ITUPublications
Recomendaciones

Unión Internacional de Telecomunicaciones
Sector de la Normalización

Recomendación

UIT-T X.1381 (03/2023)

SERIE X: Redes de datos, comunicaciones de sistemas abiertos y seguridad

Aplicaciones y servicios con seguridad (2) – Seguridad en los sistemas de transporte inteligentes (STI)

Directrices de seguridad para las redes intravehiculares basadas en Ethernet

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	X.1000-X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	X.1100-X.1199
SEGURIDAD EN EL CIBERESPACIO	X.1200-X.1299
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	X.1300-X.1499
Comunicaciones de emergencia	X.1300-X.1309
Seguridad en las redes de sensores ubicuos	X.1310-X.1319
Seguridad en redes eléctricas inteligentes	X.1330-X.1339
Correo certificado	X.1340-X.1349
Seguridad en la Internet de las cosas (IoT)	X.1350-X.1369
Seguridad en los sistemas de transporte inteligentes (STI)	**X.1370-X.1399**
Seguridad en la tecnología de libro mayor distribuido (DLT)	X.1400-X.1429
Seguridad en las aplicaciones (2)	X.1450-X.1459
Seguridad en la web (2)	X.1470-X.1489
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	X.1500-X.1599
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	X.1600-X.1699
COMUNICACIÓN CUÁNTICA	X.1700-X.1729
SEGURIDAD DE LOS DATOS	X.1750-X.1799
SEGURIDAD EN LAS REDES IMT-2020	X.1800-X.1819

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

Recomendación UIT-T X.1381

Directrices de seguridad para las redes intravehiculares basadas en Ethernet

Resumen

En esta Recomendación se ofrecen directrices de seguridad para las redes intravehiculares (IVN) basadas en Ethernet. La tendencia actual en la arquitectura eléctrica y electrónica (E/E) es integrar la Ethernet con las IVN heredadas, como la red de área de controladores (CAN), la red de interconexión local (LIN), el transporte de sistemas orientados a los medios (MOST) y FlexRay. En el pasado, la Ethernet se consideraba únicamente una conexión entre los vehículos y los entornos exteriores. Para permitir las comunicaciones entre el entorno exterior y los vehículos se han utilizado protocolos normalizados habilitados para conexiones basadas en el protocolo de Internet a través de Ethernet (por ejemplo, la comunicación de diagnóstico a través del protocolo Internet o el protocolo universal de medición y calibración). Por lo general, estos casos de uso no están sujetos a restricciones estrictas en tiempo real. Sin embargo, las aplicaciones intravehiculares que utilizan la comunicación Ethernet requieren características específicas, como una alta sensibilidad temporal y fiabilidad.

La evolución actual de las tecnologías de comunicación intravehicular exige un mayor ancho de banda en la red. En comparación con Ethernet, las IVN heredadas son insuficientes para satisfacer los requisitos de ancho de banda de las actuales aplicaciones intravehiculares. Por tanto, ahora y en el futuro, las IVN basadas en Ethernet son una parte importante de la arquitectura E/E.

Sin embargo, las contramedidas conocidas de las redes informáticas comunes no son apropiadas para una aplicación de automoción porque no fueron diseñadas teniendo en cuenta los requisitos y capacidades de la automoción.

A fin de responder a esta demanda, la presente Recomendación ofrece directrices de seguridad para la tecnología Ethernet de automoción. Incluye tanto un modelo de referencia de Ethernet de automoción como un análisis de las amenazas y vulnerabilidades de las IVN basadas en Ethernet, y detalla los requisitos de seguridad y los casos de uso de las IVN basadas en Ethernet.

Historia[*]

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único
1.0	UIT-T X.1381	03-03-2023	17	11.1002/1000/15107

Palabras clave

Seguridad de Ethernet de automoción, seguridad de los ITS.

[*] Para acceder a la Recomendación, sírvase digitar el URL https://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación.

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 se pronuncia en lo que respecta a la existencia, validez o aplicabilidad de los derechos de propiedad intelectual reclamados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patentes/derechos de autor de *software*, 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 las correspondientes bases de datos del UIT-T disponibles en el sitio web del UIT-T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

Recomendación UIT-T X.1381

Directrices de seguridad para las redes intravehiculares basadas en Ethernet

1 Alcance

En esta Recomendación se ofrecen directrices de seguridad para las redes intravehiculares (IVN) basadas en Ethernet. Se abordan los siguientes aspectos desde la perspectiva de la ciberseguridad:

1) análisis de las amenazas de seguridad;

2) requisitos de seguridad; y

3) casos de uso.

La ciberseguridad indica que la arquitectura de comunicación técnica implicada forma o puede formar parte integrante de los sistemas ciberfísicos (por ejemplo, las pilas de protocolos de comunicación para Ethernet están incorporadas en sistemas integrados).

1.1 Declaraciones de aplicabilidad

Las redes en general, y las redes Ethernet en particular, se utilizan en los servicios de comunicaciones. Por tanto, el contexto de seguridad de esta Recomendación se centra en la seguridad de las comunicaciones, aunque no se ocupa necesariamente de la seguridad de la propia información en los nodos de cálculo con conectividad Ethernet.

En consecuencia, las directrices de seguridad de esta Recomendación abordan la ingeniería de redes de las redes basadas en Ethernet que se utilizan en las aplicaciones de automoción desde la perspectiva de la ingeniería de seguridad. Así, las arquitecturas de comunicación por capas asociadas, y sus pilas de protocolos en capas, son un elemento fundamental de esas consideraciones de seguridad.

1.2 Validación de las directrices de seguridad a lo largo del tiempo

La seguridad de las arquitecturas de comunicación aplicable a las redes Ethernet intravehiculares está evolucionando de manera fundamental, en consonancia principalmente con los avances siguientes:

1) posibles cambios en las topologías de red (motivados por la evolución de las arquitecturas de computación distribuidas, que utilizan esas redes de comunicaciones para, por ejemplo, automatizar la dirección de los vehículos);

2) arquitecturas de protocolos en capas: las pilas de protocolos Ethernet y no Ethernet que se utilizan actualmente pueden cambiar, ampliarse, etc.;

3) evolución de los protocolos: los protocolos de tecnología de la información y la comunicación (TIC) vigentes (que pertenecen a organizaciones de normalización como el IEEE, IETF, UIT-T, ETSI, 3GPP) siguen siendo objeto de actividades de mantenimiento y ampliación continuas, que se reflejan en la creación de perfiles de protocolos (por ejemplo, TSN del IEEE para aplicaciones de automoción) [b-IEEE 1722-2016] o la creación de versiones de los protocolos;

NOTA – Además, las consideraciones de seguridad asociadas a especificaciones de protocolos pueden ser objeto de actualización.

4) evolución de los medios y las soluciones de seguridad en el contexto de la seguridad de las comunicaciones.

Por tanto, es previsible que esta Recomendación sea objeto de revisiones en el futuro.

Esta Recomendación se centra de forma particular en las directrices de seguridad iniciales, proporcionadas por un primer conjunto de casos de uso. El alcance primario son las IVN basadas en Ethernet de primera generación, que motivan las prácticas idóneas y directrices de seguridad vigentes en el momento en que se publica esta Recomendación.

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

[b-UIT-T X.1371] Recomendación UIT-T X.1371 (2019), *Amenazas a la seguridad de los vehículos conectados.*

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 imputabilidad [b-ITU-T X.800]: Propiedad que garantiza que las acciones de una entidad puedan ser rastreadas de una manera inequívoca para imputarlas a esa entidad.

3.1.2 autentificación [b-ITU-T X.1252]: Proceso oficializado de verificación que, de ser satisfactoria, da lugar a una identidad autentificada para una entidad.

NOTA – En el contexto de la gestión de identidad se entiende que el término autentificación se refiere a la autentificación de una entidad

3.1.3 autenticidad [b-ITU-T X.641]: Protección para la autentificación mutua y la autentificación del origen de los datos.

3.1.4 autorización [b-ITU-T X.800]: Atribución de derechos, que incluye la concesión de acceso basada en derechos de acceso.

3.1.5 disponibilidad [b-ITU-T X.800]: Propiedad de ser accesible y utilizable a petición por una entidad autorizada.

3.1.6 confidencialidad [b-ITU-T X.800]: Propiedad de una información por la que no está disponible ni es divulgada a personas, entidades o procesos no autorizados.

3.1.7 integridad de los datos [b-ITU-T X.800]: Propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada.

3.1.8 cortafuegos [b-ITU-T X.1039]: Tipo de barrera de seguridad colocada entre entornos de red –que consiste en un dispositivo especial o una combinación de diversos componentes y técnicas– a través de la cual pasa todo el tráfico de un entorno de red a otro, y viceversa, y solo se permite el tráfico autorizado que se defina en la política de seguridad local.

3.1.9 pasarela de seguridad [b-ITU-T X.1039]: Punto de conexión entre redes o entre subgrupos dentro de redes o entre aplicaciones de soporte lógico dentro de diferentes dominios de seguridad destinado a proteger una red según una determinada política de seguridad particular.

3.1.10 pasarela de vehículo (VG) [b-ITU-T F.749.1]: Una VG es un dispositivo situado en un vehículo que permite la comunicación entre un dispositivo en el vehículo y otro dispositivo que puede encontrarse físicamente dentro o fuera del vehículo (por ejemplo, una estación junto a la carretera, un servidor en la nube, etc.). Las VG proporcionan interfaces y protocolos normalizados, permiten la comunicación entre redes heterogéneas y la selección de redes optimizada de acuerdo con las necesidades de las aplicaciones y la calidad de servicio de las redes, y ofrecen arbitraje e integración de las comunicaciones de red, seguridad y conexiones de red de conmutación para mantener la continuidad del servicio.

