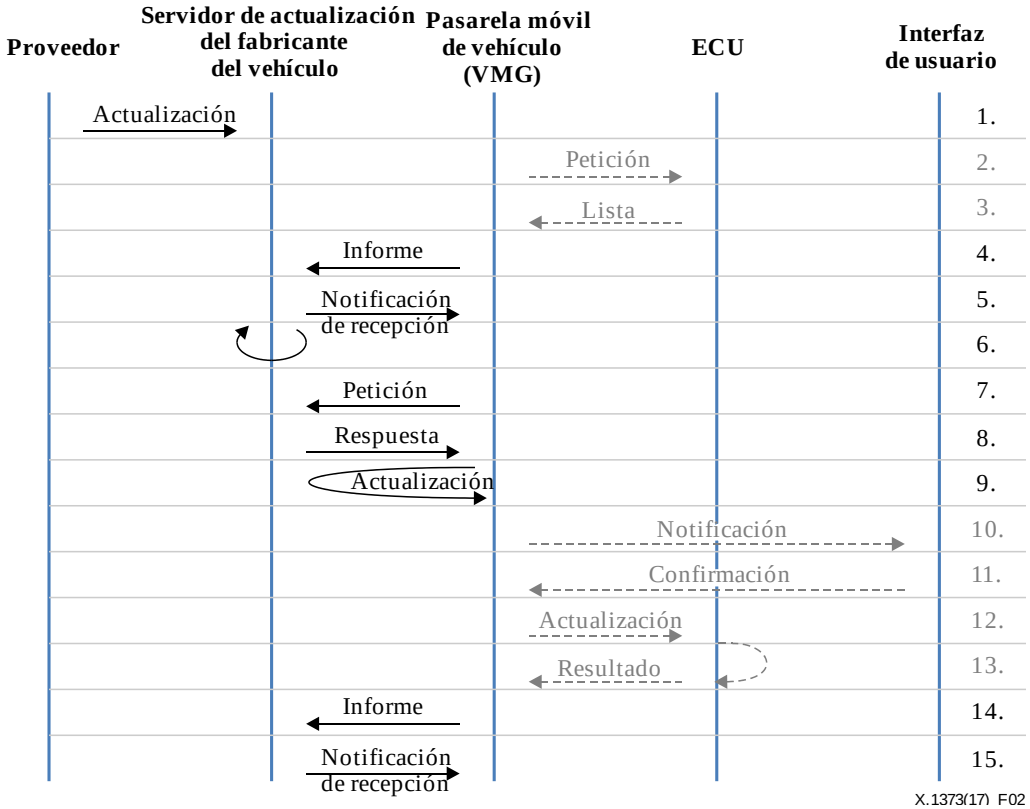

Figura 2 – Modelo del proceso de actualización de software

A continuación se describen los pasos del procedimiento de actualización, indicándose en *letra cursiva* los pasos 2, 3 y 10 a 13, incluidos sólo a efectos informativos:

1) Como primer paso del proceso, un proveedor de componentes del automóvil suministra el módulo de actualización, algo que ocurre de forma asíncrona respecto al resto de los pasos.

2) *Al iniciarse el proceso de actualización, la pasarela móvil de vehículo solicita a las ECU que le envíen las listas de sus respectivos programas*.

3) *Cada ECU verifica la situación de su software y genera una lista de módulos software, de la que informa a la VMG*.

4) La VMG envía la lista recopilada al servidor de actualización para verificar si existe alguna actualización para el vehículo.

5) El servidor de actualización envía a la VMG una notificación de recepción de la lista que aquél le ha remitido.

6) De conformidad con la lista, el servidor de actualización inspecciona la situación del software instalado en el vehículo y determina las actualizaciones de software que precisan las ECU.

7) Dado que esta inspección puede requerir un tiempo prolongado, la VMG verifica periódicamente la necesidad de actualizaciones del vehículo.

8) Si existe una actualización, el servidor de actualización envía los localizadores de recursos uniformes de acceso (URL) a las actualizaciones; en otro caso, sólo remite un mensaje de acuse de recibo.

9) Si existe alguna actualización para el vehículo, la VMG se conecta con el servidor de actualización para descargar los módulos de actualización para el vehículo.

10) *Antes de instalar las actualizaciones en las ECU, la VMG lo notifica al conductor para que confirme la instalación de las actualizaciones*.

11) *El conductor confirma y acepta que se instalen las actualizaciones*.

12) *La VMG entrega los ficheros de actualización a las correspondientes ECU y les solicita que instalen las actualizaciones (véase la cláusuola 6.2.3).*

13) *Cada ECU instala la actualización e informa del resultado a la pasarela móvil de vehículo*.

14) La pasarela móvil de vehículo envía un informe con los resultados de la instalación al servidor de actualización.

15) Finalmente, el servidor de actualización devuelve una notificación de recepción de la información de actualización. Si la instalación de la actualización ha fallado o se determina que aún hay pendiente alguna actualización, el servidor de actualización reintenta el procedimiento desde el paso 6 al 14 hasta que la aplicación se haya instalado con éxito (véase la cláusula 6.2.2).

6.2.2 Consideraciones sobre reintentos ilimitados

Según el paso 15 del procedimiento descrito en la cláusula anterior, se realizan reintentos hasta realizar la actualización con éxito, sin embargo, puede ocurrir el procedimiento no se complete con éxito nunca, en cuyo caso la VMG continuaría realizando un número ilimitado de intentos. Para evitarlo, debe limitarse el número de intentos a un número "N" establecido en función de la política del procedimiento de actualización. La forma de definir la política de actualización queda fuera del alcance de esta Recomendación.

6.2.3 Consideración sobre la limitación de recursos

En relación con la instalación de software de actualización en un vehículo (véase el paso informativo 12 en la cláusula 6.2.1), en el mismo existen módulos sin recursos de memoria suficientes para realizar la actualización completa de una sola vez. Para dichos módulos, es necesario utilizar la tecnología de actualización secuencial mediante el envío de flujos de datos fragmentados.

En general, para cualquier módulo de un vehículo, cualquiera que sea el sistema de actualización, debe tenerse debidamente en cuenta las limitaciones derivadas de los recursos finitos de los dispositivos, como memoria, almacenamiento y caudal de la red.

7 Especificación del procedimiento seguro de actualización de software

En este apartado se especifica un procedimiento práctico y los correspondientes formatos de los mensajes de la aplicación entre el servidor de actualización y el vehículo (VMG) para la actualización de software con funciones de seguridad. Obsérvese que en esta Recomendación no se especifican funciones sobre la confidencialidad de los mensajes. La confidencialidad puede lograrse mediante protocolos de capa inferior (por ejemplo, el protocolo de transferencia de hipertexto seguro (HTTPS) y el protocolo de tunelizado seguro, etc.).

El procedimiento debe tener en cuenta las distintas capacidades de seguridad de los vehículos. En consecuencia, según esta Recomendación, para un intercambio de mensajes seguro los vehículos con algoritmo criptográfico asimétrico aplican el método de firma digital (véase la cláusula 7.1.1) y los vehículos que carecen de algoritmo criptográfico asimétrico, aplican el método del código de autenticación de mensaje (MAC) (véase la cláusula 7.1.2).

7.1 Formato del mensaje general con funciones de seguridad

En este apartado se presenta un formato general de mensajes con funciones de seguridad, incluido el método de autenticación del emisor del mensaje y la verificación de la integridad del mismo. En cuanto a los aspectos técnicos sobre integridad y autenticación, puede aplicarse el método de firma digital con algoritmo de clave pública y/o el método del código de autenticación de mensajes con algoritmo de clave compartida. En el procedimiento de actualización segura de software cada mensaje debe construirse utilizando uno de los métodos de seguridad tal como se indica a continuación.

7.1.1 Método de firma digital

Entre los métodos de implementación, puede utilizarse la firma digital basada en UIT-T X.509 para la autenticación de entidades y la verificación de la integridad de mensajes entre vehículos con capacidades criptográficas asimétricas mediante el módulo hardware de seguridad (HSM) (por ejemplo, el módulo de la plataforma de confianza, TPM).

7.1.2 Método MAC

El algoritmo de clave compartida es adecuado para dispositivos con capacidades de proceso reducidas porque requiere menos carga de procesamiento que el algoritmo de clave pública. Sin embargo, en el algoritmo de clave compartida el emisor y el receptor utilizan la misma clave y, por tanto, gran número de dispositivos comparten la misma clave. Este modo de funcionamiento requiere la actualización de las claves en todos los dispositivos del sistema cuando se produce una filtración de la misma. Además, debido a que la clave compartida no autentica al emisor, cada mensaje debe contener un ID del dispositivo emisor, algo que presupone que no existe una manipulación indebida del identificador del dispositivo.

7.2 Definición del protocolo y formato de datos

El formato de datos de la aplicación está dedicado a la distribución de mensajes exclusivamente relacionados con la actualización de software, algo que tiene en cuenta el formato de mensaje general descrito en la cláusula anterior. En este apartado se definen, en primer lugar, los tipos de mensajes utilizados en el procedimiento de actualización de software y, en segundo lugar, se presentan las especificaciones de los tipos de mensajes. A título informativo, se incluyen ejemplos de mensajes en formato XML (lenguaje de marcación extendida).

7.2.1 Visión general del protocolo

En base al modelo del procedimiento de actualización de software descrito en la cláusula 6, los mensajes se clasifican en varios tipos de acuerdo con sus objetivos, tal como se muestra en la Figura 3. Los procedimientos de comunicación en el interior del vehículo están fuera del alcance de esta Recomendación y se representan en la Figura 3 con caracteres de color gris.

NOTA – El procedimiento de comunicaciones en el interior del vehículo puede consultarse en [b-ISO 14229] e [b-ISO 13440].

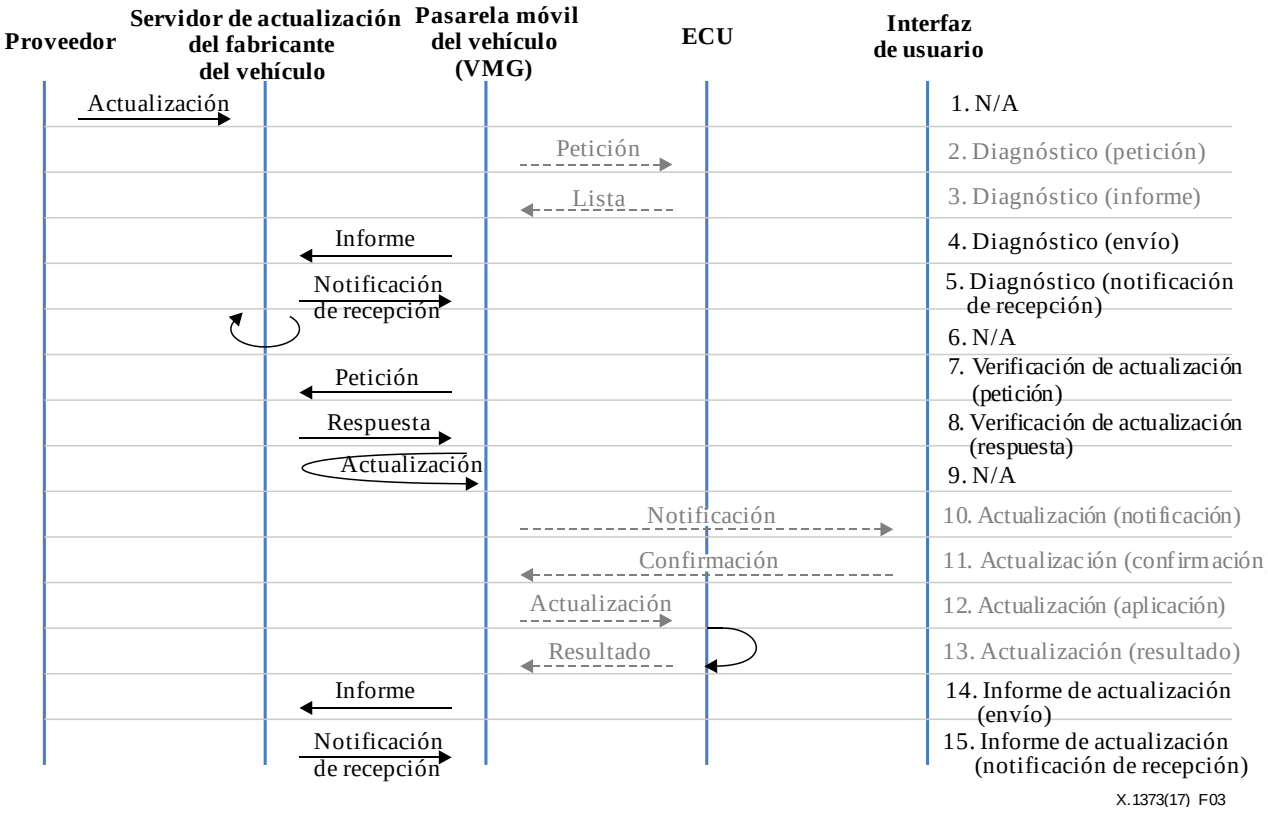

Figura 3 – Definición de los tipos de mensajes

Dado que el propósito de los mensajes de los pasos 2, 3, 4 y 5 es la petición e información relativa al diagnóstico de la situación del software en cada ECU, los mensajes se consideran de "diagnóstico" ("*diagnose*"). De igual modo, los mensajes de los pasos 7 y 8 se clasifican como de "verificación de la actualización" ("*update_check*"). Los mensajes de los pasos 10, 11, 12 y 13 son de "actualización" ("*update*"), ya que se trata de mensajes que confirman e instalan las actualizaciones. Finalmente, los resultados de las actualizaciones se envían como mensajes de "informe de actualización" ("*update_report*"), tal como se refleja en los pasos 14 y 15. En el Cuadro 1 se muestran los tipos, subtipos y códigos de los mensajes.