NOTA 1 – El término "pasarela central" que se utiliza en esta Recomendación suele ser sinónimo de "pasarela de vehículo" en las redes intravehiculares (IVN) abstraídas o de "pasarela de vehículo limítrofe" en las arquitecturas de IVN más detalladas.

NOTA 2 – El término "pasarela de vehículo para sistemas de transporte inteligentes (ITS)" es prácticamente sinónimo de "pasarela de vehículo".

3.2 Términos definidos en la presente Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 arquitectura eléctrica y electrónica (arquitectura E/E): Arquitectura vehicular acoplada en dos planos, a saber: 1) un plano de redes de distribución de energía eléctrica; y 2) un plano arquitectónico de redes de comunicación y procesamiento de la información.

NOTA – En ocasiones, se añade una tercera etiqueta a E/E para representar la tecnología de propulsión vehicular, es decir, E^3; donde la tercera E se refiere a un vehículo eléctrico.

3.2.2 pasarela de vehículo limítrofe: Una pasarela de vehículo que está ubicada en los límites y dentro de uno o varios dominios de red vehicular interna y uno o varios dominios de red vehicular externa. En consecuencia, todo el tráfico de comunicación entre el vehículo y su entorno (V2X) se encamina a través de una pasarela de vehículo de este tipo.

NOTA 1 – El término "pasarela de vehículo" también incluye este significado; por tanto, podría resultar suficiente para las arquitecturas de redes intravehiculares (IVN) en las que solo hay desplegada una pasarela de vehículo. Sin embargo, las IVN también pueden utilizar pasarelas de vehículo, aunque solo con fines de interconexión e interfuncionamiento internos. En estos contextos de red, puede resultar necesario diferenciar entre los tipos de pasarela de forma más pormenorizada.

NOTA 2 – Las funciones de interfuncionamiento específicas que admite un tipo de pasarela concreto suelen expresarse con un nombre de pasarela extendido, que indica, por ejemplo, la ubicación en una jerarquía de red (como el nivel de acceso o de red básica), el tipo de límite o conexión entre redes (como los dominios de seguridad), o unas interfaces de red o tecnologías de comunicación determinadas.

NOTA 3 – Se entiende que una unidad de control de las comunicaciones es un componente técnico que pertenece a la categoría de pasarela de vehículo limítrofe (funciones).

NOTE 4 – La comunicación V2X abarca todos los tipos de tráfico, por ejemplo, el tráfico procedente de servicios de diagnóstico o telemáticos o de un ITS.

3.2.3 arquitectura eléctrica y electrónica por zonas: arquitectura eléctrica y electrónica (E/E) que agrupa los componentes intravehiculares (Nota 1), como sensores, accionadores y nodos de cálculo, en función de su ubicación (Nota 2) en los subdominios de red. Cada subdominio, esto es, cada zona (Nota 3), contiene un nodo de cálculo vehicular zonal diferenciado, denominado controlador de zona en las aplicaciones de automoción, que está conectado a todos los componentes intravehiculares de los subdominios. Los controladores de zona de cada zona vuelven a estar interconectados con un nodo de cálculo intravehicular superior de alto rendimiento. En consecuencia, desde el punto de vista de la arquitectura de computación distribuida, se establece una jerarquía de procesamiento entre las zonas y el dominio de red intravehicular (IVN) general.

NOTA 1 – Determinación del alcance de los componentes de computación y red en el contexto de las IVN.

NOTA 2 – La "ubicación" hace referencia a la ubicación de la red en el nivel topológico físico o virtual de la IVN.

NOTA 3 – En este caso, el concepto de zona está relacionado fundamentalmente con el concepto de dominios de red en el contexto de la arquitectura E/E. No incluye necesariamente los conceptos de zona de seguridad, zona de confianza o zona desmilitarizada que se utilizan en otras Recomendaciones del UIT-T relativas a la seguridad, como [b-ITU-T Y.2770].

4 Siglas y acrónimos

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

ADAS Sistema avanzado de asistencia al conductor (*advanced driver assistance system*)

ARP Protocolo de resolución de direcciones (*address resolution protocol*)

AUTOSAR Arquitectura de sistema abierto para automoción (*automotive open system architecture*)

AVB Transmisión sincronizada de audio y vídeo (*audio video bridging*)

CAN Red de área de controladores (*controller area network*)

CGW Pasarela central (*central gateway*)

CPU Unidad de procesamiento central (*central processing unit*)

CRC Comprobación de redundancia cíclica (*cyclic redundancy check*)

DHCP Protocolo de configuración dinámica de anfitrión (*dynamic host configuration protocol*)

DoIP Comunicación de diagnóstico a través del protocolo Internet (*diagnostic communication over Internet protocol*)

DoS Denegación de servicio (*denial of service*)

DTLS Seguridad de la capa de transporte de datagramas (*datagram transport layer security*)

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

E/E Eléctrica y electrónica (*electrical and electronic*)

FDB Base de datos de retransmisión (*forwarding database*)

FIB Base de información de retransmisión (*forwarding information base*)

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

ICMP Protocolo de mensajes de control de Internet (*Internet control message protocol*)

ID Identificador (*identifier*)

IDS Sistema de detección de intrusiones (*intrusion detection system*)

IP Protocolo Internet (*Internet protocol*)

IPsec Seguridad del protocolo Internet (*Internet protocol security*)

IPv4 Protocolo Internet versión 4 (*Internet protocol version 4*)

IPv6 Protocolo Internet versión 6 (*Internet protocol version 6*)

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

IVN Red intravehicular (*in-vehicle network*)

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

MAC Control de acceso a los medios (*media access control*)

MACsec Seguridad de control de acceso a los medios (*media access control security*)

MCU Unidad de microcontrolador (*microcontroller unit*)

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

MPU Unidad de control multipunto (*multipoint control unit*)

OBD Diagnóstico a bordo (*on-board diagnostic*)

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

PDU Unidad de datos de protocolo (*protocol data unit*)

PVID ID de VLAN de puerto (*port VLAN ID*)

QoS Calidad de servicio (*quality of service*)

SecOC Comunicación a bordo segura (*secure onboard communication*)

SR Recomendación de seguridad (*security recommendation*)

TARA Análisis de amenazas y evaluación de riesgos (*threat analysis and risk assessment*)

TCP Protocolo de control de transmisión (*transmission control protocol*)

TIC Tecnología de la información y la comunicación

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

TSN Creación de redes sensibles al tiempo (*time-sensitive networking*)

UDP Protocolo de datagrama de usuario (*user datagram protocol*)

UDS Servicio de diagnóstico unificado (*unified diagnostic service*)

V2X Vehículo y su entorno (*vehicle to everything*)

VG Pasarela de vehículo (*vehicle gateway*)

VID Identificador de VLAN (*VLAN identifier*)

VLAN Red de área local virtual (*virtual local area network*)

5 Convenciones

En esta Recomendación se presenta una lista de requisitos de seguridad, etiquetados como [SR-*x*], donde *x* es un número. Estos requisitos de seguridad utilizan las frases siguientes, con los significados que se indican a continuación.

La expresión "**se recomienda**" o "**debería**" indica que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio. El cumplimiento de ese requisito no es necesario para acreditar la conformidad.

La expresión "**se tiene la opción de**" u "**opcionalmente**" indica que el requisito se permite, sin que ello signifique que se recomienda. El uso de este término no implica que el fabricante deba ofrecer esta opción y que el operador de red/proveedor de servicio tenga la posibilidad de activarla. Significa, más bien, que el fabricante tiene la opción de proporcionar esta función sin que ello afecte a la conformidad con la presente especificación.

6 Descripción de las arquitecturas intravehiculares basadas en Ethernet de automoción y su evolución

La Ethernet de automoción es una red física que conecta componentes de un vehículo a través de una red alámbrica. También se utiliza esta denominación para referirse a toda la red Ethernet intravehicular, que incluye todas las capas de protocolos y protocolos empleados en ese dominio de red. Se ha diseñado con el objetivo de satisfacer las necesidades del mercado de la automoción, a saber, los requisitos eléctricos (emisiones de interferencias de radiofrecuencias/interferencias electromagnéticas y susceptibilidad), los requisitos de ancho de banda, los requisitos de latencia, los

requisitos de sincronización y los requisitos de gestión de redes. Ahora que las tecnologías de sistema avanzado de asistencia al conductor (ADAS) y vehículo autónomo van adquiriendo importancia, los vehículos modernos suelen ir equipados con múltiples cámaras, sistemas de diagnóstico a bordo (OBD) y sistemas de infoesparcimiento que requieren una gran cantidad de ancho de banda. Además, a medida que crece el número de funciones, se incrementa el número de nodos de cálculo interconectados (como las unidades de control electrónicas, o ECU) de un vehículo. Esto conlleva un cableado más grande y una masa de vehículo mayor, lo que reduce el rendimiento y la eficiencia del combustible. La arquitectura E/E por zonas es un buen ejemplo de arquitectura intravehicular de red y de computación, donde la Ethernet también se utiliza en el nivel jerárquico de la red para interconectar todas las zonas (la llamada red troncal) de toda la arquitectura. Cuando se integra con Ethernet una IVN heredada, que incluye una red de área de controladores (CAN), una red de interconexión local (LIN), el transporte MOST (*media-oriented systems transport*) o FlexRay, puede utilizarse cableado Ethernet normalizado para reducir la masa significativamente y rebajar los costes. Además, debido al elevado ancho de banda, es posible disminuir el número de sistemas de control y la complejidad.

No obstante, no todos los dominios de IVN, como el grupo motopropulsor, la carrocería y el chasis, cambiarán a la Ethernet de automoción. En realidad, los dominios (por ejemplo, una carrocería que requiere pocos datos y banco de anda) no tienen que cambiar los protocolos de conexión de redes, lo que requeriría recursos y esfuerzos adicionales.

En la Figura 1 se muestra una IVN mixta con protocolos de IVN heredada, como CAN, y la Ethernet de automoción. Las comunicaciones que requieren poco ancho de banda pueden seguir utilizando los protocolos de IVN heredada, mientras que las comunicaciones que requieren un ancho de banda elevado, como las funciones ADAS o autónomas, pueden cambiarse a una IVN basada en Ethernet.

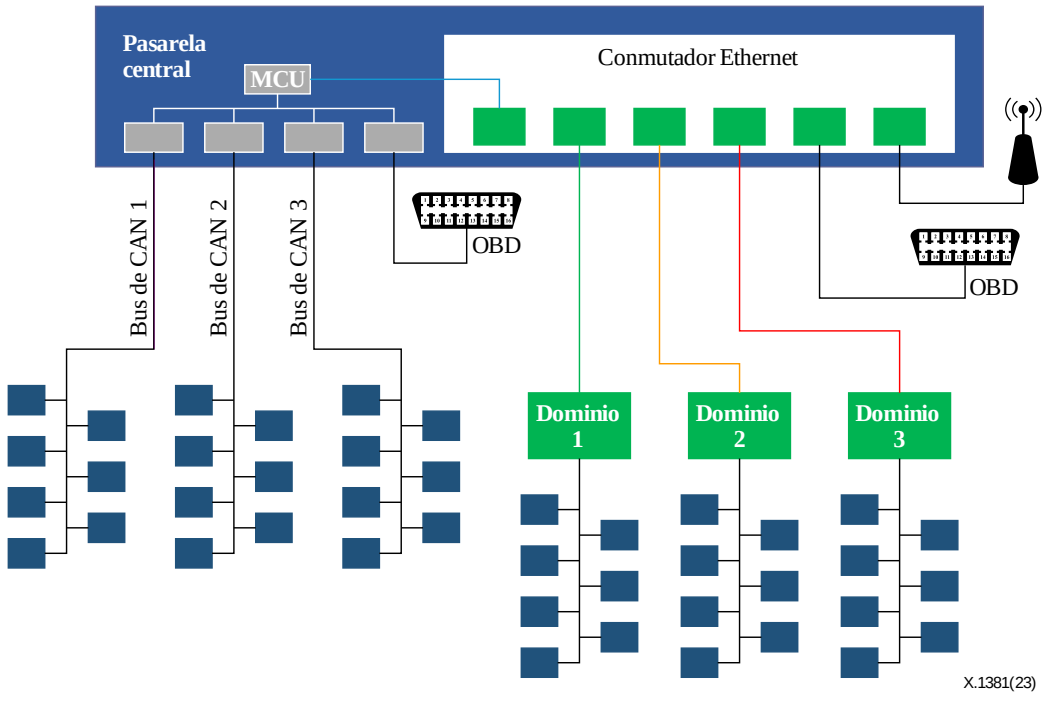

Figura 1 – Heterogeneidad de una red intravehicular típica actual, basada en protocolos heredados y Ethernet de automoción

Se espera que las IVN basadas en Ethernet evolucionen a lo largo del tiempo. Estos avances de las redes suelen acompañarse de cambios en la arquitectura de comunicación (determinada por las topologías de comunicación, las pilas de protocolos en capas, etc.), que probablemente repercutirán a su vez en las arquitecturas de seguridad de las comunicaciones asociadas.

En el pasado, ya se han analizado los conceptos de seguridad de las arquitecturas E/E clásicas (es decir, basadas en CAN/FlexRay/LIN y, en ocasiones, MOST) y algunos de los mecanismos propuestos han llegado a ser normalizados. La Ethernet y los protocolos de capa superior conexos no solo reemplazarán de manera sencilla y más rápida los sistemas de bus para automoción heredados, sino que, con toda probabilidad, también cambiarán conceptos fundamentales de las arquitecturas E/E que se utilizan hoy en día.

La introducción de la Ethernet brinda una oportunidad inigualable para mejorar la seguridad intravehicular puesto que muchos problemas de seguridad complejos de las aplicaciones de automoción ya se han solucionado para la Ethernet; un ejemplo son las llamadas actividades de TIC con calidad de operador (como las redes de área metropolitana basadas en Ethernet o las redes de acceso radioeléctrico terrenales basadas en Ethernet), así como las actividades de tecnología de la información clásicas (esto es, la Ethernet como conectividad de base en redes de área local empresariales y privadas). Sin embargo, también plantea dificultades importantes (por ejemplo, debido a las restricciones de los sistemas integrados o de automoción) a la hora de garantizar al menos el mismo nivel de seguridad que se espera actualmente para las arquitecturas E/E con seguridad mejorada existentes.

6.1 Arquitectura electrónica y eléctrica de red y computación en un vehículo

Las arquitecturas E/E antiguas presentan una pasarela central (CGW, también denominada VG o pasarela de vehículo para ITS en ese tipo de IVN) para la comunicación intravehicular y la interconexión entre diferentes subdominios. Por tanto, hay conexiones de extremo a extremo que se encaminan a través de esas VG.

NOTA 1 – En este contexto, "encaminarse" hace referencia a la función genérica de encaminamiento del tráfico, no a otros tipos de encaminamiento, como el IP. Las IVN basadas en Ethernet actuales no utilizan entidades encaminadoras IP, solo pasarelas de tipo IP. Este uso del IP y la Ethernet deriva en algo similar a una red IP conmutada (para los servicios de comunicaciones basados en el IP).

Este aspecto es determinante desde el punto de vista de la seguridad de las comunicaciones, ya que reduce los objetivos de seguridad relacionados con el IP (por ejemplo, no se producirán amenazas a la seguridad debido a los protocolos de encaminamiento IP).

La comunicación basada en Ethernet que se espera conseguir cumplirá los requisitos de alto rendimiento en tiempo real y comunicación fiable y se beneficiará de una tecnología y técnica de comunicación establecida, de eficacia demostrada y uso generalizado.

NOTA 2 – En [b-IEEE 802.1], y especialmente en [b-IEEE 802.1CB], se permite la comunicación fiable, que incluye una arquitectura en anillo con una función de redundancia en la capa 2 (R-Tag).

En concreto, CAN, FlexRay, LIN y MOST se utilizan de serie para la comunicación intravehicular, y CAN es la opción más popular. Las CGW, las VG en general y las pasarelas de vehículo limítrofe en particular son, como tales, elementos de red y seguridad esenciales en las redes intravehiculares y las arquitecturas de comunicación. En los Apéndices II y III se facilita información complementaria que podría resultar útil desde el punto de vista de la seguridad de las comunicaciones.

En el pasado, no se podía acceder a un vehículo en remoto (por ejemplo, utilizando la conexión de taller con fines diagnósticos o las múltiples opciones de tipos de comunicación V2X). Las ECU intravehiculares se conectaban entre sí a través de uno o varios buses de campo de automoción nativos optimizados.

Legalmente, el acceso postproducción solo se autorizaba mediante una conexión alámbrica física directa. Por tanto, la conexión punto a punto en una distancia corta se utiliza exclusivamente para los servicios diagnósticos que requieren una conexión con el puerto OBD a través del protocolo CAN. Los fabricantes de equipo original conocían el mayor riesgo de seguridad asociado a la funcionalidad de diagnóstico y sabían que el protocolo CAN nativo no proporciona ninguna función de seguridad. [b-Autosar 654] se ha centrado en la autenticidad e integridad de los mensajes CAN y los

correspondientes conceptos de seguridad utilizan principalmente códigos de autenticación de mensajes.

Con los avances actuales, se puede utilizar comunicación basada en Ethernet entre dispositivos externos y el vehículo. Por regla general, se establece una ECU dedicada dentro del vehículo como punto de acceso para algún tipo de comunicación externa. De ser necesario, la ECU encamina la información de interés a las demás ECU a través de redes de automoción comunes y reenvía el tráfico a una CGW a través de una conexión basada en Ethernet para que sea encaminado hacia otras ECU que suelen estar conectadas.

6.2 Comparación entre las características de seguridad de las arquitecturas eléctricas y electrónicas actuales y futuras

Debido a varios casos de uso indebido relacionados con componentes intravehiculares, se han definido mecanismos de seguridad para las arquitecturas E/E actuales. En lo que respecta a los sistemas de comunicación, se han publicado y normalizado mecanismos de autenticación de la red CAN predominante, que se aplicarán parcialmente en las generaciones futuras de vehículos. La arquitectura de sistema abierto para automoción AUTOSAR especifica un módulo de comunicación segura a bordo que se centra en la autenticidad e integridad de la comunicación intravehicular. Es importante tener en cuenta que los mecanismos de autenticación no comprueban únicamente la autenticidad de los mensajes transmitidos, sino que también garantizan la autenticidad de los asociados en la comunicación.