Cuadro 1 – Tipos de mensajes

Tipo	Subtipo	De	A	Propósito
diagnóstico (diagnose)	*petición (request)*	*VMG*	*ECU*	*Petición del diagnóstico de situación del software*
	Informe (report)	*ECU*	*VMG*	*Resultado del diagnóstico, incluida la situación del software*
	envío (submit)	VMG	Usvr	Informe de resultados de las ECU en un vehículo
	notificación de recepción (receipt)	Usvr	VMG	Notificación de recepción del envío del informe de diagnóstico
verificación de actualización (update_check)	petición (request)	VMG	Usvr	Petición del módulo de actualización
	respuesta (response)	Usvr	VMG	Actualización de módulo facilitada
actualización (update)	*notificación (notification)*	*VMG*	*UI*	*Mensaje de notificación para presentar la actualización al conductor*
	sonfirmación (confirmation)	*UI*	*VMG*	*Mensaje de confirmación del conductor para instalar la actualización*
	aplicación (application)	*VMG*	*ECU*	*Mensaje de petición, incluido el módulo de actualización*
	resultado (result)	*ECU*	*VMG*	*Resultado de la instalación del módulo de actualización*
informe de actualización (update_report)	envío (submit)	VMG	Usvr	Informe de la aplicación de la actualización
	notificación de recepción (receipt)	Usvr	VMG	Notificación de recepción del informe
* Usvr: servidor de actualización * UI: interfaz de usuario				

NOTA – En el Cuadro 1, los caracteres en color gris y letra cursiva indican elementos que están fuera del alcance de esta Recomendación y se incluyen sólo a título informativo.

7.2.2 Mensajes diagnóstico (*diagnose*)

A fin de determinar los módulos de actualización necesarios en un vehículo, se utilizan mensajes de diagnóstico entre el servidor de actualización y la VMG para transmitir información relativa al software desde los vehículos al servidor de actualización.

7.2.2.1 Mensaje diagnóstico (envío) (*diagnose (submit)*)

Una vez recopilados los resultados del diagnóstico del vehículo, la VMG envía una lista con información del software al servidor de actualización del fabricante (o del taller). El mensaje diagnóstico (envío) incluye la identidad del vehículo (vid) y una lista de información del software extraída de los mensajes diagnóstico (informe) (*diagnose (report)*).

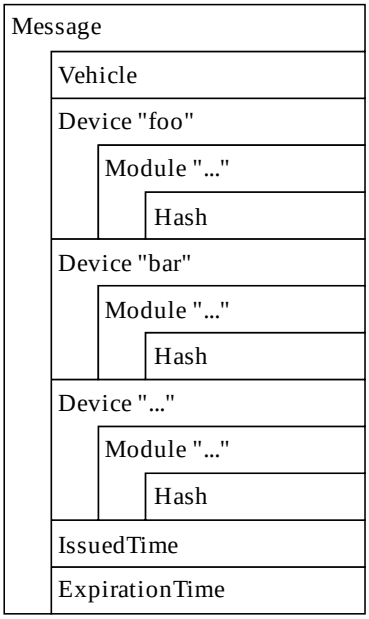

Figura 4 – Estructura del mensaje diagnóstico (envío) (*diagnose (submit)*)

Cuadro 2 – Elementos del mensaje diagnóstico (envío) (*diagnose (submit)*)

Elemento	Atributos del elemento	Descripción
Message	–	Contenedor del mensaje
	protocol	Siempre "1.0"
	version	Número de la versión del remitente del mensaje
	type	Tipo de mensaje (siempre "diagnóstico" ("*diagnose*"))
	subtype	Subtipo de mensaje (siempre "envío" ("*submit*"))
	sessionid	Identificador (ID) de sesión es un identificador global de usuario (GUID) aleatorio asociado con la sesión de diagnóstico. Un ID de sesión idéntico se aplica a los mensajes diagnóstico (petición, informe, envío y notificación de recepción)
	trustlevel	El nivel de confianza (*trust level*) se determina en base a la capacidad en términos de seguridad y a los requisitos de protección del dispositivo que ha generado el mensaje
	ownerid	ID del propietario suministrado por el fabricante/proveedor del vehículo
	messageid	ID del mensaje es un GUID aleatorio asociado con un mensaje individual
Vehicle	–	Contenedor de información sobre el vehículo. Contiene varios elementos módulo (*module*)
	name	Nombre del vehículo, si existe
	model	Nombre del modelo del vehículo que proporciona el fabricante
	modelid	Nombre del modelo del vehículo
	vehicleid	ID del vehículo definido por el fabricante/proveedor del vehículo
	locale	Información sobre el emplazamiento del vehículo

Cuadro 2 – Elementos del mensaje diagnóstico (envío)
(*diagnose (submit)*)

Elemento	Atributos del elemento	Descripción
Device	–	Contenedor de información sobre el dispositivo. Contiene varios elementos módulo (*module*)
	name	Nombre del dispositivo, si lo tiene
	type	Nombre del tipo de dispositivo, como "ECU de gestión de la potencia", "ECU de control de los cinturones de seguridad", etc.
	model	Nombre del modelo del dispositivo
	deviceid	ID del dispositivo definido por el fabricante/proveedor del vehículo
	hwversion	Versión de este módulo hardware
Module	–	Contenedor de información sobre el módulo, que contiene un elemento *hash* (de troceo)
	moduleid	ID de módulo es un identificador único que proporciona el fabricante/proveedor del vehículo
	version	Versión de este módulo software
	nextversion	Versión de la actualización de módulo en curso, utilizada principalmente para enviar un mensaje de respuesta durante una actualización
Hash	–	*Hash* es un contenedor de un valor *hash* con información de su algoritmo de *hash* (troceo)
	algorithm	Algoritmo de la función *hash* (por ejemplo, SHA-3, SHA-256, etc.)
IssuedTime	–	Hora de transmisión de este mensaje
ExpirationTime	–	Hora de expiración de este mensaje

Cuadro 3 – Ejemplo de mensaje diagnóstico (envío)
(*diagnose (submit)*)

```
<message protocol="1.0" version="1.0.2" type="diagnose" subtype="submit"
sessionid="{7316A97D-8C04-428B-B498-0F51087A1093}" ownerid="oid987239487"
messageid="{BBCE3B0B-2A10-443A-97D0-EF4650457422}" trustlevel="3">
    <Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale="CH"/>
    <Device name="device1" type="ECU" model="model1" id="did0987234" hwversion="HB-01">
        <Module moduleid="{66E6F81E-F293-4531-B2FC-A93F177373AA }" version="1.3.23.0"
nextversion=""/>
            <Hash algorithm="SHA-256">hash data here</Hash>
        </Module>
        <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}" version="2.4.34.0"
nextversion=""/>
            <Hash algorithm="SHA-256">hash data here</Hash>
        </Module>
    </Device>
    <Device name="device2" type="ECU" model="model1" id="did0987234" hwversion="HC-02">
        <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}" version="3.5.45.0"
nextversion=""/>
            <Hash algorithm="SHA-256">hash data here</Hash>
        </Module>
    </Device>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

7.2.2.2 Mensajes diagnóstico (notificación de recepción) (*diagnose (receipt)*)

Después de enviar al servidor de actualización la información del software del vehículo con el mensaje diagnóstico (envío) (*diagnose (submit)*), éste devuelve una notificación de recepción con el mensaje diagnóstico (notificación de recepción), para informar al vehículo que el envío ha tenido éxito y que puede proceder a la fase siguiente (verificación de actualización, *update_check*)

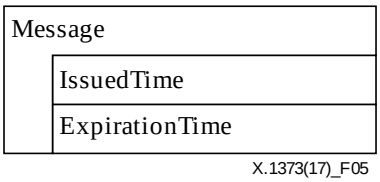

Figura 5 – Estructura del mensaje diagnóstico (notificación de recepción) (*diagnose (receipt)*)

Cuadro 4 – Elementos del mensaje diagnóstico (notificación de recepción) (*diagnose (receipt)*)

Elemento	Atributos del elemento	Descripción
Message	–	Contenedor del mensaje
	protocol	Siempre es "1.0"
	version	Número de la versión del remitente del mensaje
	type	Tipo de mensaje (siempre "diagnóstico", "*diagnose*")
	subtype	Subtipo de mensaje (siempre "notificación de recepción", "*receipt*")
	sessionid	ID de sesión es un identificador mundialmente único (GUID) aleatorio asociado a la sesión de diagnóstico. Un ID de sesión idéntico se aplica a los mensajes diagnóstico (petición, informe, envío y notificación de recepción)
	trustlevel	El nivel de confianza (*trust level*) se determina en base a la capacidad de seguridad y a los requisitos de protección del dispositivo que ha generado el mensaje
	ownerid	ID del propietario suministrado por el fabricante/proveedor del automóvil
	messageid	ID del mensaje es un aleatorio asociado con un mensaje individual
	status	Acuse de recibo del informe de diagnóstico (envío)
IssuedTime	–	Hora de transmisión de este mensaje
ExpirationTime	–	Hora de expiración de este mensaje

Cuadro 5 – Ejemplo del mensaje diagnóstico (notificación de recepción) (*diagnose (receipt)*)

```
<message protocol="1.0" version="1.0.2" type="diagnose" subtype="receipt"
sessionid="{7316A97D-8C04-428B-B498-0F51087A1093}" ownerid="oid987239487"
messageid="{E313159C-2081-4A10-B61D-4F81D074D54F}" trustlevel="3" status=”yes”>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

7.2.3 Mensajes verificación de actualización (*update_check*)

Una vez cargada la información del software en el servidor de actualización mediante un mensaje diagnóstico (*diagnose*), el servidor de actualización inicia un análisis para determinar qué módulos de actualización necesita el vehículo, algo que puede durar un tiempo prolongado. El mensaje verificación de actualización se envía periódicamente para interrogar sobre esa decisión al servidor de actualización. Existen dos subtipos del mensaje verificación de autorización, a saber, petición y respuesta, que se transfieren entre la VMG y el servidor de actualización.

7.2.3.1 Mensaje verificación de actualización (petición) (*update_check (request)*)

El mensaje verificación de actualización (petición) se transmite desde la VMG al servidor de actualización para verificar la necesidad de actualizaciones. Este mensaje incluye información sobre los módulos que deben ser inspeccionados, algo bastante similar al mensaje diagnóstico (notificación de recepción) (*diagnose (receipt)*).