Además, en tanto que tecnología de bus de la capa física, la CAN transmite los mensajes únicamente como mensajes de radiodifusión.

NOTA 1 – Por consiguiente, el carácter fundamental de la comunicación por medio físico compartido, como una topología de bus, es contrario al enfoque de un diseño de red Ethernet conmutada.

Así, cada participante puede leer todo el tráfico transmitido a través del bus CAN. Los diferentes dominios de red basados en bus, así como los subdominios adicionales, separan el tráfico relacionado con la seguridad de otros tipos de tráfico, por ejemplo, de infoesparcimiento o comodidad. La comunicación entre los dominios de red solo puede realizarse a través de una CGW, que suele utilizar mecanismos de aplicación de reglas de política (como normas relacionadas con los filtros) para evitar los ataques por inundación y garantizar la disponibilidad de la red.

NOTA 2 – Las pasarelas de vehículo como las CGW ofrecen un conjunto de funciones de red, entre cuyos subgrupos figura uno en concreto relacionado con la seguridad de las comunicaciones. Por consiguiente, se aplican reglas de política no solo para cuestiones de seguridad, sino también para otros aspectos (por ejemplo, interfuncionamiento de red de área local virtual [VLAN], reenvío de IP o definición de acciones QoS impulsadas por TSN).

La Ethernet es una norma de comunicación de redes consolidada que cuenta con una gran variedad de aplicaciones. Se utiliza en redes (por ejemplo, informáticas) de comunicación de máquina comunes que abarcan múltiples escalas de red de área (como área pequeña, local o metropolitana) y en redes de acceso radioeléctrico terrenales para comunicaciones móviles. A la vista de la historia y el contexto de las redes, hay patrones de seguridad de redes que podrían reutilizarse.

Debido a su uso frecuente, las comunicaciones basadas en Ethernet (incluidos los protocolos de capa superior) pueden ser objeto de diferentes ataques, si bien existen contramedidas para diferentes casos de uso. Por ejemplo, en Internet, se recomienda encarecidamente utilizar la seguridad de la capa de transporte (TLS) en los servicios de transporte basados en el protocolo de control de transmisión (TCP) (únicamente) a fin de garantizar la autenticidad, integridad y confidencialidad de la comunicación. También se recomienda utilizar la seguridad de la capa de transporte de datagramas (DTLS) con protocolo de seguridad de transporte como complemento para los servicios de transporte basados en el protocolo de datagrama de usuario (UDP). Cuando se utiliza la Ethernet como norma establecida y generalizada para la comunicación intravehicular, se pueden reutilizar los mecanismos de seguridad IP asociados con pilas. Sin embargo, las contramedidas conocidas de las redes

informáticas comunes no se pueden considerar apropiadas para una aplicación de automoción porque no fueron diseñadas específicamente para sus requisitos y capacidades. Por ejemplo, es posible que no ofrezcan garantías en tiempo real y que necesiten un rendimiento mayor que no pueda ser facilitado por dispositivos integrados con limitación de recursos. Por tanto, durante la elaboración de la presente Recomendación no se tiene en cuenta la integración de los mecanismos de seguridad para protocolos de comunicación basados en Ethernet y sensibles al tiempo.

Por motivos de seguridad, la separación de la comunicación intravehicular es esencial. Actualmente, los fabricantes de equipo original materializan el aislamiento lógico del tráfico Ethernet por medio de la virtualización de las redes, que hace referencia a una VLAN como red privada virtual de capa 2 en el caso de la Ethernet. Es importante destacar que la separación del tráfico intravehicular puede ejecutarse por otros medios, como VPN de capa 1 (con redes Ethernet separadas físicamente) o de capa 3 (utilizando una solución de VPN conocida para los servicios de comunicación de IP por Ethernet).

Una VLAN constituye un método probado para proporcionar aislamiento lógico en la capa de enlace de datos de las redes informáticas comunes. Con frecuencia, las VLAN se utilizan para separar las redes físicas en diferentes redes lógicas. La aplicación intravehicular de la VLAN se basa principalmente en el hecho de que la VLAN permite establecer prioridades en el tráfico, por ejemplo, correlacionando los puntos de código de prioridad de la VLAN directamente con las clases de tráfico TSN.

NOTA 3 – Los aspectos de seguridad de las VLAN jerárquicas, que podrían considerarse en IVN futuras para modelos específicos de interconexión V2X, son ajenos al alcance de la edición actual de esta Recomendación. Por tanto, se plantea únicamente la hipótesis de VLAN basadas en puertos o con un solo rótulo.

La aplicación de la conocida norma Ethernet en la comunicación intravehicular ofrece algunas posibilidades, aunque es importante tener un cuidado especial. No solo no se aplica ningún mecanismo de seguridad, sino que tampoco se recomienda equipo especial para conectar un dispositivo externo con el vehículo a través de Ethernet.

A los usuarios les puede resultar conveniente intentar enchufar sus ordenadores portátiles o utilizar sus teléfonos inteligentes para mejorar el acceso a las IVN. Si se utiliza un conmutador Ethernet como componente adicional, una persona no autorizada con formación especial dispondrá de un vector de ataque tentador. Los atacantes pueden ejecutar ataques desconocidos desde Internet o *exploits* publicados para conmutadores Ethernet comunes. De forma similar a la seguridad de las comunicaciones, existen contramedidas para los conmutadores Ethernet comunes. Sin embargo, es preciso continuar descubriendo e investigando los entornos de automoción.

En el Cuadro 1 se muestran las diferencias entre los protocolos de IVN heredada por bus de campo y los protocolos de IVN basados en Ethernet de manera muy abstracta. En la primera columna de cada elemento de la comparación se indica la madurez de los criterios respectivos, que se representa con el símbolo que corresponde, como mala (–), neutra (0), bueno (+) y óptima (++). Es importante observar que este cuadro se ha preparado intencionadamente como una simplificación; para realizar una evaluación más detallada de los protocolos sería preciso comparar la Ethernet con cada una de las tecnologías de comunicación de bus de vehículo o de campo.

Cuadro 1 – Comparación entre la arquitectura de comunicación basada en Ethernet y la arquitectura de comunicación heredada de un vehículo

Criterio	**Protocolos IVN orientados al bus de campo (Nota 1)**		**IVN basada en Ethernet**	
Sencillez	–	Pasarela compleja, heterogénea, multiprotocolo	++	Muy homogénea, con conmutadores (en su mayoría) de capa 2

Cuadro 1 – Comparación entre la arquitectura de comunicación basada en Ethernet y la arquitectura de comunicación heredada de un vehículo

Criterio	Protocolos IVN orientados al bus de campo (Nota 1)		IVN basada en Ethernet	
Flexibilidad	–	Ampliación/adaptación difícil de subredes nuevas (fácil dentro de subredes)	++	Ampliación/adaptación fácil de subredes nuevas o dentro de subredes
Rendimiento	+	Depende del tipo de bus	++	Hasta varios gigabits por segundo
En tiempo real	++	Eficacia demostrada a lo largo de decenios	−	Capaz pero no contemplado
Masa de material físico relacionado con las redes	–	Cableado individual por bus	+	Un par trenzado para todos
Costes (inversión, no funcionamiento)	–	Producción específica para automoción en pequeños lotes	+	Producción en masa global, no solo para automoción
Grado de normalización	–	Normalizado con amplia diversidad	+	Normalizado con poca diversidad
Modelos de conectividad en capa de enlace de datos y física (Nota 2)	–	Solo modelos de comunicación de punto a multipunto debido al uso compartido de los medios físicos (bus)	+	Ethernet admite ambos modelos de comunicación, punto a punto y punto a multipunto (Nota 3)
Integridad del mensaje (Nota 4)	+	Comprobación de redundancia cíclica (CRC) + medidas específicas de bus	+	CRC, códigos de bloque
Medidas de seguridad (Nota 5)	−	Prácticamente ninguna	0	Complementos (protocolo Internet versión 4, o IPv4), seguridad del protocolo Internet (IPsec) (protocolo Internet versión 6, o IPv6)

NOTA 1 – Las evaluaciones realizadas aplicando los criterios enumerados reflejan el diseño de protocolo típico, pero no son válidas para todos los casos de tecnologías de la comunicación orientadas al bus de campo, por ejemplo, la CAN no ofrece un protocolo inherente para la comunicación en tiempo real.
NOTA 2 – Se presupone que las aplicaciones intravehiculares suelen requerir servicios de comunicación con topologías de comunicación de tipo punto a punto o punto a multipunto. Estas topologías deben abastecerse con topologías de conexión lógica, lo que implica asumir que las topologías de conexión de capa de enlace son la "capa de protocolo" denominador común de las tecnologías de comunicación analizadas.
NOTA 3 – Las redes Ethernet intravehiculares se desplegarán y utilizarán en "modo conmutado" únicamente (enfocadas principalmente a objetivos de calidad del servicio [QoS]), por lo que los modos de conexión punto a punto solo se admiten en la capa de medios físicos Ethernet. El medio físico no se comparte; más bien, cada punto extremo de capa 1 Ethernet tiene acceso exclusivo a los recursos de capa física. Sin embargo, las topologías de comunicación punto a multipunto también se pueden utilizar: directamente a través de la capacidad de radiodifusión y multidifusión Ethernet integrada, en las funciones de reenvío de la capa de enlace de datos, o indirectamente con protocolos de capa superior (por ejemplo, IP o el tipo de difusión [radiodifusión, multidifusión o cualquier tipo] de la dirección de red).
NOTA 4 – En este caso, la integridad relacionada con la seguridad se refiere a: a) la integridad de los bits; b) la integridad de los datos, es decir, la integridad que afecta a bits individuales de una unidad de datos de protocolo (PDU) o a toda la PDU como tal (en capas de protocolo específicas).
NOTA 5 – Las medidas de seguridad se evalúan tanto si la especificación de protocolo correspondiente tiene funciones de seguridad inherentes como si no las tiene.

Los criterios de comparación presentados abarcan la ingeniería de redes básica y la ingeniería de servicios de comunicaciones, así como aspectos de seguridad específicos.

6.3 Servicios de comunicación que utilizan Ethernet en aplicaciones de automoción

Actualmente, la Ethernet de automoción se utiliza principalmente para el diagnóstico y la transmisión de trenes multimedia, como datos de vídeo desde los sensores de cámara hasta el ADAS. Además, desde mediados de la década de 2010 permite que los nodos de cálculo (como las ECU) de los vehículos se comuniquen a través de Ethernet.

6.3.1 Diagnóstico

El método de diagnóstico convencional de un vehículo consiste en conectar una herramienta de diagnóstico a un puerto OBD-II y comunicarse con la ECU objetivo a través de un protocolo de servicio de diagnóstico unificado (UDS). El UDS es un protocolo del nivel de la aplicación diseñado por la industria de la automoción que permite que los sistemas de diagnóstico se comuniquen con las ECU para diagnosticar las anomalías y reprogramar las ECU en consecuencia (véase [b-ISO 14229-5]).

La comunicación de diagnóstico a través del protocolo Internet (DoIP) se basa en la IP (véase [b-ISO 13400-2]). La DoIP posibilita la transmisión de mensajes UDS a través de Ethernet entre un vehículo y un equipo de prueba externo, así como la recuperación remota de los datos de diagnóstico de un vehículo sin conexión física con el vehículo. La DoIP permite encapsular los mensajes UDS en paquetes TCP o datagramas UDP, como se muestra en la Figura 2.

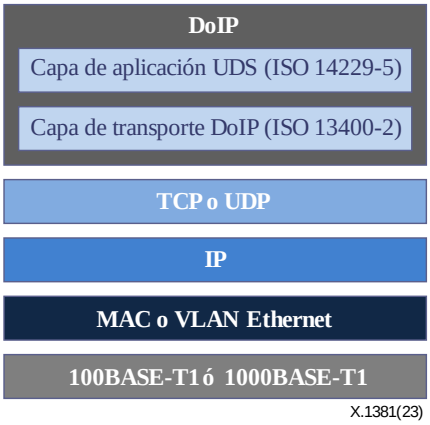

Figura 2 – Pila de protocolos para la comunicación de diagnóstico a través de una aplicación de protocolo Internet

En sí misma, la DoIP no tiene en cuenta ningún mecanismo de seguridad de las comunicaciones. En general, los mensajes no se autentican ni encriptan de ninguna manera. La DoIP puede recurrir a una autenticación en las capas superiores, pero no es obligatoria.

6.3.2 Trenes de medios en el contexto de los servicios multimedia

En el ADAS, los vehículos totalmente autónomos y altamente automatizados deben desplegar muchos sensores, como cámaras de alta definición y funciones de conectividad, para obtener información suficiente y conocer el entorno del vehículo. Además, muchos vehículos cuentan con dispositivos que utilizan o transmiten trenes de medios del nivel de la aplicación – que no deben mezclarse con las (sub)capas de medios físicos en el caso de la Ethernet – que se utilizan en los sistemas de infoesparcimiento, sistemas de control de visión periférica, sistemas de asistencia al aparcamiento, sistemas de asistencia contra cambio de carril, visión nocturna, etc. En el caso de las cámaras, se generan trenes de medios relativamente grandes (en lo que respecta al volumen de tráfico) con objetivos de QoS basados en aplicaciones para la transmisión de baja latencia y gran calidad. Si el

protocolo es CAN, no es posible satisfacer los requisitos anteriores debido a las limitaciones inherentes del diseño del protocolo, como el rango de tamaños de la carga útil.

La Ethernet de automoción puede cumplir estos requisitos si utiliza el marco AVB (transmisión sincronizada de audio y vídeo) de IEEE.

NOTA – El término AVB hace referencia a un conjunto de normas [b-IEEE 802.1], incluidas las normas [b-IEEE 802.1Qav], [b-IEEE 802.1AS] y [b-IEEE 802.1Qat]. Por tanto, en 2012, el grupo de trabajo sobre AVB de IEEE pasó a denominarse grupo de trabajo sobre TSN (TSN Task Group), que ahora incluye las normas AVB.

La AVB puede satisfacer requisitos de TSN más generales, por lo que ofrece la posibilidad de utilizar una única red que gestione las funciones de infoesparcimiento, control corporal y asistencia a la conducción, e incluso algunas funciones críticas para la seguridad.

En el caso el sistema de control de visión periférica, se dispone de una serie de cámaras que ofrecen una vista sincronizada de 360° de los alrededores del vehículo. Este tren de medios de tipo vídeo puede enviarse al sistema de información para el conductor, que puede ser un sistema de visualización de visualización frontal (*head-up display*) o un sistema de navegación de vídeo. También se pueden sincronizar los datos de sensores adicionales y las ECU conexas a través de la red AVB.

6.3.3 Eje de la red intravehicular

Los vehículos modernos pueden llegar a tener más de 100 ECU. Una ECU o nodo de cálculo vehicular hace referencia a un nodo de red de la topología IVN Ethernet, con uno o varios nodos finales (dependiendo del número de interfaces de conexión Ethernet físicas, lógica o virtuales por nodo de cálculo). Además, el número de ECU podría aumentar aún más, de manera que el ADAS y los vehículos autónomos empezarían a requerir una capacidad de transporte de IVN elevada (denominada coloquialmente ancho de banda) para la IVN.

Por otra parte, los protocolos IVN heredados utilizan el sistema de cableado, que es pesado y supone un coste elevado. Si la Ethernet se utiliza como eje de la IVN, se puede reducir el coste de conexión intravehicular en un 80% y el cableado intravehicular en un 30% como máximo.

Tal y como se muestra en la Figura 1, la IVN basada en Ethernet cuenta con varios dominios. Se utilizan protocolos IVN heredados en cada dominio, y la Ethernet se emplea en la comunicación entre dominios, es decir, en el nivel de red básica (si se compara con las redes TIC), que también se conoce comúnmente como eje o red troncal.

La Ethernet de automoción no presenta la misma topología que un sistema de bus. No hay ningún conductor bus conectado a múltiples ECU, sensores y accionadores, sino que están conectados punto a punto con un conmutador Ethernet. Las funciones de interfuncionamiento de red, como las que se proporcionan en los conmutadores Ethernet, las pasarlas VLA y, posiblemente, los encaminadores IP y las pasarelas IP de la IVN basada en Ethernet, se ocupan con facilidad de enviar mensajes de comunicación de un dominio a otro. Por el contrario, para comunicarse con puntos extremo de redes Ethernet, los protocolos de bus de campo intravehiculares heredados necesitan soporte de interfuncionamiento de redes y, posiblemente, también del servicio, que suele ubicarse en las pasarelas.

7 Análisis de amenazas

7.1 Metodología del análisis de amenazas

En este apartado se analizan los escenarios de amenazas de seguridad en el contexto de las redes Ethernet intravehiculares. Las amenazas generales identificadas en los vehículos conectados se describen en [UIT-T X.1371].

Para obtener el concepto de seguridad, se deberían formular objetivos de seguridad. Se realiza un análisis de amenazas y evaluación de riesgos (TARA) para determinar el método de gestión del riesgo en la fase de los objetivos de seguridad. Para ejecutar un TARA, se deberían identificar los activos y

objetivos de seguridad, así como las amenazas conexas. El concepto de seguridad se puede determinar si, a la hora de decidir el método de gestión de los riesgos respectivos, se realiza una valoración del impacto y una valoración de la viabilidad del ataque basándose en los activos de seguridad, los objetivos de seguridad y las amenazas que se han identificado (véase [b-ISO/SAE 21434] para obtener más información).En este apartado se identifican los activos de seguridad y los objetivos de seguridad conexos y, a continuación, las amenazas a la seguridad, de acuerdo con el enfoque de análisis de las amenazas que se expone en [b-ISO/SAE 21434].

Los procesos de valoración del impacto, valoración de la viabilidad del ataque y decisión sobre el riesgo son ajenos al alcance de esta Recomendación y deben ser examinados más a fondo.

7.2 Activos de seguridad

Un activo de seguridad es un objeto de datos, una función o un recurso que deberían ser protegidos. En el Cuadro 2 se enumeran los activos de seguridad extraídos, desde el punto de vista de las IVN basadas en Ethernet.