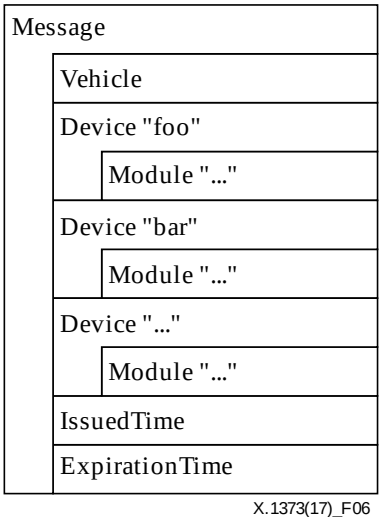

Figura 6 – Estructura del mensaje verificación de actualización (petición) (*update_check (request)*)

Cuadro 6 –Elementos del mensaje verificación de actualización (petición) (*update_check (request)*)

Elemento	Atributos del elemento	Descripción
Message	–	Contenedor del mensaje
	protocol	Siempre es "1.0"
	version	Número de la versión del remitente del mensaje
	type	Tipo de mensaje (siempre "verificación de actualización", "*update_check*")
	subtype	Subtipo de mensaje (siempre "petición", "*request*")
	sessionid	ID de sesión es un identificador mundialmente único (GUID) aleatorio asociado a la sesión verificación de actualización ("*update_check*"). Un ID de sesión idéntico se aplica a los mensajes verificación de actualización (petición y respuesta)
	trustlevel	El nivel de confianza (*trust level*) se determina en base a la capacidad de seguridad y a los requisitos de protección del dispositivo que ha generado el mensaje
	ownerid	ID del propietario suministrado por el fabricante/proveedor del automóvil
	messageid	ID del mensaje es un aleatorio asociado con un mensaje individual

Cuadro 6 –Elementos del mensaje verificación de actualización (petición) (*update_check (request)*)

Elemento	Atributos del elemento	Descripción
Vehicle	–	Contenedor de información sobre el vehículo. Contiene varios elementos módulo (*module*)
	name	Nombre del vehículo, si existe
	model	Nombre del modelo del vehículo que proporciona el fabricante
	modelid	Nombre del modelo del vehículo
	vehicleid	ID del vehículo definido por el fabricante/proveedor
	locale	Información sobre el emplazamiento del vehículo
Device	–	Contenedor de información sobre el dispositivo. Contiene varios elementos módulo (*module*)
	name	Nombre del dispositivo, si lo tiene
	type	Nombre del tipo de dispositivo, como "ECU de gestión de la potencia", "ECU de control de los cinturones de seguridad", etc.
	model	Nombre del modelo del dispositivo
	deviceid	ID del dispositivo definido por el fabricante/proveedor del vehículo
	hwversion	Versión este módulo hardware actual
Module	–	Contenedor del módulo de información que contiene un elemento *hash*
	moduleid	ID de módulo es un identificador único que proporciona el fabricante/proveedor del vehículo
	version	Versión de este módulo software
	nextversion	Versión de la actualización de módulo en curso, utilizada principalmente para enviar un mensaje de respuesta durante una actualización
IssuedTime	–	Hora de transmisión de este mensaje
ExpirationTime	–	Hora de expiración de este mensaje

Cuadro 7 – Ejemplo de mensaje verificación de actualización (petición) (*update_check (request)*)

```
<message protocol="1.0" version="1.0.2" type="update_check" subtype="request"
sessionid="{19622672-A025-4500-B26A-BB626BC61C62}" ownerid="oid987239487"
messageid="{4604A6C9-F72F-452B-ABA5-94168CCD8FD6}" trustlevel="3">
    <Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale=”CH”/>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion=”HB-01”>
        <Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}"
version="1.3.23.0" nextversion=""/>
        <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion=""/>
    </Device>
    <Device name="device2" type="ECU" model="model1" id="did0987234"
hwversion=”HC-02”>
        <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion=""/>
    </Device>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

7.2.3.2 Mensaje verificación de actualización (respuesta) (*update_check (response)*)

En respuesta al mensaje verificación de actualización (petición) (*update_check (request)*), el servidor de actualización devuelve el resultado del análisis. Si algunos módulos del vehículo necesitan actualización, el mensaje verificación de actualización (respuesta) descarga las URL necesarias para obtener los módulos de actualización. Obsérvese que un mensaje actualización no contiene el fichero binario del módulo de actualización, sino que la VMG lo descarga mediante la conexión que establece en base a la información de recursos incluida en el mensaje verificación de actualización (respuesta).

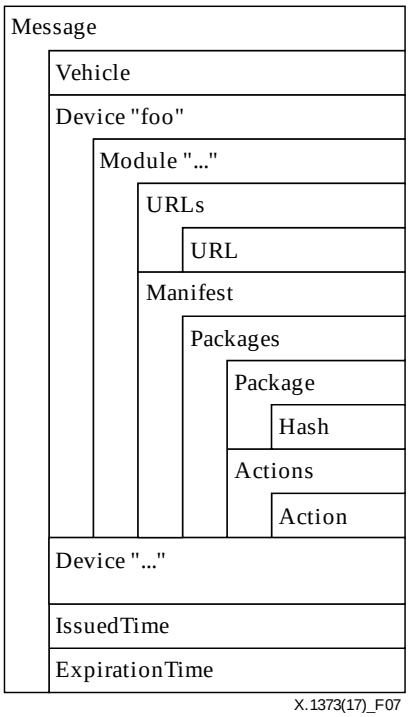

Figura 7 – Estructura del mensaje verificación de actualización (respuesta) (*update_check (response)*)

Cuadro 8 – Elementos del mensaje verificación de actualización (respuesta) (*update_check (response)*)

Elemento	Atributo del elemento	Descripción
Message	–	Contenedor del mensaje
	protocol	Siempre es "1.0"
	version	Número de la versión del remitente del mensaje
	type	Tipo de mensaje (siempre "verificación de actualización" ("*update_check*"))
	subtype	Subtipo de mensaje (siempre "respuesta" ("*response*"))
	sessionid	ID de sesión es un identificador mundialmente único (GUID) aleatorio asociado a la sesión de verificación de actualización (*update_check*). Un ID de sesión idéntico se aplica a los mensajes verificación de actualización (petición y respuesta)
	trustlevel	El nivel de confianza (*trust level*) está determinado por la capacidad de seguridad y los requisitos de protección del dispositivo que ha generado el mensaje
	ownerid	ID del propietario suministrado por el fabricante/proveedor del automóvil
	messageid	ID del mensaje es un aleatorio asociado con un mensaje individual

Cuadro 8 – Elementos del mensaje verificación de actualización (respuesta) (*update_check (response)*)

Elemento	Atributo del elemento	Descripción
Vehicle	–	Contenedor de información sobre el vehículo. Contiene varios elementos módulo (*module*)
	name	Nombre del vehículo, si existe
	model	Nombre del modelo del vehículo que proporciona el fabricante
	modelid	Nombre del modelo del vehículo
	vehicleid	ID del vehículo definido por el fabricante/proveedor
	locale	Información sobre el emplazamiento del vehículo
Device	–	Contenedor de información sobre el dispositivo. Contiene varios elementos módulo (*module*)
	name	Nombre del dispositivo, si lo tiene
	type	Nombre del tipo de dispositivo, como "ECU de gestión de la potencia", "ECU de control de los cinturones de seguridad", etc.
	model	Nombre del modelo del dispositivo
	deviceid	ID del dispositivo definido por el fabricante/proveedor del vehículo
	hwversion	Versión de este módulo hardware
Module	–	Contenedor del módulo de información que contiene un elemento de troceo (*hash*)
	moduleid	ID de módulo es un identificador único que proporciona el fabricante/proveedor del vehículo
	version	Versión de este módulo software
	nextversion	Versión de la actualización de módulo en curso, utilizada principalmente para enviar un mensaje de respuesta durante una actualización
	status	Situación de la inspección de actualización. Toma el valor "*noupdate*" si no existen actualizaciones, y el valor "*ok*" si existe alguna actualización para este módulo
URLs	–	Contenedor de elementos URL en caso de que haya actualizaciones. Este elemento está incluido en un elemento módulo (*module*) cuando la situación (*status*) es ok
URL	–	URL del fichero actualizado. El elemento URL debe incluirse al menos dos veces como respaldo del primer URL (servidor). El número máximo de elementos URL debe determinarse cuidadosamente en función de los recursos de computación de la VMG
	codebase	Ubicación del fichero de actualización
Manifest	–	Describe el modulo que debe instalarse y las actuaciones necesarias a realizar con dichos ficheros
	version	Nuevo número de la versión específica de este módulo software
Packets	–	Conjunto de ficheros que deben instalarse. No contiene atributos. Contiene uno o más elementos vástagos paquete (*packet*)
Packet	–	Un único fichero para su instalación en el módulo
	name	Describe el nombre del fichero del módulo de actualización
	size	Contiene el tamaño en bytes del módulo de actualización
	description	Descripción del módulo de actualización
Hash	–	Contenedor de un valor de troceo (*hash*) e información sobre su algoritmo *hash*
	algorithm	Algoritmo de la función *hash* (por ejemplo, SHA-3, SHA-256, etc.)

Cuadro 8 – Elementos del mensaje verificación de actualización (respuesta) (*update_check (response)*)

Elemento	Atributo del elemento	Descripción
Actions	–	Actuaciones que deben realizarse para instalar el módulo una vez que se han descargado satisfactoriamente todos los elementos paquetes
Action	–	Actuación específica singular que debe realizarse como parte del proceso de instalación
	event	Cadena fija que señala cuándo debe ejecutarse esta actuación. Una de entre "preinstalación", "instalación", "postinstalación" y "actualización"
	arguments	Argumentos que deben pasarse al proceso de instalación
IssuedTime	–	Hora de transmisión de este mensaje
ExpirationTime	–	Hora de expiración de este mensaje

Cuadro 9 – Ejemplo del mensaje verificación de actualización (respuesta) (*update_check (response)*)

```
<message protocol="1.0" version="1.0.2" type="update_check" subtype="response "
sessionid="{19622672-A025-4500-B26A-BB626BC61C62}" ownerid="oid987239487"
messageid="{4604A6C9-F72F-452B-ABA5-94168CCD8FD6}" trustlevel="3">
    <Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale=”CH”/>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion=”HB-01”>
        <Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}"
version="1.3.23.0" nextversion="" status="ok">
            <Urls>
                <Url codebase="http://update1.server/this/is/an/example/url/"/>
                <Url codebase="http://update2.server/this/is/an/example/url/"/>
                <Url codebase="http://update3.server/this/is/an/example/url/"/>
            </Urls>
            <Manifest version="1.4.0">
                <Packages>
                    <Package name="module1.bin" size="589" description=”This update
provides ...”>
                        <Hash algorithm="SHA-256">hash data here</Hash>
                    </Package>
                </Packages>
                <Actions>
                    <Action arguments="--argument-for-installation"
event="install"/>
                </Actions>
            </Manifest>
        </Module>
        <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion="" status="noupdate">
        </Module>
    </Device>
    <Device name="device2" type="ECU" model="model1" id="did0987234"
hwversion=”HC-02”>
        <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion="" status="noupdate">
        </Module>
    </Device>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

7.2.4 Mensajes actualización (*update*)

El proceso de actualización realizado en el interior del vehículo está fuera del alcance de esta Recomendación. No se incluye definición ni especificación alguna de los mensajes de actualización.

7.2.5 Mensajes informe de actualización (*update_report*)

Como paso final de la secuencia del procedimiento de actualización, la VMG envía al servidor de actualización todos los informes recopilados sobre la aplicación, es decir, instalación, de una actualización en los dispositivos, de forma que el servidor de actualización pueda acceder a cada vehículo y gestionarlo a distancia. La VMG envía un informe al servidor de actualización mediante un mensaje informe de actualización (envío) (*update_report (submit)*). Finalmente, el servidor actualización envía una notificación de recepción del informe (mensaje informe de actualización (notificación de recepción), (*update_report (receipt)*) a la VMG para informarle del final del proceso completo de actualización.

7.2.5.1 Mensaje informe de actualización (envío) (*update_report (submit)*)

Tras recopilar de los dispositivos informes de la instalación, la VMG envía al servidor de actualización un mensaje informe de actualización (envío). Este mensaje incluye los resultados de las instalaciones, así como la situación actual del software, de forma similar al mensaje diagnóstico (envío) (*diagnose (submit)*).