Cuadro 2 – Activos de seguridad

Activo	Descripción
Datos de gestión	Los datos de gestión incluyen dos categorías (Nota 1): 1) datos de configuración, que caracterizan el comportamiento funcional de los elementos de red o las funciones de red con conexión Ethernet, como una pasarela, un conmutador Ethernet, un sistema de detección de intrusiones (IDS) y un cortafuegos; 2) datos de estado operativo, que describen tanto el comportamiento actual de esas entidades de red como todos los servicios de gestión que utilizan notificaciones [b-UIT-T M.3702], como la notificación de alarmas [b-UIT-T M.3703] en el marco de la gestión de anomalías. En esencia, los flujos de datos de gestión de ambas categorías que conectan a la entidad gestora y a la entidad gestionada son objeto de protección de seguridad. Sin embargo, por regla general, el impacto sobre la seguridad (derivado, por ejemplo, de la manipulación de los datos de configuración) debería ser mucho mayor que el impacto en los datos del estado operativo. Por otra parte, la situación de anomalía actual podría empeorar, por ejemplo, debido a la supresión intencionada de una alarma emitida por un elemento de red Ethernet.
Unidades de datos de protocolo de capa 2 relacionadas con la comunicación Ethernet	El tráfico de Ethernet está formado por el tráfico de la capa de enlace de datos, esto es, las tramas de control de acceso a los medios (MAC) de Ethernet (como PDU de capa 2) que se transfieren a la IVN de automoción basada en Ethernet.
Datos de gestión generados mediante registro (Nota 2)	Se puede someter a auditoría la detección satisfactoria de eventos de seguridad y la información conexa.
Material criptográfico	Claves y certificados de planes simétricos y asimétricos, incluidas otras credenciales, como la contraseña.
Firmware o imagen de *software*	El código compilado que se ejecutará en nodos de cálculo vehiculares como las ECU.
NOTA 1 – Véase el marco de gestión de redes aplicable a Ethernet, por ejemplo, que se describe en: [b-UIT-T M.3010], [b-UIT-T X.703], [b-UIT-T G.8013] y [b-UIT-T Y.1730]. Los datos de gestión para entidades de red Ethernet se basan en YANG [b-IETF RFC 6020] como especificación y lenguaje de modelado de datos de gestión. La IEEE 802 (como propietario tecnológico de la Ethernet) proporciona modelos de datos de gestión basados en YANG para las diferentes entidades Ethernet, esto es, la principal referencia de datos de gestión de esta Recomendación.	

Cuadro 2 – Activos de seguridad

Activo	Descripción
NOTA 2 – Le gestión de las funciones de registro [b-UIT-T M.3705] no se contempla en este cuadro. En este contexto, el registro hace referencia al evento de sistema causado por flujos de información de gestión que se anotan utilizando las funciones de registro (véase [b-UIT-T G.7710] sobre flujos internos de datos de gestión de equipos de red). NOTA 3 – Esta función de detección se inscribe en la categoría de prueba de hipótesis estadísticas, debido principalmente a las incertidumbres asociadas a la descripción de eventos o a la descripción de condiciones de reglas de políticas con miras a la identificación no ambigua de tales eventos. Por tanto, si la detección se completa de manera correcta, se obtienen únicamente resultados probabilísticos inherentes, que incluyen tanto verdaderos positivos como falsos positivos. A continuación, se debería calificar y cuantificar el nivel de calidad de la detección, por ejemplo, calculando la proporción prevista de positivos no verdaderos.	

7.3 Objetivos de seguridad

Los activos de seguridad (véase la cláusula 7.1) se analizan con referencia a una lista de objetivos de seguridad, como figura en el Cuadro 3.

Cuadro 3 – Objetivos de seguridad

Activo de seguridad	Objetivo de seguridad	Explicación
Datos de gestión	Integridad, confidencialidad	No se deberían manipular los datos que determinan el comportamiento funcional de los elementos de red Ethernet, como la pasarela de vehículo, el conmutador Ethernet, el IDS y el cortafuegos
Unidades de datos de protocolo de capa 2 relacionadas con la comunicación Ethernet	Confidencialidad	Se impide que se muestren las unidades de datos de protocolo de capas específicas ((Lx)-PDU) transferidas a una IVN de automoción basada en Ethernet
	Disponibilidad	Se debería poder prestar servicios de comunicaciones entre IVN de automoción basadas en Ethernet cuando resulte necesario, siempre y cuando se respeten las limitaciones relacionadas con el servicio de comunicación
	Autenticidad	Las comunicaciones en IVN de automoción basada en Ethernet deberían detectar y rechazar a los impostores de otros componentes
	Integridad	Se impide la manipulación de los datos de comunicación intercambiados en la automoción basada en Ethernet
Datos de gestión generados mediante registro	Integridad	Se impide la manipulación sin posibilidad de detección de las pruebas y la información de los eventos de seguridad registrados que se pueden someter a auditoría. La integridad incluye la integridad de los bits y los datos en relación con la información registrada
Material criptográfico	Confidencialidad	Se impide que se muestren las claves secretas y privadas, además de las credenciales de usuario como las contraseñas
	Integridad	Se impide la manipulación sin posibilidad de detección de las claves y los certificados

Cuadro 3 – Objetivos de seguridad

Activo de seguridad	Objetivo de seguridad	Explicación
Firmware o imagen de *software*	Confidencialidad	Se impide que se muestre a entidades no autorizadas el contenido del *firmware* y el *software*, como el código compilado y los datos de calibración relacionados con la propiedad intelectual
	Integridad	Se impide la manipulación del *firmware* y las imágenes de *software*, por ejemplo, como objetos de los procedimientos de cambio de capacidad (como el *firmware* o *software* por vía aérea o la gestión de *software* en general)

7.4 Amenazas detectadas

7.4.1 Amenazas a la confidencialidad

– Exposición no autorizada del tráfico de comunicación Ethernet (formado por PDU de capa física Ethernet [L1] o de capa de enlace de datos [L2])

Un atacante puede rastrear el tráfico de comunicación Ethernet conectando el componente responsable de la comunicación externa con el conmutador Ethernet. A continuación, el atacante analiza la información del tráfico de comunicación rastreando las PDU relacionadas con Ethernet.

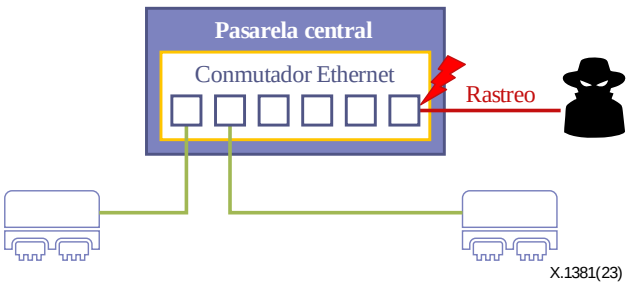

Figura 3 – Amenazas a la confidencialidad por rastreo

– Exposición no autorizada de material criptográfico

Un atacante puede rastrear material criptográfico de las maneras siguientes:

- obteniendo material criptográfico mediante la apertura física de la caja de almacenamiento;
- leyendo el material criptográfico de la memoria de cada componente en el que se utiliza el material;
- modificando el *firmware* y alterando el flujo de control para exponer el material criptográfico.

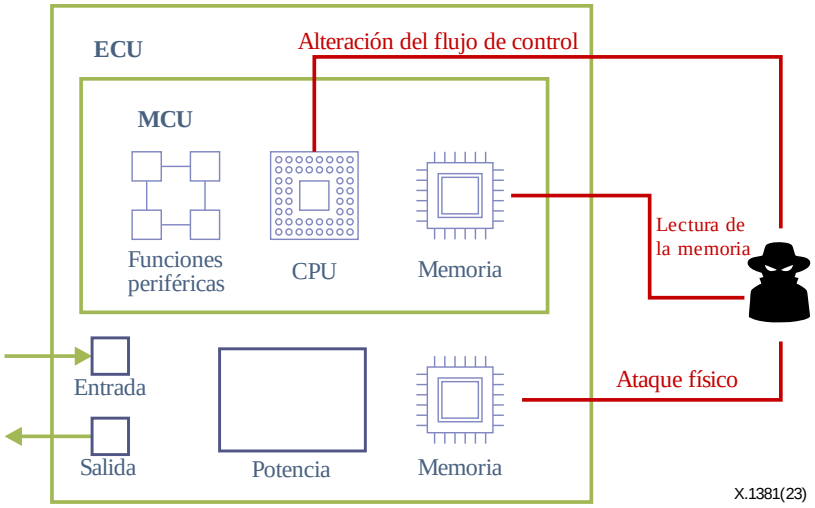

Figura 4 – Amenazas a la confidencialidad de material criptográfico

7.4.2 Amenazas a la integridad

El contexto de la integridad se limita a los objetos de datos en general, que se indican aquí mediante casos de uso de seguridad específicos.

– Manipulación de los datos de configuración

Un atacante puede manipular los datos de configuración del conmutador Ethernet.

– Manipulación de los datos de registro

Un atacante puede eliminar o modificar los datos de registro, y en especial los registros de auditoría de eventos de seguridad del IDS, el cortafuegos y el sistema por vía aérea.

– Manipulación de material criptográfico

Un atacante puede cambiar material criptográfico válido por sí solo.

– Manipulación del *firmware*

Un atacante puede convertir el *firmware* en *firmware* malicioso.