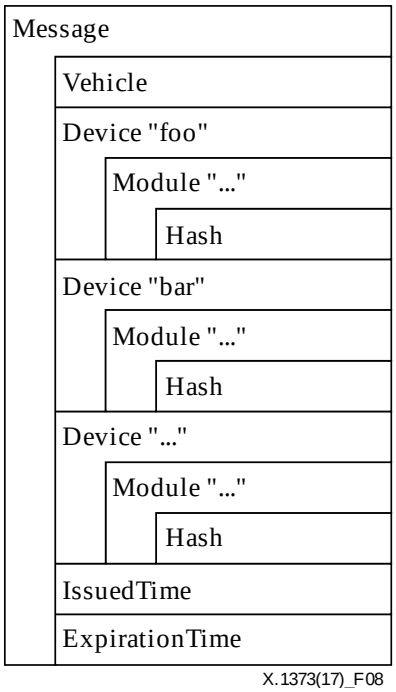

Figura 8 – Estructura del mensaje informe de actualización (envío) (*update_report (submit)*)

Cuadro 10 – Elementos del mensaje informe de actualización (envío) (*update_report (submit)*)

Elemento	Atributos del elemento	Descripción
Message	–	Contenedor del mensaje
	protocol	Siempre es "1.0"
	version	Número de la versión del remitente del mensaje
	type	Tipo de mensaje (siempre "informe de actualización" ("*update_report*"))
	subtype	Subtipo de mensaje (siempre "envío" ("*submit*"))
	sessionid	ID de sesión es un identificador mundialmente único (GUID) aleatorio asociado a la sesión informe de actualización (*update_report*). Un ID de sesión idéntico se aplica a los mensajes informe de actualización (envío y notificación de recepción)
	trustlevel	El nivel de confianza (*trust level*) está determinado por la capacidad de seguridad y los requisitos de protección del dispositivo que ha generado el mensaje
	ownerid	ID del propietario suministrado por el fabricante/proveedor del automóvil
	messageid	ID del mensaje es un aleatorio asociado con un mensaje individual
Vehicle	–	Contenedor de información sobre el vehículo. Contiene varios elementos "*module*"
	name	Nombre del vehículo, si existe
	model	Nombre del modelo del vehículo que proporciona el fabricante
	modelid	Nombre del modelo del vehículo
	vehicleid	ID del vehículo definido por el fabricante/proveedor
	locale	Información sobre el emplazamiento del vehículo
Device	–	Contenedor de información sobre el dispositivo. Contiene varios elementos módulo (*module*)
	name	Nombre del dispositivo, si lo tiene
	type	Nombre del tipo de dispositivo, como "ECU de gestión de la potencia", "ECU de control de cinturones de seguridad", etc.
	model	Nombre del modelo del dispositivo
	deviceid	ID del dispositivo definido por el fabricante/proveedor del vehículo
	hwversion	Versión de este módulo hardware
Module	–	Contenedor del módulo de información que contiene un elemento *hash*
	moduleid	ID de módulo es un identificador único que proporciona el fabricante/proveedor del vehículo
	version	Versión de este módulo software
	nextversion	Versión de la actualización de módulo en curso, utilizada principalmente para enviar un mensaje de respuesta durante una actualización
	status	Resultado de la instalación de este módulo
Hash	–	*Hash* es el contenedor de un valor de *hash* (troceo) y de información sobre su algoritmo *hash*
	algorithm	Algoritmo de la función hash (por ejemplo, SHA-3, SHA-256, etc.)
IssuedTime	–	Hora de transmisión de este mensaje
ExpirationTime	–	Hora de expiración de este mensaje

Cuadro 11 – Ejemplo de mensaje informe de actualización (envío) (*update_report (submit)*)

```
<message protocol="1.0" version="1.0.2" type="update_report" subtype="submit"
sessionid="{9AFFEB5A-F36B-4E05-819F-5BDCD3A0E3EC}" ownerid="oid987239487"
messageid="{3F7A6438-8306-447E-A1BB-99CED4C2B6AD}" trustlevel="3">
    <Vehicle name="vehicleName" modelid="mid34987130" type="ECU"
model="modelName" vid="vid0987234" locale=”CH”/>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion=”HB-01”>
        <Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}"
version="1.4.0" nextversion="" status="ok">
            <Hash algorithm="SHA-256">hash data here</ModuleHash>
        </Module>
        <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion="" status="ok">
            <Hash algorithm="SHA-256">hash data here</ModuleHash>
        </Module>
    </Device>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion=”HB-02”>
        <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion="" status=”ok”>
            <Hash algorithm="SHA-256">hash data here</ModuleHash>
        </Module>
    </Device>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

7.2.5.2 Mensaje informe de actualización (notificación de recepción) (*update_report (receipt)*)

Al final de la secuencia, el servidor de actualización envía un mensaje informe de actualización (notificación de recepción) (*update_report (receipt)*) a la VMG, que informa al vehículo de la finalización del proceso de actualización. El formato de mensaje informe de actualización (notificación de recepción) es muy similar al del mensaje diagnóstico (notificación de recepción) (*diagnose (receipt)*).

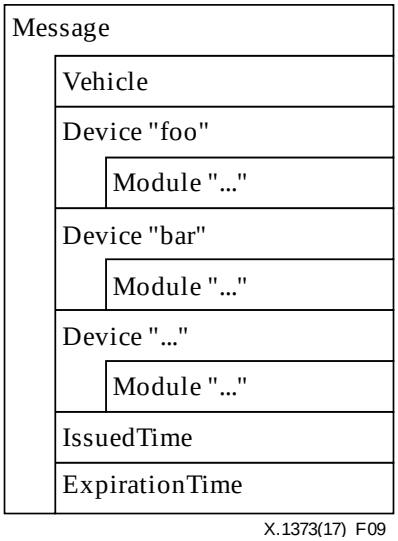

Figura 9 – Estructura del mensaje informe de actualización (notificación de recepción) (*update_report (receipt)*)

Cuadro 12 – Elementos del mensaje informe de actualización (notificación de recepción) (*update_report (receipt)*)

Elemento	Atributos del elemento	Descripción
Message	–	Contenedor del mensaje
	protocol	Siempre es "1.0"
	version	Número de versión del remitente del mensaje
	type	Tipo de mensaje (siempre "informe de actualización" ("*update_report*"))
	subtype	Subtipo de mensaje (siempre "notificación de recepción" ("*receipt*"))
	sessionid	ID de sesión es un identificador mundialmente único (GUID) aleatorio asociado a la sesión informe de actualización (*update_report*). Un ID de sesión idéntico se aplica a los mensajes informe de actualización (envío y notificación de recepción)
	trustlevel	El nivel de confianza (*trust level*) está determinado por la capacidad de seguridad y los requisitos de protección del dispositivo que ha generado el mensaje
	ownerid	ID del propietario suministrado por el fabricante/proveedor del automóvil
	messageid	ID del mensaje es un aleatorio asociado con un mensaje individual
Vehicle	–	Contenedor de información sobre el vehículo. Contiene varios elementos módulo (*module*)
	name	Nombre del vehículo, si existe
	model	Nombre del modelo del vehículo que proporciona el fabricante
	modelid	Nombre del modelo del vehículo
	vehicleid	ID del vehículo definido por el fabricante/proveedor del vehículo
	locale	Información sobre el emplazamiento del vehículo
Device	–	Contenedor de información sobre el dispositivo. Contiene varios elementos módulo (*module*)
	name	Nombre del dispositivo, si lo tiene
	type	Nombre del tipo de dispositivo, como "ECU de gestión de la potencia", "ECU de control de los cinturones de seguridad", etc.
	model	Nombre del modelo del dispositivo
	deviceid	ID de dispositivo definido por el fabricante/proveedor del vehículo
	hwversion	Versión de este módulo hardware
Module	–	Contenedor del módulo de información que contiene un elemento de troceo (*hash*)
	moduleid	ID de módulo es un identificador único que proporciona el fabricante/proveedor del vehículo
	version	Versión de este módulo software
	nextversion	Versión de la actualización de módulo en curso, utilizada principalmente para enviar un mensaje de respuesta durante una actualización
	status	Acuse de recibo del informe de este módulo
IssuedTime	–	Hora de transmisión de este mensaje
ExpirationTime	–	Hora de expiración de este mensaje

Cuadro 13 – Ejemplo del mensaje informe de actualización (notificación de recepción) (*update_report (receipt)*)

```
<message protocol="1.0" version="1.0.2" type="update_report" subtype="receipt"
sessionid="{9AFFEB5A-F36B-4E05-819F-5BDCD3A0E3EC}" ownerid="oid987239487"
messageid="{B5585708-6BDA-4B07-B2CB-5E9241F63271}" trustlevel="3">
    <Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale=”CH”/>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion=”HB-01”>
        <Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}"
version="1.4.0" nextversion="" status="ok"/>
        <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion="" status="ok"/>
    </Device>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion=”HB-02”>
        <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion="" status="ok"/>
        </Module>
    </Device>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

Apéndice I

Metodología de análisis del riesgo

(Este apéndice no es parte integrante de esta Recomendación.)

I.1 Metodología de análisis del riesgo basada en [b-JASO TP15002]

En este apéndice se proporciona información detallada relacionada con el Apéndice II. La información se basa en las directrices sobre seguridad de la información del automóvil [b-JASO TP15002].

La seguridad de la información se ha convertido en un factor muy importante en el diseño de sistemas integrados. En el ámbito de los sistemas de las tecnologías de la información (TI) se conoce un amplio abanico de ataques/amenazas a la seguridad, que permite que el conocimiento adquirido en la evaluación de riesgos pueda utilizarse en la fase de diseño de los sistemas de TI. En [ISO/CEI 15408-1] se describen los conceptos de seguridad básicos necesarios para la evaluación de productos TI. En el contexto de la evaluación, en [ISO/CEI 15408-1] se utiliza el término "objetivo de la evaluación" (TOE, *target of evaluation*). Algunos activos son entidades a las que el propietario del TOE atribuye un determinado valor. [ISO/CEI 15408-1] pretende establecer los objetivos de seguridad de un TOE, algo que constituye una declaración del propósito de luchar contra las amenazas identificadas y/o cumplir las políticas y/o principios de seguridad de la organización. Las amenazas suponen un riesgo para los activos en función de la probabilidad de que éstas se materialicen y de la repercusión sobre los activos cuando eso ocurre. No obstante, en [ISO/CEI 15408-1] no se especifica cómo realizar la extracción de la amenaza (su identificación y eliminación) y el análisis del riesgo.

En este Apéndice se describen las amenazas identificadas de los sistemas integrados y se realiza un análisis del riesgo de acuerdo con [ISO/CEI 15408-1]. Se pretende que el análisis del riesgo no dependa del conocimiento que exista sobre el diseño en materia de seguridad. Por tanto, en esta Recomendación el método de análisis del riesgo CRSS [b-JASO TP15002] calcula un nivel de riesgo de la amenaza para el sistema integrado. Este método se caracteriza por lo siguiente: 1) formulación del resultado en los pasos de definición del modelo del sistema y de análisis de la amenaza; 2) establecimiento del valor del parámetro utilizando la información obtenida en los pasos anteriores.

El proceso de evaluación de la seguridad según [b-JASO TP15002] consta de las fases siguientes:

Fase 1: Definición del objetivo de la evaluación

Fase 2: Identificación de las amenazas

Fase 3: Análisis del riesgo

A continuación se describe cada fase.

I.1.1 Fase 1: Definición del objetivo de la evaluación

Clarificación del objetivo para el que se identifican amenazas en la fase siguiente.

En la fase 1 se llevan a cabo los cuatro pasos siguientes:

Paso 1: Establecimiento de conocimiento compartido

En base a la documentación que contiene la visión general del sistema, y a fin de que todos los miembros del proyecto tengan el mismo nivel de conocimiento sobre el ciclo de vida del sistema objetivo y la construcción del sistema, se elabora, entre otras, una representación gráfica de cómo está construido el sistema, las funciones del sistema y los datos utilizados por el mismo.

Paso 2: Construcción de una representación gráfica del modelo del objetivo de la evaluación

Se elabora una "representación gráfica del modelo del objetivo de la evaluación" que identifica los componentes del sistema y los flujos de información entre estos.

Paso 3: Definición de una visión general de las funciones módulo

Para cada módulo componente descrito en la representación gráfica del modelo del objetivo de la evaluación, se clarifican las funciones suministradas y los activos que éstas protegen. De esta forma, se crea un cuadro con una "visión general de las funciones del módulo".

Las amenazas a la seguridad pueden describirse en los términos siguientes: "quiénes son agentes de la amenaza y qué actuaciones adversas realizan sobre qué activos" del sistema objetivo de la evaluación. Además de información, algo que habitualmente se trata como un activo a proteger, los activos que componen los sistemas integrados del automóvil también incluyen el software del sistema integrado y las funciones que controlan mecanismos como el motor o los frenos.

A partir de la naturaleza de los activos y de los diagramas de flujo de los datos que especifican flujos de datos relacionados con esos activos, se elabora un modelo del sistema.

Respecto a qué actuaciones adversas pueden materializarse (las amenazas), se analiza todo lo que pueda ocurrir en cada punto de entrada, así como todos los posibles tipos de fallos en cada tipo de activo en materia de confidencialidad, integridad o disponibilidad. En este sentido, es importante que el desarrollo operacional de las funciones de un sistema de TI del automóvil sea el previsto y se prevengan fallos que afecten a la integridad o la disponibilidad. Igualmente, es importante que se proteja la información intercambiada entre los servidores centrales así como los dispositivos del sistema de transporte inteligente (ITS) del vehículo de su divulgación y modificación indeseada, así como de fallos que afecten a su confidencialidad o integridad. En el Cuadro I.1 se muestran ejemplos de información y de activos que deben proteger los vehículos.

Cuadro I.1 – Ejemplos de información y de otros activos que deben proteger los vehículos (seguridad de la información del vehículo)

Objetos que deben protegerse	Descripción
Operación de las "funciones de control básicas"	Coherencia y disponibilidad de las "funciones de control básicas", entorno de ejecución de las "funciones de control básicas", comunicaciones operacionales
Información única del vehículo	Información singular el vehículo (ID del vehículo, ID del dispositivo, etc.), código de autenticación e información acumulada, como historial de circulación e historial operacional del vehículo
Información de la situación del vehículo	Datos representativos de la situación del vehículo, como ubicación, velocidad y destino
Información de usuario	Información personal, información de autenticación, información de facturación, historial de uso e historial operacional del usuario (conductor/pasajeros)
Software	Software relacionado con las "funciones de control básicas" y las "funciones ampliadas" del vehículo. Un ejemplo es el software para las ECU
Contenidos	Datos para aplicaciones de vídeo, música, mapas, etc.
Información de configuración	Ajuste de datos que determinan el comportamiento del hardware, software, etc.

Paso 4: Definición del alcance del objetivo de un ciclo de vida

Se crea un "cuadro de ciclos de vida" que clarifique todo el ciclo vital del sistema objetivo.

Se consideran agentes de la amenaza a todas aquellas personas involucradas en algún momento del ciclo de vida del vehículo, que incluye, la fabricación, el uso por parte del propietario, ya sea un vehículo comprado nuevo o de segunda mano, e incluso la reventa del vehículo. Ello es debido a que la información confidencial que poseen los sistemas integrados del automóvil permanece almacenada y es accesible no sólo durante la utilización normal del vehículo, sino también en otras fases, como la fabricación, la entrega del vehículo o el servicio de mantenimiento del mismo. En el Cuadro I.2 se muestra información detallada sobre el ciclo de vida del TOE.

Cuadro I.2 – Ciclo de vida del TOE

Fase	Subfase	Visión general	Personas involucradas
Operación	Transporte	El personal del fabricante del equipo original (OEM) transporta un vehículo fabricado hasta el concesionario. Esta labor se encarga a un transportista.	• Personal del OEM • Transportista • Personal del concesionario • Tercero
	Entrega del vehículo	El personal del concesionario entrega el vehículo al propietario.	• Personal del concesionario • Propietario • Tercero
	Funcionamiento/ uso normal	El propietario o usuario hace uso el vehículo. Un administrador del servidor actúa como administrador del servidor de actualización del software. Un operador de telecomunicaciones proporciona la red de comunicaciones.	• Propietario o usuario • Administrador del servidor • Operador de telecomunicaciones • Tercero
	Funcionamiento/ uso normal Descarga del software	Para preparar la actualización del software a través del servidor de actualización, el vehículo descarga el software de éste último.	• Personal del OEM • Personal del proveedor • Administrador del servidor • Operador de telecomunicaciones • Tercero
	Mantenimiento (actualización del software a través del servidor de actualización) Actualización del software	Una vez estacionado el vehículo, se lleva a cabo la actualización del software. El administrador del servidor realiza la labor de administrador del servidor de actualización. El operador de telecomunicaciones actúa como proveedor de la red de comunicaciones. El personal del proveedor realiza la función de proveedor de servicio que utiliza la red de comunicaciones.	• Personal del OEM • Personal del proveedor • Administrador del servidor • Operador de telecomunicaciones • Tercero
	Mantenimiento (actualización del software a través del conector de diagnosis a bordo, OBD)	El personal del concesionario o el personal de mantenimiento en fábrica realiza la actualización del software a través de un conector OBD durante la inspección del vehículo.	• Personal del concesionario • Personal de mantenimiento de fábrica • Propietario o usuario • Tercero

I.1.2 Fase 2: Identificación de las amenazas

Se identifican los problemas de seguridad que afectan al TOE definidos en la fase 1.

En la fase 2 se llevan a cabo los tres pasos siguientes:

Paso 1: Determinación de supuestos

Al objeto de clarificar el ámbito en que se identifican las amenazas, se definen supuestos sobre la de la representación gráfica del modelo del objetivo de la evaluación, la visión general de las funciones del módulo y el cuadro del ciclo de vida. El ámbito en el que se identifican las amenazas en la fase 2 es limitado. Se definen los supuestos que afectan al entorno del TOE. A cada amenaza identificada se asigna un identificador con el prefijo "A". De esta forma, se construye un "cuadro de supuestos".

El cálculo del TOE se realiza teniendo en cuenta los supuestos siguientes:

A.Reliability_OfficeStaff (fiabilidad del personal del OEM/personal del proveedor/personal del concesionario/personal de mantenimiento en fábrica)

El personal del OEM o del proveedor no accede físicamente al vehículo objeto de ataque. Además, el personal del concesionario/personal de mantenimiento en fábrica no accede físicamente al vehículo en su funcionamiento/utilización normal.

A.Reliability_ServiceProvider (fiabilidad del administrador del proveedor de servicio/operador de telecomunicaciones)

El administrador del servidor de actualización/operador de telecomunicaciones no accede físicamente al vehículo. Además, el administrador del servidor de actualización/operador de telecomunicaciones no genera amenazas de forma intencionada.

A.Reliability_User (fiabilidad del propietario/usuario)

En la fase de mantenimiento, el propietario/usuario no accede físicamente al vehículo objeto de ataque.

En la fase de mantenimiento, el propietario/usuario no accede físicamente al vehículo. Además, en condiciones normales de funcionamiento/utilización, el propietario/usuario siempre cierra la puerta con llave. Además, el propietario/usuario no permite que otras personas no autorizadas accedan al interior del vehículo en la fase normal de uso y funcionamiento.

A.Operation_Server (protección del servidor al margen del objetivo de la evaluación)

El servidor de actualización está operado correctamente, es decir, las personas concernidas no tendrán acceso ni podrán manipular información almacenada en el servidor.

A.Control_OBD-Tool (protección del dispositivo de medición, etc., al margen del objetivo de la evaluación)

Un dispositivo de medición se opera correctamente, es decir, las personas concernidas no tienen acceso ni pueden manipular información almacenada en el dispositivo de medición.

Paso 2: Identificación de amenazas

Las amenazas se identifican desde las perspectivas recogidas en el Cuadro I.3 en base a la representación gráfica del modelo del objetivo de la evaluación, la visión general de las funciones del módulo y el cuadro del ciclo de vida de cada componente del sistema, es decir, dónde (puntos de entrada), quién (agentes de las amenazas), cuándo (fase del ciclo de vida), por qué (motivos) y qué (actuaciones adversas). Se asigna un identificador con el prefijo "T" para cada amenaza ("Threat") identificada. De esta forma, se construye un "cuadro de amenazas".

Al aplicar esas perspectivas al modelo del sistema, al ciclo de vida y a las actuaciones adversas estudiadas en la fase de definición del sistema objetivo de la evaluación (TOE) descrito en la cláusula I.1, pueden identificarse exhaustivamente los agentes responsables de las amenazas, qué actuaciones adversas realizan, sobre qué activos y en qué fases.

Cuadro I.3 – Perspectivas para la identificación de amenazas

Perspectiva	Explicación
Dónde	Identifica los puntos de entrada de los ataques
Quién	Identifica los agentes que son una amenaza
Cuándo	Identifica las fases del ciclo de vida de los ataques
Por qué	Identifica los motivos de los ataques
Qué	Identifica las actuaciones adversas

Paso 3: Establecimiento de la política de seguridad de la organización

La política de seguridad de una organización determina los requisitos de las contramedidas de seguridad por motivos distintos a las amenazas en sí mismas. Por ejemplo, las debidas al marco jurídico y a las directrices de la industria que han de aplicarse en el establecimiento del TOE y en el entorno operacional. Se identifican aquellos aspectos del marco jurídico o de la normativa de la empresa que afectan al funcionamiento del sistema que deben considerarse problemas de seguridad del TOE. A cada política de seguridad se le asigna un identificador con el prefijo "O". De esta forma, se construye un "cuadro de la política de seguridad de la organización".

No se aplica al TOE ninguna política en materia de seguridad de la organización.

I.1.3 Fase 3: Análisis del riesgo

En este paso se especifica los niveles de riesgo de todas las amenazas identificadas.

Para cada amenaza del cuadro de amenazas se calcula su nivel de prioridad.

En la fase 3 se llevan a cabo los dos pasos siguientes:

Paso 1: Evaluación del riesgo

El riesgo de una amenaza para un sistema de TI se ha evaluado típicamente a partir del valor de los activos y del coste del ataque, que depende de cómo se ejecuta la amenaza. Se trata de un enfoque eficaz cuando existen numerosos ejemplos de ataques y se ha podido llegar a un consenso sobre el coste del método de ataque, incluyendo factores como el tiempo necesario para ejecutarlo y las capacidades de las personas que lo realizan. En el caso de los sistemas integrados del automóvil, para los que se han identificado algunos ataques a nivel de laboratorio, no existe una variedad suficientemente amplia de métodos de ataque a sistemas de TI. En consecuencia, es difícil estimar el coste de los métodos de ataque.

I.1.3.1 CRSS

El sistema de puntuación de riesgos basado en el CVSS (CRSS) es un método de evaluación del riesgo basado en el sistema común de puntuación de vulnerabilidades (CVSS), es decir, el sistema de puntuación del riesgo (RSS) de [UIT-T X.1521] utilizado para puntuar la gravedad de las vulnerabilidades de los sistemas IT [b-JASO TP15002]. El CVSS se compone de tres grupos de métricas: básica, temporal y ambiental, compuesta cada una por un conjunto de métricas. Estos grupos de métricas se describen de la forma siguiente:

– Básica: representa las características intrínsecas y fundamentales de una vulnerabilidad que son invariables a lo largo del tiempo y en distintos entornos de usuario.

– Temporal: representa las características de una vulnerabilidad que cambian a lo largo del tiempo pero no para distintos entornos de usuario.
– Ambiental: representa las características de una vulnerabilidad que son pertinentes y específicas para un determinado entorno de usuario.

El CRSS evalúa las puntuaciones del riesgo mediante el *grupo de métricas básicas* de puntuación del CVSS. El grupo de métricas básicas identifica las características de una vulnerabilidad que son invariables con el tiempo y para distintos entornos de usuario. El vector de acceso, la complejidad del acceso y las métricas de autenticación, determinan la forma en que se accede a la vulnerabilidad y si se requieren o no condiciones especiales para explotarla.

El método CRSS asigna un valor a cada uno de los activos en términos de confidencialidad, integridad y disponibilidad, y a partir de ello calcula una puntuación del riesgo a partir de la facilidad para perpetrar un ataque y de sus efectos.

El grado de la facilidad con que se puede perpetrar un ataque se obtiene de métricas que reflejan la cercanía que precisan los agentes de la amenaza para acceder a los activos y la existencia de barreras que deben superarse para acceder a los mismos. En el Cuadro I.4 se muestra un ejemplo de clasificación respecto a la facilidad para perpetrar un ataque.

El grado de la incidencia mide cómo afecta directamente a un activo la explotación de una vulnerabilidad, cuyos efectos se definen en función del grado de pérdida de confidencialidad, integridad y disponibilidad. Por ejemplo, una determinada vulnerabilidad puede causar una pérdida parcial de integridad y de disponibilidad, pero no de confidencialidad. En el Cuadro I.5 se muestra un ejemplo de clasificación en función del grado de incidencia.