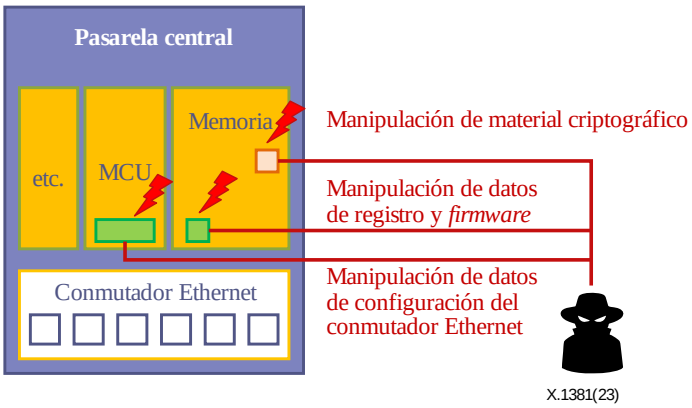

Figura 5 – Amenazas a la integridad de las unidades de datos objeto de comunicación

7.4.3 Amenazas a la disponibilidad

En este contexto, la disponibilidad de atributos de calidad del sistema hace referencia a la disponibilidad del servicio de comunicaciones para comunicaciones basadas en Ethernet, que se traduce en requisitos generales de disponibilidad de conexión de capa y red, lo que puede traducirse a su vez, por ejemplo, en disponibilidad de trayectos Ethernet en el caso de una IVN Ethernet con trayectos redundantes.

– Amenazas específicas contra la disponibilidad: Ataque de denegación de servicio (DoS) en IVN basada en Ethernet

Un atacante puede lanzar un ataque DoS para obstruir la funcionalidad de una ECU específica, como una CGW, una pasarela de vehículo limítrofe o una unidad de control de conectividad.

Tal y como se muestra en la Figura 6, un atacante puede hacer que una ECU y una CGW específicas no están disponibles para las ECU contrarias deseadas utilizando técnicas de ataque DoS conocidas, por ejemplo, ataques específicos contra el protocolo de transporte IP como inundación SYN del TCP o ataques por fragmentación (*teardrop*) contra el TCP Además, un atacante puede agotar los recursos de la IVN, por ejemplo, con ataques de tormenta de difusión de capa 2, de manera que ya no se puedan intercambiar las tramas MAC de Ethernet normales (como las PDU de capa 2).

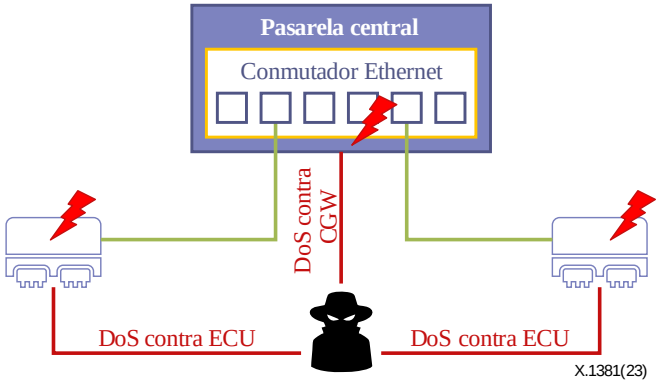

Figura 6 – Amenazas a la disponibilidad

7.4.4 Amenazas a la autenticidad

– Suplantación de nodos de cálculo intravehiculares (como ECU)

Un atacante puede suplantar un componente válido, como una ECU, y enviar mensajes maliciosos a otros componentes. Un atacante puede fingir ser un punto extremo de comunicación válido (por ejemplo, albergado por una ECU) y enviar mensajes maliciosos o conseguir el tráfico de comunicaciones transmitido. En el ejemplo que se muestra en la Figura 7, la situación normal viene determinada por las conexiones de capa superior entre las ECU A y B (por ejemplo, conexiones de transporte IP de punto a punto), y como resultado la ECU-A envía el tráfico Ethernet a la ECU-B (y, posiblemente, viceversa). Un atacante finge ser la ECU-A utilizando métodos de ataque como falsificación del protocolo de resolución de direcciones (ARP) o falsificación de IP (véase, por ejemplo, [b-IETF RFC 2827], [b-IETF RFC 4953], [b-IETF RFC 6575], [b-IETF RFC 6959]) y, a continuación, envía un mensaje malicioso a la ECU-B.

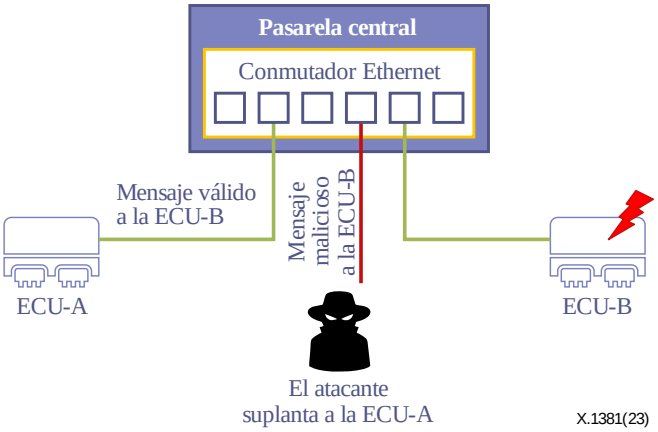

Figura 7 – Amenazas a la autenticidad

8 Requisitos de seguridad

En este apartado se describen los requisitos de seguridad que se ocupan de amenazas identificadas en entornos de IVN basada en Ethernet.

8.1 Confidencialidad

– [SR-01] Se recomienda que una ECU que almacena y utiliza material criptográfico haga uso del almacenamiento seguro, como un módulo de seguridad de *hardware* (HSM), para almacenar el material criptográfico con seguridad.

– [SR-02] Se recomienda utilizar en el despliegue los algoritmos y protocolos conocidos especificados, por ejemplo, por organizaciones internacionales de normalización.

– [SR-03] En los mensajes de las comunicaciones Ethernet se recomienda utilizar mecanismos de seguridad para evitar la escucha clandestina.

Opcionalmente, se pueden aplicar varios protocolos de seguridad de capas específicas a la capa de protocolo correspondiente con miras a su cifrado y a la PDU específica del protocolo (en su totalidad o parcialmente) como parte del tráfico de comunicación basada en Ethernet de un vehículo. Algunos ejemplos de estos protocolos de seguridad de las comunicaciones son la seguridad de control de acceso a los medios (MACsec), IPsec, TLS y DTLS.

– [SR-04] Se impide que una entidad no autorizada muestre material criptográfico sensible.

El mecanismo de seguridad de un vehículo deja de ser seguro cuando se expone el material criptográfico a entidades no autorizadas.

– [SR-05] Se recomienda que solo el personal y el equipo autorizados de acuerdo con una política de control de acceso en vehículo manejen el material criptográfico durante la etapa de producción.

– [SR-06] Se recomienda que la tabla de direcciones MAC del conmutador Ethernet esté configurada en estático.

Las ECU predefinidas puede acceder a una Ethernet en un vehículo configurando en estático la tabla de direcciones MAC en el conmutador Ethernet.

Las direcciones MAC dinámicas pueden provocar problemas de seguridad, como falsificación e inundación de MAC. Cuando la tabla almacene un número elevado de direcciones MAC, el conmutador puede comunicar la trama de datos por radiodifusión a todos los puertos de red. En el caso de un vehículo, la tabla de direcciones MAC se puede configurar en estático para prevenir estos problemas de seguridad, puesto que ya se ha especificado la ECU que se comunica con el conmutador.

– [SR-07] Se recomienda deshabilitar la función de aprendizaje dinámico de una tabla de direcciones MAC en un conmutador Ethernet.

  Si se desactiva la función de aprendizaje dinámico de la tabla de direcciones MAC, se puede evitar una inundación de MAC, que puede causar la transmisión de mensajes de Ethernet a destinos no intencionados.

  Sin embargo, cuando la función sea crucial para el funcionamiento o mantenimiento del vehículo, el conmutador no debería almacenar direcciones MAC aprendidas por un tiempo limitado únicamente.

– [SR-08] Se recomienda que las interfaces de red de IP de las funciones de anfitrión IP (por ejemplo, alojado por ECU) que utilizan la Ethernet consigan direcciones IP fijas asignadas por la función de gestión de redes responsable.

NOTA – En esta SR, cuando se habla de funciones de gestión de red específicas se hace referencia a la gestión de identidades, que incluye la gestión de direcciones de red. Estas funciones de gestión pueden realizarse a lo largo de diferentes ciclos de vida y en distintas etapas operativas de la IVN basada en Ethernet, por ejemplo, gestión de configuración dinámica y estática combinada y totalmente estática *a priori*, y dependen de que se utilicen los protocolos de funcionamiento de redes para las capas de Internet y Ethernet.

Esta SR se aplica no solo a las ECU individuales en conjunto, sino también a cada partición o nodo de una red de Ethernet (por ejemplo, cada máquina virtual).

8.2 Integridad

– [SR-09] Se recomienda que los datos de registro y configuración de un conmutador Ethernet estén protegidos contra modificaciones y supresiones no autorizadas.

– [SR-10] Se recomienda que las actualizaciones de los datos de configuración sean ejecutadas únicamente por entidades autorizadas.

– [SR-11] Se recomienda que una ECU utilice funciones de arranque seguro junto con un control de la integridad del *firmware*.

Se debería comprobar la integridad, durante la ejecución o antes de ella, del *firmware* de una ECU y de los datos de conmutador Ethernet almacenados en la memoria de la ECU. Se puede utilizar un control de integridad de los parámetros de configuración y entrada del *firmware* para garantizar la seguridad del arranque.

8.3 Disponibilidad

En este contexto, "disponibilidad" hace referencia a la disponibilidad de red de los dominios Ethernet, esto es, el servicio de comunicación disponible. Los ataques a la seguridad pueden afectar a estos objetivos de disponibilidad, pero también a otros tipos de eventos específicos ajenos a la seguridad, como la escasez de componentes o un fallo de comunicación.

Por tanto, los requisitos de disponibilidad (de este apartado) son en realidad requisitos de seguridad que pueden afectar a los objetivos de disponibilidad.