Cuadro I.4 – Ejemplo de clasificación con respecto a la facilidad para perpetrar un ataque (Cuadro D.2 de [b-JASO TP15002])

Parámetro	Principio considerado	Clasificación	Ejemplos
Vector de acceso (AV): Clasificación del origen del ataque	Clasificación en términos del origen (dónde) del ataque que causó la amenaza	Local (L)	Memoria USB
		Red adyacente (A)	Dispositivo de conexión WiFi
		Red (N)	Línea móvil
Complejidad del acceso (AC): Grado de complejidad de la condición necesaria para el ataque	Clasificación en términos del número de habilidades y conocimientos necesarios para realizar el ataque	Alto (H)	Se requieren tanto capacidad como conocimientos sobre el ataque
		Medio (M)	Se requieren conocimientos sobre el ataque
		Bajo (L)	No se requiere ninguna (o pocas) habilidad y conocimientos sobre el ataque
Autenticación (Au): Número de autenticaciones necesarias antes del ataque	Clasificación en términos del número de autenticaciones entre el activo y el agente que amenaza	Varias (M)	Varias
		Una (S)	Una
		Ninguna (N)	Innecesaria

Cuadro I.5 – Ejemplo de clasificación con respecto al grado de la incidencia (Cuadro D.3 de [b-JASO TP15002])

Activo	Clasificación	C: incidencia en la confidencialidad			I: incidencia en la integridad			A: incidencia en la disponibilidad		
		Ninguno	Parcial	Total	Ninguno	Parcial	Total	Ninguno	Parcial	Total
Función comunicación móvil	Servicio de actualización	S					S			S
Información de autenticación móvil				S			S	S		
Función obtención de software		S					S			S
Software				S			S	S		
Función actualización de software a distancia		S					S			S
Software				S			S	S		
Función recepción de GPS	Proceso de información	S				S			S	
Función conexión WiFi		S				S			S	
Información de autenticación WiFi			S			S		S		
Función conexión USB		S				S			S	
Función comunicación CAN	Control del vehículo	S					S			S
Función pasarela CAN		S					S			S
Tabla raíz				S			S	S		
Función conexión OBD		S					S			S

Para cada amenaza descrita en base a los cinco parámetros (dónde, quién, cuando, por qué, qué), se puede calcular la puntuación asociada al riesgo.

En el Cuadro I.6 se facilita un ejemplo de evaluación de la puntuación del riesgo.

Cuadro I.6 – Ejemplo de evaluación de la puntuación del riesgo (Cuadro D.4 de [b-JASO TP15002])

#	Amenaza	AV	AC	Au	Grado de facilidad del ataque	C	I	A	Grado del impacto	Valor del riesgo
1	T.control_fcn_Mobile_3rd_opearation_on_purpose of interfere-function	Red	Medio	Único		Innecesario	Grande	Grande		
		1	0,61	0,56	6,83	0	0,66	0,66	9,20	7,95
2	T.vehicle_status_WiFi_dealer_main_purpose_forge	Red adyacente	Único(s)	Único		Pequeño	Pequeño	Ninguno		
		0,646	0,71	0,56	5,14	0,275	0,275	0	4,94	4,14
3	T.info_transfer_USB_3rd_operation_pursuse_misop	Local	Bajo	Ninguno		Ninguno	Pequeño	Ninguno		
		0,395	0,71	0,704	3,95	0	0,275	0	2,86	2,11

Incluso en casos como los sistemas integrados utilizados en el ámbito del automóvil para los que hasta ahora existe un escaso conocimiento acumulado sobre amenazas a la seguridad, el método CRSS puede calcular analíticamente un valor del riesgo a partir de las definiciones de las amenazas y del sistema de evaluación. En la evaluación del riesgo también pueden considerarse factores como el riesgo para la vida, tratando las funciones como activos y, al objetivo de realizar una valoración, aumentando el valor estimado del activo en caso de funciones para las que la pérdida de integridad o de disponibilidad tiene graves consecuencias.

Paso 2: Identificación de las causas de las amenazas

Para cada amenaza cuya puntuación de riesgo supere un determinado valor, se realiza un análisis lógico de las causas mediante un árbol de fallas (FT).

I.2 Verificación de datos mediante algoritmos MAC

Los algoritmos MAC juegan un papel importante en el ámbito de la criptografía y la seguridad gracias a que mantienen la integridad del mensaje (autenticación). En términos de MAC, la ISO/CEI ha obtenido resultados significativos tales como [b-ISO/CEI 9797-1] (mecanismos que utilizan cifrado en bloque), [b-ISO/CEI 9797-2] (mecanismos que utilizan una función *hash* (de troceo) dedicada) y [b-ISO/CEI 9797-3] (mecanismos que utilizan una función *hash* universal).

Teniendo en cuenta los limitados recursos para la ejecución disponibles en un vehículo, es conveniente utilizar normas criptográficas ligeras. Desde esta perspectiva, existen dos tipos de MACs. El primero es un MAC basado en cifrado en bloque que utiliza [b-ISO/CEI 9797-1] y [b-ISO/CEI 29192-2] (cifrado en bloque ligero). El segundo es un MAC basado en una función *hash* que utiliza [b-ISO/CEI 9797-2] y [b-ISO/CEI 29192-5] (función *hash* ligera).

A fin de seleccionar posibles candidatos para la seguridad en el ámbito del automóvil, los algoritmos MAC han de ofrecer mejoras en términos de garantía de seguridad o de calidad de funcionamiento respecto a los algoritmos MAC normalizados existentes. El principal objetivo de utilizar MAC es conseguir implementaciones de software compactas y rápidas que funcionen sobre microcontroladores, así como la seguridad que requieren las aplicaciones objetivo. En particular, es deseable disponer de algoritmos MAC muy eficientes para su utilización en microcontroladores.

Apéndice II

Amenazas, requisitos de seguridad y controles de seguridad

(Este apéndice no es parte integrante de esta Recomendación.)

En el ámbito de los sistemas de las tecnologías de la información (TI) se conoce un amplio abanico de ataques/amenazas a la seguridad, que permite que el conocimiento adquirido en la evaluación de riesgos pueda utilizarse en la fase de diseño de los sistemas de TI. En [ISO/CEI 15408-1] se describen los conceptos de seguridad básicos necesarios para la evaluación de productos TI. En el contexto de la evaluación, en [ISO/CEI 15408-1] se utiliza el término 'objetivo de la evaluación' (TOE). Algunos activos son entidades a las que el propietario del TOE atribuye un determinado valor. [ISO/CEI 15408-1] pretende establecer los objetivos de seguridad de un TOE, algo que constituye una declaración del propósito de luchar contra las amenazas identificadas y/o cumplir las políticas de seguridad de la organización. Las amenazas suponen un riesgo para los activos en función de la probabilidad de que éstas se materialicen y de la repercusión sobre los activos cuando eso ocurre. No obstante, en [ISO/CEI 15408-1] no se especifica cómo realizar la identificación de una amenaza y el análisis del riesgo. Por otro lado, existen métodos conocidos para la identificación de amenazas y el análisis del riesgo. En este apartado, tras definir un TOE para la VMG, que se considera un componente principal y básico de la actualización segura de software, se identifican las principales amenazas y se analizan los requisitos de seguridad asociados a las mismas. Finalmente se proporcionan controles de seguridad de alto nivel para cumplir los requisitos de seguridad.

II.1 Definición de objetivo de la evaluación

En este apartado se define el TOE para la VMG, que se considera un componente principal y básico del proceso de actualización segura de software descrito en esta Recomendación.

La interfaz con el exterior se compone de un conector de diagnosis de abordo (OBD), un módulo de comunicaciones móviles, un dispositivo de recepción de señales del sistema mundial de navegación y determinación de la posición por satélite (GPS/GLONASS), equipamiento WiFi, equipamiento de radio/televisión, una conexión Bluetooth, una conexión con la CAN0/1, una interfaz de usuario para disco versátil digital/disco compacto (DVD/CD), un conector de bus serie universal (USB) y un conector digital seguro (SD). Aunque en este apartado el bus de datos en el interior del vehículo está compuesto por la red de área del controlador (CAN), un análisis idéntico es extensible a otros tipos de buses de datos en el vehículo, como MOST (transporte de sistemas orientados a los medios), LIN (red de interconexión local), FlexRay, etc.

En la Figura II.1 se define el TOE como el área encerrada por la línea de puntos, que realiza un control seguro de la comunicación como interfaz de conexión con el exterior del vehículo.

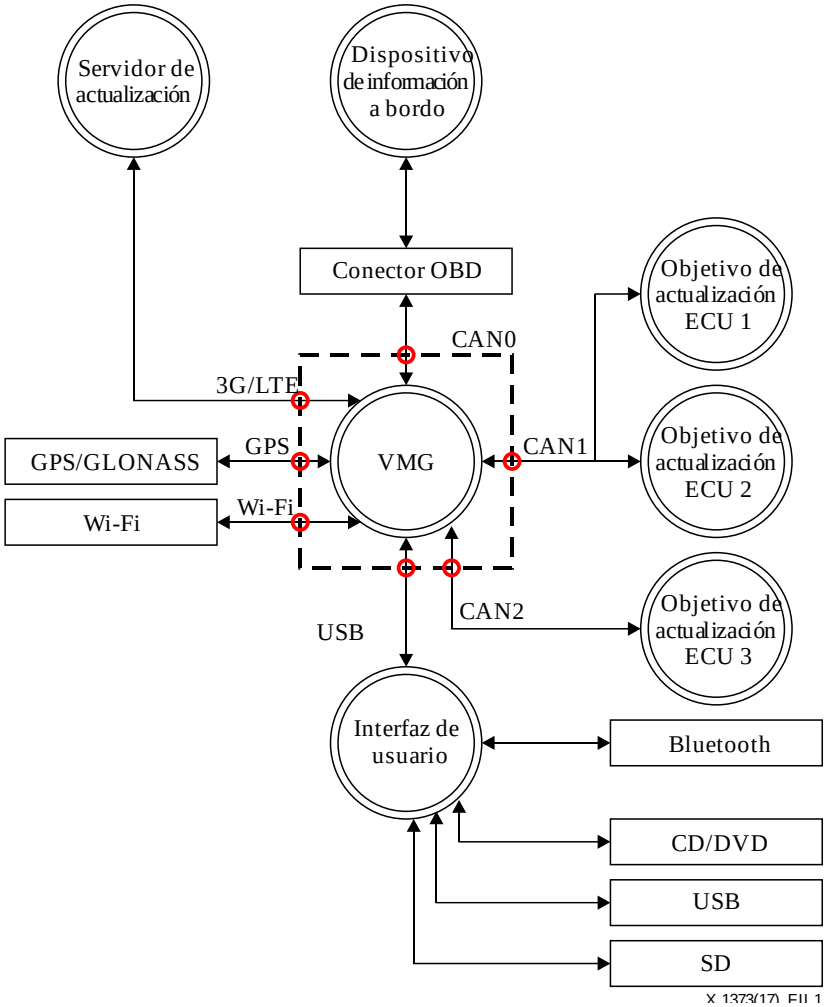

Figura II.1 – Modelo de TOE

En el Cuadro II.1 se presenta una visión general de las funciones de los módulos del TOE. Este cuadro también muestra las relaciones existentes entre las funciones descritas en el TOE y las características de seguridad más importantes, es decir, confidencialidad (C), integridad (I) y/o disponibilidad (D) a fin de definir los requisitos de seguridad basados en el TOE que se describen en la cláusula II.3.

Cuadro II.1 – Visión general de las funciones de los módulos del TOE

#	Módulo	Función		Activo	C	I	D
1	Pasarela móvil de vehículo	Función comunicación móvil	Se comunica con el servidor a través de una conexión móvil. Utiliza información de autenticación para autenticar el servidor.	Función comunicación móvil		S	S
				Información de autenticación	S	S	
		Función obtención de software	Obtiene el software a distancia a través de una conexión móvil o del conector OBD.	Función obtención del software		S	S
				Información del software	S	S	
		Función actualización de software a distancia	Actualiza el software a distancia a través de una conexión móvil o del conector OBD. Si el software se actualiza a distancia, durante la actualización utiliza información de seguridad para autenticar el servidor.	Función actualización de software a distancia		S	S
				Información de seguridad para la actualización	S	S	
				Información del software	S	S	
		Función recepción GPS	Recibe datos del satélite GPS.	Función recepción GPS		S	S
		Función conexión WiFi	Establece la conexión a Internet de los dispositivos a través de la conexión WiFi. Utiliza información de autenticación a través de la conexión WiFi.	Función conexión WiFi		S	S
				Información de autenticación	S	S	
		Función conexión USB	Comunica a través de un cable USB con la interfaz de usuario.	Función conexión USB		S	S
		Función comunicación CAN	Envía/recibe datos por la CAN a/desde la ECU.	Función comunicación CAN		S	S
		Función pasarela CAN	Encamina la comunicación por la CAN mediante referencias de una tabla de encaminamiento. Tabla de encaminamiento.	Función pasarela CAN		S	S
				Tabla de encaminamiento	S	S	
		Función conexión OBD	Envía datos por la CAN a través del conector OBD.	Función conexión OBD		S	S

II.2 Identificación de las principales amenazas

Este apartado identifica, en base a la definición del TOE para la actualización del software dla cláusula II.1, las amenazas más importantes localizadas en el TOE de conformidad con el marco de [ISO/CEI 15408-1].

En esta Recomendación se utiliza el método de análisis del riesgo descrito en el Apéndice I (informativo) para la identificación de las principales amenazas más importantes en base al TOE.

Cuadro II.2 – Principales amenazas basadas en el modelo del TOE

#	Etiqueta	Quién	Cuándo (fase)	Por qué	Dónde/Qué
1	T.DoS-Functions-From-OBD-Device	Tercero Personal de mantenimiento en fábrica	Funcionamiento normal Mantenimiento	Intencionadamente	Para funciones de activos de la VMG, suplanta al dispositivo de conexión del conector de OBD, envía un gran volumen de datos e interfiere con la funcionalidad
2	T.Malfunction-Functions-From-OBD-Device	Tercero Personal de mantenimiento en fábrica	Funcionamiento/ uso/mantenimiento normal Mantenimiento	Intencionadamente	Para funciones de activos de la VMG, suplanta al dispositivo de conexión del conector de OBD, envía datos no autorizados y causa un funcionamiento inadecuado de la funcionalidad
3	T.MissDoS-Functions-From-OBD-Device	Concesionario Personal de mantenimiento en fábrica	Mantenimiento	Accidentalmente	Para funciones de activos de la VMG, envía por error un gran volumen de datos o de datos no autorizados desde el dispositivo de conexión del conector OBD y causa un funcionamiento inadecuado de la funcionalidad
4	T.DoS-Functions-From-ECU	Tercero Personal de mantenimiento en fábrica	Funcionamiento/ uso/mantenimiento normal Mantenimiento	Intencionadamente	Para funciones de activos de la VMG, utiliza ingeniería inversa del mismo producto como firmware de la ECU conectado a CAN0-2, actualiza el firmware de la ECU conectado a CAN0-2 con un firmware no autorizado; de esta forma, envía un gran volumen de datos desde la ECU conectada a CAN1-5 e interfiere con la funcionalidad
5	T.Malfunction-Functions-From-ECU	Tercero Personal de mantenimiento en fábrica	Funcionamiento/ uso/mantenimiento normal Mantenimiento	Intencionadamente	Para funciones de activos de la VMG, utiliza ingeniería inversa del mismo producto como firmware de la ECU conectada a CAN1-5, actualiza el firmware de la ECU conectado a CAN1-5 con un firmware no autorizado; de esta forma, envía datos no autorizados desde la ECU conectada a CAN1-5, causa un funcionamiento inadecuado de la funcionalidad
6	T.DoS-Functions-From-Mobile-Device	Tercero	Funcionamiento/ uso/mantenimiento normal	Intencionadamente	Para funciones de activos de la VMG, suplanta al servidor, envía un gran volumen de datos a la VMG desde un dispositivo de conexión móvil e interfiere con la funcionalidad

Cuadro II.2 – Principales amenazas basadas en el modelo del TOE

#	Etiqueta	Quién	Cuándo (fase)	Por qué	Dónde/Qué
7	T.Spoofing-Server_ToGet-Data	Tercero	Funcionamiento/ uso/mantenimiento normal	Intencionadamente	Para información de activos de la VMG, envía una instrucción para obtener información de activos de la VMG desde el dispositivo de conexión móvil mediante la interceptación del canal de comunicación o la suplantación de un dispositivo de conexión móvil. De esta forma, recibe información del activo de la VMG
8	T.MissDoS-Functions-From-mobile-Device	Administrador del servidor	Funcionamiento/ uso/mantenimiento normal	Accidentalmente	Para funciones de activos de la VMG, el servidor envía, por un manejo inadecuado, un gran volumen de datos o de datos no autorizados desde el dispositivo de conexión móvil, interfiere con la funcionalidad y causa un funcionamiento inadecuado de la funcionalidad
9	T.Leaking-Mobile-Information-From-Mobile-Device	Propietario/ usuario Administrador del servidor/ personal del concesionario Administrador del servidor	Funcionamiento/ uso normal Entrega del vehículo Funcionamiento/ uso/mantenimiento normal	Accidentalmente	Para información de activos de la VMG, desde el dispositivo de conexión móvil, y por un manejo inadecuado, envía una instrucción a la VMG para obtener el activo de protección de la VMG (información) y obtiene y filtra el activo de protección de la VMG (información)
10	T.MissUpdate-Mobile-Information-From-Mobile-Device	Propietario/ usuario Administrador del servidor/ personal del concesionario Administrador del servidor	Funcionamiento/ uso normal Entrega del vehículo Funcionamiento/ uso/mantenimiento normal	Accidentalmente	Para información de activos de la VMG, desde el dispositivo de conexión móvil, por un manejo inadecuado, envía por error una instrucción a la VMG para actualizar el activo de protección de la VMG (información) y actualiza el activo de protección de la VMG (información)
11	T.Malfunction-Functions-From-mobile-Device	Tercero	Funcionamiento/ uso/mantenimiento normal	Intencionadamente	Para funciones de activos de la VMG, desde el dispositivo de conexión móvil suplanta a un servidor, envía datos no autorizados y causa un funcionamiento inadecuado de la funcionalidad
12	T.Spoofing-Server_ToRe write-Data	Tercero	Funcionamiento/ uso normal	Intencionadamente	Para activos de protección (información) de la VMG, desde el dispositivo de conexión móvil suplanta a un dispositivo de conexión móvil, envía una instrucción para reescribir el activo de protección de la VMG (información) y reescribe el activo de protección de la VMG (información)

Cuadro II.2 – Principales amenazas basadas en el modelo del TOE

#	Etiqueta	Quién	Cuándo (fase)	Por qué	Dónde/Qué
13	T.DoS-Functions-From-Wi-Fi-Device	Tercero	Funcionamiento/ uso/mantenimiento normal	Intencionadamente	Para la función conexión WiFi, suplanta a un dispositivo de conexión WiFi, envía un gran volumen de datos e interfiere con la funcionalidad
14	T.Malfunction-Functions-From-Wi-Fi-Device	Tercero	Funcionamiento/ uso/mantenimiento normal	Intencionadamente	Para la función conexión WiFi, suplanta a un dispositivo de conexión WiFi, envía datos no autorizados y causa un funcionamiento inadecuado de la funcionalidad
15	T.MissDoS-Functions-From-Wi-Fi-Device	Propietario/ usuario	Funcionamiento/ uso normal	Accidentalmente	Para la función conexión WiFi, por un funcionamiento inadecuado del dispositivo de conexión WiFi o por la infección por software malicioso del dispositivo de conexión WiFi, envía un gran volumen de datos o datos no autorizados, interfiere con la funcionalidad y causa un funcionamiento inadecuado de la funcionalidad
16	T.Spoofing-Wi-Fi-Device_ToGet-Wi-Fi-Information	Tercero	Funcionamiento/ uso/mantenimiento normal	Intencionadamente	Para la función conexión WiFi, suplanta el dispositivo de conexión WiFi y envía una instrucción para obtener información de autenticación de la conexión WiFi y utiliza la información de autenticación de la conexión WiFi
17	T.Spoofing-Wi-Fi-Device_ToRewrite-Wi-Fi-Information	Tercero	Funcionamiento/ uso/mantenimiento normal	Intencionadamente	Para la función conexión WiFi, suplanta el dispositivo de conexión WiFi, envía una instrucción para reescribir información de autenticación de la conexión WiFi y reescribe la información de autenticación de la conexión WiFi
18	T.Leaking-Wi-Fi-Information-From-Wi-Fi-Device	Personal del concesionario Propietario/ usuario	Entrega del vehículo Funcionamiento/ uso normal	Accidentalmente	Para información de autenticación de la conexión WiFi, envía una instrucción para obtener información de autenticación de la conexión y obtiene y filtra información de autenticación de la conexión WiFi
19	T.MissUpdate-Wi-Fi-Information-From-Wi-Fi-Device	Personal del concesionario Propietario/ usuario	Entrega del vehículo Funcionamiento/ uso normal	Accidentalmente	Para información de autenticación de la conexión WiFi, envía una instrucción para reescribir información de autenticación de la conexión WiFi y reescribe información de autenticación de la conexión WiFi

II.3 Requisitos de seguridad del TOE

En las subcláusulas siguientes se describen, en base a las amenazas identificadas en la cláusula II.2, tres componentes de los requisitos de seguridad para el modelo del TOE. Cada requisito de seguridad es consecuencia de amenazas definidas en la cláusula II.2. A cada requisito de seguridad descrito en la cláusula II.3 se asocia un conjunto de números de identificación de amenazas, ID (#), que figuran en el Cuadro II.2.

II.3.1 Requisitos de seguridad (SR) del TOE

II.3.1.1 SR.protección de la integridad/disponibilidad de funciones de la VMG a través de la comunicación en la CAN

La integridad y disponibilidad de las funciones de la VMG deben estar garantizadas frente a ataques de denegación de servicio (DoS) y ataques desde las ECU, realizados a través de la comunicación CAN0-CAN2 que provoquen un funcionamiento defectuoso (véanse las amenazas 4 y 5).

Descripción

En la comunicación en la CAN, sólo se encaminan los datos de la CAN a los que se les haya asignado identificadores especificados (ID) de la CAN. Si la VMG recibe un gran volumen de paquetes de datos de comunicación y/o confirma la existencia de patrones irregulares procedentes de dispositivos con conexión CAN0-CAN2, no es preciso que realice operaciones anormales.

II.3.1.2 SR.protección de la confidencialidad de datos de la VMG

La confidencialidad de los contenidos de las comunicaciones entre la VMG y el servidor debe protegerse de forma que una tercera parte no pueda leer dichos contenidos (véanse las amenazas 7, 16 y 17).

II.3.1.3 SR.protección de la integridad/disponibilidad de funciones de la VMG a través de comunicación móvil

La integridad y la disponibilidad de las funciones de la VMG deben estar garantizadas frente a ataques de denegación de servicio (DoS) y ataques que dan lugar a un funcionamiento defectuoso realizados desde dispositivos móviles a través de los sistemas de comunicaciones móviles (véanse las amenazas 6, 7, 8, 9, 10, 11 y 12).

Descripción

En la comunicación con un dispositivo de conexión móvil, la VMG necesita confirmar si la parte con la que se comunica es un dispositivo de conexión móvil autorizado. La VMG debe protegerse contra la suplantación del servidor cuando recibe datos no autorizados/atípicos a través de una comunicación móvil. Si la VMG recibe una enorme cantidad de paquetes de comunicación de dispositivos con conexión móvil y/o confirma la existencia de patrones irregulares procedentes de dispositivos con conexión móvil, no es preciso que realice operaciones anormales. Además, la VMG debe confirmar la consistencia entre instrucciones enviadas desde dispositivos con conexión móvil y la frecuencia de transmisión de las mismas.

II.3.1.4 SR.tolerancia al fallo de funciones de la VMG

Las operaciones previstas de la VMG deben seguir realizándose aunque se observen irregularidades debidas a ataques, aunque probablemente con una intensidad reducida (véanse las amenazas 1, 2, 3, 4, 5, 6, 8, 11 y 15).

II.3.1.5 SR. protección de la integridad/disponibilidad de funciones de la VMG a través de OBD

La integridad y la disponibilidad de las funciones de la VMG deben estar garantizadas frente a ataques de denegación de servicio (DoS) y ataques que dan lugar a un funcionamiento defectuoso realizados desde dispositivos con conexión OBD a través de un conector OBD (véanse las amenazas 1, 2 y 3).

Descripción

Respecto a la conexión de la CAN a través de un conector OBD, sólo se permite el acceso a la ECU de dispositivos especificados. La VMG debe protegerse frente a la suplantación de dispositivos de conexión ODB cuando se reciben datos no autorizados/atípicos a través del conector ODB. Si la VMG recibe un gran volumen de comunicaciones o instrucciones no autorizadas desde dispositivos con conexión ODB, no es preciso que realice operaciones anormales.

II.3.1.6 SR. protección de la confidencialidad/integridad/disponibilidad de la VMG a través de comunicación WiFi

La VMG debe protegerse frente a la suplantación de dispositivos de comunicación WiFi cuando recibe datos no autorizados/atípicos a través de comunicación WiFi (véanse las amenazas 13, 14, 15, 16, 17, 18 y 19).

Descripción

En la comunicación con un dispositivo WiFi, la VMG ha de confirmar si el dispositivo ha sido previamente registrado. Si la VMG recibe una gran cantidad de paquetes de comunicación de dispositivos WiFi y/o confirma la existencia de patrones irregulares procedentes de dispositivos WiFi, no es preciso que realice operaciones anormales.

II.3.2 Requisitos de seguridad del entorno operacional (SER) del TOE desde la perspectiva de las TI

II.3.2.1 SRE.protección de la ECU

El módulo ECU debe protegerse contra el análisis del firmware de la ECU realizado con técnicas de ofuscación del módulo. La ECU debe protegerse contra ataques que utilicen datos no autorizados de sensores. La ECU ha de protegerse físicamente contra ataques basados en la sustitución no autorizada de la ECU (véanse las amenazas 4 y 5).

II.3.2.2 SRE.protección de la comunicación de la CAN

La comunicación de la CAN debe protegerse contra el análisis del protocolo de comunicación de la CAN mediante operaciones de aleatorización (operaciones ligeras tales como la alteración de bits, etc.) realizadas sobre datos de la carga útil de la CAN. La CAN debe protegerse físicamente contra el ataque de un tercero malicioso que altere su cableado (véanse las amenazas 4 y 5).

II.3.2.3 SRE.protección de la red de comunicación móvil

La red de comunicación móvil que utiliza la VMG para comunicarse con el servidor debe protegerse contra ataques de dispositivos no autorizados. Debe protegerse la confidencialidad de la información de la configuración de la red. La red debe supervisarse para detectar ataques (véanse las amenazas 6, 7, 11 y 12).

II.3.2.4 SRE.protección de la comunicación inalámbrica

Las comunicaciones inalámbricas deben protegerse contra el análisis del protocolo de comunicación inalámbrica almacenando exclusivamente los datos mínimos necesarios de la carga útil de los paquetes de comunicación, o mediante la aleatorización de los datos de la carga útil aplicando operaciones ligeras tales como la alteración de bits (*bit flipping*), etc. (véanse las amenazas 7, 12, 16 y 17).

II.3.3 Requisitos de seguridad del entorno operacional desde una perspectiva de operación/ gestión distinta a las TI

II.3.3.1 SREN.medidas precautorias

Debe señalarse que un ataque al sistema interno de un vehículo es un delito. Además, debe restringirse la venta de productos que ayuden a propósitos delictivos (véanse las amenazas 1, 2, 4, 5, 6, 7, 11, 12, 13, 14, 16 y 17).

II.3.3.2 SREN.servidor de red

El administrador del servidor debe evitar que los datos almacenados se filtren o sean manipulados por una gestión inadecuada del servidor (véanse las amenazas 7 y 8).

II.3.3.3 SREN.protección de herramientas OBD

Las herramientas OBD conectadas al vehículo deben protegerse frente a una utilización no autorizada mediante una gestión protegida. Además, antes de su utilización deben confirmarse los métodos de funcionamiento de las herramientas conectadas al vehículo (véase la amenaza 3).

II.3.3.4 SREN.usuario

Los usuarios deben ser informados sobre las precauciones que han de adoptar cuando utilizan un vehículo.

Descripción

Un vehículo debe mantenerse cerrado con llave para impedir el acceso indeseado de un tercero cuando el usuario está alejado del mismo. Un vehículo debe ser estacionado en un lugar al que un tercero no puede aproximarse fácilmente al mismo si no está siendo utilizado. Antes de utilizar el vehículo, el usuario debe confirmar que en el mismo no existe un dispositivo no identificado. El usuario debe actuar con precaución cuando conecte productos comerciales al conector OBD, que es una interfaz para mantenimiento (véanse las amenazas 1, 2, 4, 5, 13, 14, 16 y 17).

II.3.3.5 SREN.exploración para la detección de virus

Los dispositivos conectados al sistema a través de conexiones móviles/WiFi deben explorarse periódicamente (véanse las amenazas 9, 10, 15,18 y 19).

II.3.3.6 SREN.protección del dispositivo inalámbrico

La persona concernida debe confirmar cómo se utiliza el dispositivo conectado a través de móvil/WiFi antes de utilizarlo. Además, la persona debe actuar con precaución para evitar la filtración de la palabra de paso del dispositivo conectado a través de WiFi y de instrucciones conexas (véanse las amenazas 9, 10, 12, 13, 14, 16, 17, 18 y 19).

II.3.3.7 SREN.pantalla inalámbrica

Los usuarios que utilicen dispositivos de conexión WiFi/móviles deben confirmar si envían, mediante una opción presentada en la pantalla del dispositivo, instrucciones "get/write" (obtener/escribir) de información de activos de la VMG (véanse las amenazas 9, 10, 18 y 19).

II.4 Controles de seguridad

En base a los requisitos de seguridad de II.3, en este apartado se proporcionan controles de seguridad que cumplen los requisitos de seguridad, especialmente desde la perspectiva de las TI.

II.4.1 SC.carga de confianza

Es recomendable que en todas las cargas de software de la ECU se implementen, como contramedida frente al análisis (es decir, manipulación) del módulo de programa original de la ECU, mecanismos de autoprueba del software utilizando el mecanismo de protección de la carga del módulo hardware de seguridad (HSM).

Requisito de seguridad correspondiente

– SRE.protección de la ECU en la cláusula II.3.2.1

II.4.2 SC.verificación del mensaje

El método de verificación del mensaje es efectivo frente a ataques de manipulación, escucha y reproducción para preservar la autenticación de entidades y la integridad de mensajes.

A tal fin existen dos métodos adecuados: el primero consiste es utilizar la firma digital (método de la firma digital) y el segundo utiliza el código de autenticación de mensajes (MAC).

Por otra parte, en las implementaciones reales de las ECU en vehículos, las capacidades criptográficas de los dispositivos difieren en función del tipo de vehículo. Por ejemplo, un vehículo de lujo puede tener módulos hardware de seguridad (HSM) para todas sus ECU, mientras que un vehículo popular puede tener HSM sólo para algunas de sus ECU. Además, existen diferencias entre las capacidades criptográficas en función de los tipos de HSM utilizados.

Por tanto, la arquitectura de seguridad debe tener en cuenta las diferencias en términos de capacidades de seguridad de los vehículos. En concreto, en esta Recomendación se aplica el método de firma digital basado en [UIT-T X.509] para la verificación del mensajes de vehículos con algoritmo criptográfico asimétrico (por ejemplo, un módulo de plataforma confiable (TPM)). Por otro lado, se utiliza MAC para la verificación del mensaje en vehículos sin algoritmo criptográfico asimétrico (por ejemplo HSM y tarjeta inteligente). En la cláusula 7 se incluye información adicional sobre el protocolo de comunicación, incluida la verificación de mensajes. Este control de seguridad es una medida esencial para la actualización de software a distancia a fin de verificar mensajes incluidos en esta Recomendación.

Requisitos de seguridad correspondientes

– SR.protección de confidencialidad de los datos de la VMG en la cláusula II.3.1.2;

– SR.protección de la confidencialidad/integridad/disponibilidad de la VMG a través de comunicaciones WiFi en la cláusula II.3.1.6;

– SRE.protección de la red de comunicaciones móviles en la cláusula II.3.2.3;

– SRE.protección de las comunicaciones inalámbricas en la cláusula II.3.2.4.

II.4.3 SC.autenticación de la entidad de comunicación

Para evitar la suplantación de entidades de comunicación (es decir suplantación de la ECU, la VMG y el servidor de actualización), es recomendable que dichas entidades se autentiquen mutuamente al inicio de cada comunicación. Éste control de seguridad debe implementarse en la capa de transporte y los procedimientos de actualización segura de software de esta Recomendación deben estar protegidos mediante funciones de capa inferior. Como contramedida específica de protección de la autenticación de entidades de comunicación, resulta efectivo que la autenticación del cliente y la autenticación del servidor utilicen la capa de conector segura/seguridad de la capa de transporte (SSL/TLS) en el marco de la autoridad de certificación (CA).

Requisitos de seguridad correspondientes

– SR.protección de la confidencialidad/integridad/disponibilidad de la VMG mediante comunicación WiFi en la cláusula II.3.1.6;

– SRE.protección de la red de comunicaciones móviles en la cláusula II.3.2.3;

– SRE.protección de las comunicaciones inalámbricas en la cláusula II.3.2.4.

II.4.4 SC.filtrado de mensajes

Como ejemplo de ataques DoS contra la VMG, una ECU puede verse comprometida por un atacante y enviar masivamente mensajes falsos a la VMG para consumir de manera inadecuada sus recursos de computación. Uno de los métodos más efectivos para reducir el impacto sobre la seguridad de dichos ataques DoS es la técnica de filtrado de mensajes. Es recomendable que la VMG descarte mensajes irrelevantes en función del identificador del remitente, el tipo de mensaje, el tamaño, la frecuencia, etc. o una combinación de todos esos criterios.

Requisitos de seguridad correspondientes

– SR.protección de la integridad/disponibilidad de funciones de la VMG a través de la comunicación en la CAN en la cláusula II.3.1.1;

– SR.protección de la integridad/disponibilidad de funciones de la VMG a través de las comunicaciones móviles en la cláusula II.3.1.3;

– SR.protección de la integridad/disponibilidad de funciones de la VMG a través de OBD en la cláusula II.3.1.5.

II.4.5 SC.tolerancia a fallos de funciones de la VMG

Se recomienda firmemente que los proveedores de VMG diseñen el software de la VMG a prueba de fallos de forma que la VMG pueda seguir funcionando correctamente en situaciones irregulares debidas a ataques. En particular, la VMG ha de supervisar el funcionamiento y adoptar medidas si detecta irregularidades (por ejemplo, recarga del software u otra) de forma que recupere un estado normal. Si dicha recuperación no es posible, informa al conductor y suspende su funcionamiento de forma segura.

Requisito de seguridad correspondiente

– SR.tolerancia al fallo de funciones de la VMG en la cláusula II.3.1.4.

Bibliografía

[b-UIT-T F.749.1] Recomendación UIT-T F.749.1 (2015), *Requisitos funcionales de las pasarelas de vehículos*.

[b-ISO/CEI 9797-1] ISO/CEI 9797-1:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50375>

[b-ISO/CEI 9797-2] ISO/CEI 9797-2:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*.
<http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51618>

[b-ISO/CEI 9797-3] ISO/CEI 9797-3:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 3: Mechanisms using a universal hash-function*.
<http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51619>

[b-ISO/CEI 29192-2] ISO/CEI 29192-2:2012, *Information technology – Security techniques – Lightweight cryptography – Part 2: Block ciphers*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56552>

[b-ISO/CEI 29192-5] ISO/CEI 29192-5:2016, *Information technology – Security techniques – Lightweight cryptography – Part 5: Hash functions.*
<http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67173>

[b-JASO TP15002] JASO TP15002:2015, *Guideline for automotive information security analysis*.

[b-FIPS-202] Federal Information Processing Standards Publication-202 (2015), *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. National Institute of Standards and Technology,
<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf>

[b-ISO 14229] ISO 14229-1:2013, *Road vehicles – Unified diagnostic services (UDS) – Part 1: Specification and requirements*.

[b-ISO 13400] ISO 13400-1:2011, *Road vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 1: General information and use case definition*.

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 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, 2017