– [SR-12] Se recomienda que los ataques DoS contra IVN basadas en Ethernet se tengan en cuenta durante la etapa de diseño de un vehículo.

– [SR-13] Se recomienda que un conmutador detecte los ataques DoS y proteja contra ellos mediante mensajes de comunicación Ethernet.

  La supervisión y el control de los flujos de tráfico entre ECU son cruciales para minimizar los riesgos derivados de los ataques DoS en una IVN.

– [SR-14] Se recomienda utilizar funciones de seguridad crítica para el aislamiento respecto de otras redes de un vehículo.

8.4 Autenticidad

Por "autenticidad" se entiende la capacidad de garantizar que la información facilitada no ha sido modificada o falsificada y ha sido elaborada de verdad por la entidad que asegura haber proporcionado la información.

– [SR-15] Se recomienda facilitar contramedidas para que los mensajes de comunicación Ethernet estén protegidos frente a ataques por suplantación.

– [SR-16] Se recomienda que las interfaces de red Ethernet físicas de los elementos de red IVN, que no se han concebido para ser utilizadas en un vehículo de producción, permitan realizar cambios de estado administrativo temporales (habilitar, inhabilitar) utilizando el valor de configuración predeterminado correspondiente a "desactivado".

NOTA – Un requisito de gestión de redes de este tipo conlleva, evidentemente, la compatibilidad con un modelo de datos de gestión granulares finos para Ethernet.

Este requisito limita la superficie de ataque al reducir el número de puntos de entrada disponibles.

– [SR-17] Se recomienda limitar la interfaz de comunicación de acceso de acuerdo con el principio de menor privilegio posible, independientemente de que se materialice en el dominio de *hardware* o de *software*.

– [SR-18] Se recomienda configurar una interfaz de depuración de una ECU como protección frente a entidades no autorizadas. Este requisito se aplica a las interfaces de depuración locales de nodo de cálculo vehicular, así como a las interfaces de depuración remotas con acceso basado en IVN a un nodo de cálculo de este tipo.

En el Cuadro 4 se muestra la correspondencia entre las amenazas identificadas en la cláusula 7 y los requisitos de seguridad de la cláusula 8.

Cuadro 4 – Correspondencia entre los requisitos de seguridad y las amenazas

Amenazas	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Exposición no autorizada de un mensaje de comunicación Ethernet	–	S	S	–	–	–	–	–	–	–	–	–	–	–	–	–	–	S
Exposición no autorizada de material criptográfico	S	S	–	S	S	–	–	–	–	–	–	–	–	–	–	–	–	S
Manipulación de datos de configuración	S	S	–	–	–	S	S	–	S	S	S	–	–	–	–	–	–	S
Manipulación de datos de registro	S	S	–	–	–	–	–	–	S	–	S	–	–	–	–	–	–	S
Manipulación de material criptográfico	S	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	S
Ataque DoS contra IVN basada en Ethernet	–	–	–	–	–	–	–	–	–	–	–	S	S	S	–	–	–	–
Suplantación de ECU	–	S	–	–	–	S	S	S	–	–	–	–	–	S	S	S	S	S

Todas las amenazas identificadas se pueden resolver si se satisfacen los requisitos de seguridad correspondientes marcados con S. Por ejemplo, los requisitos de seguridad de la primera amenaza, Exposición no autorizada de un mensaje de comunicación Ethernet, son [SR-2], [SR-3] y [SR-18].

9 Implementación de redes intravehiculares basadas en Ethernet con seguridad

9.1 Consideraciones previas relativas a la implementación

En esta Recomendación se facilitan consideraciones relativas a la implementación con los objetivos siguientes:

- presentar los aspectos de seguridad que dependen de limitaciones técnicas;
- ilustrar los problemas de seguridad de una arquitectura de IVN técnica típica que son específicos de la implementación.

El valor de esta información de seguridad está intrínsecamente vinculado con su correspondiente perspectiva técnica únicamente, aunque esta conexión podría quedar obsoleta en el futuro, por ejemplo, si se producen cambios en las arquitecturas de sistema técnico de las IVN.

No obstante, todavía no se dispone de arquitecturas o modelos de referencia de IVN no técnicos y aplicables que puedan utilizarse como punto de partida del debate sobre los aspectos de seguridad específicos de la implementación. Por tanto, en esta Recomendación se presentan al menos algunas consideraciones de seguridad a través de ejemplos de sistemas técnicos de IVN (como se mencionó en la cláusula 6).

9.2 Funciones de pasarela de seguridad asociadas a la Ethernet de automoción

Para minimizar el riesgo de acceso no autorizado y ataque DoS en IVN basadas en Ethernet, es importante supervisar y controlar el flujo de comunicación entre los diferentes dominios de red lógica (por ejemplo, VLAN, subred IPv4, subred definida por prefijo IPv6; cada dominio de red lógica representa un dominio de seguridad específico en función de sus atributos de seguridad). Las pasarelas de seguridad en general, o los cortafuegos en particular, se utilizan para permitir o rechazar los datos de comunicación de acuerdo con normas predeterminadas en la IVN o en el cruce de las redes intravehiculares y externas a fin de aumentar el nivel de seguridad del vehículo.

Para la aplicación de esas funciones de pasarela de seguridad (como cortafuegos), tal y como se conocen en la actual arquitectura E/E técnica intravehicular, se recomienda utilizar los componentes técnicos siguientes, capaces de supervisar los mensajes de comunicación procedentes del exterior del vehículo o la IVN.

– Conmutador Ethernet.

NOTA 1 – El componente de conmutador Ethernet. lógico representa un tipo de nodo de red, no un nodo final. Existen dos opciones de implementación de IVN: un conmutador Ethernet como componente técnico independiente o un conmutador Ethernet integrado monolíticamente como nodo frontal o final en un nodo de cálculo vehicular.

– Pasarela de vehículo limítrofe.

NOTA 2 – Es la elección natural ya que ese componente técnico representa el único punto de observación del tráfico de comunicación V2X regular.

– ECU: Cuando la ECU dispone de comunicación externa directa.

NOTA 3 – Un nodo de cálculo vehicular puede proporcionar interfaces de comunicación adicionales para la comunicación externa directa del vehículo (esto es, evitando la pasarela de vehículo limítrofe), por ejemplo, con fines diagnósticos.

El cortafuegos utiliza varios mecanismos para el filtrado de paquetes, como el filtrado de paquetes estáticos, la inspección de paquetes con o sin estado, o la inspección superficial, moderada o incluso detallada de paquetes.

NOTA 4 – Los términos, en ocasiones metafóricos, "superficial", "detallada", etc. deben correlacionarse y asociarse con: a) la capa de protocolo; y b) el tipo de información contextual de la PDU (véase, por ejemplo, [b-UIT-T Y.2770], [b-UIT-T Y.2771]) para evitar la ambigüedad; por ejemplo, habitualmente la "inspección superficial de paquetes" sería una inspección de encabezamiento L3,4 en el caso del tráfico de Internet.

En particular, los mecanismos de filtrado de paquetes estáticos se basan en reglas de políticas predefinidas. Por consiguiente, se recomienda definir reglas de políticas específicas en función de la arquitectura vehicular E/E y el protocolo de comunicación aplicado. Además, la política de cortafuegos se aplica de forma predeterminada al método de la lista blanca, que básicamente bloquea todas las comunicaciones que no están permitidas de manera explícita.

Una característica importante del cortafuegos es la defensa contra ataques DoS. Los cortafuegos pueden proteger la red frente a ataques DoS definiendo umbrales con valores prealmacenados, como contadores, o aplicando filtros de frecuencia.

Otra función complementaria del cortafuegos es la función de registro (esto es, el elemento de red del cortafuegos, en tanto que entidad gestionada, proporciona una función integrada de gestión de registros conforme a [b-UIT-T M.3705]). Se espera que, en general, los servicios de registro actúen en caso de evento relacionado con la seguridad. Por tanto, cuando se produce un evento de seguridad, los cortafuegos, IDS o pasarelas de seguridad en general registran la información, de manera que no solo ayudan a los especialistas forenses a analizar la situación del evento, sino que también mejoran la precisión de la política de cortafuegos mediante estudios como los registros de bloqueo. En consecuencia, al almacenar el registro, es necesario utilizar el mecanismo criptográfico para garantizar la integridad.

9.3 Configuración de VLAN segura

Para que la seguridad de las comunicaciones de la IVN pueda cumplir los requisitos [SR-14] y [SR-17] es muy importante configurar una VLAN segura. Se espera que los fabricantes de equipo original sean la autoridad responsable de la especificación de esa VLAN, ya que la configuración de la VLAN depende de la arquitectura vehicular E/E seleccionada por los fabricantes de equipo original.

Cada VLAN cuenta con un valor único denominado identificador (ID) de VLAN. De acuerdo con la especificación de la VLAN, puede utilizarse un ID de VLAN (VID) entre 0 y 4094, aunque no se debería utilizar el VID predeterminado descrito en el Cuadro 5. El VID 1 también puede utilizarse para los ataques que utilizan un doble rótulo; por tanto, el conmutador debería cambiar el VID 1 por otro VID.

Cuadro 5 – ID de VLAN reservados

Valor de VID (hexadecimal)	Significado/Uso
0	El VID nulo indica que el encabezado de rótulo contiene únicamente información prioritaria; la trama no contiene ningún VID. El valor de VID no debería configurarse como un ID de VLAN de puerto (PVID) o un miembro de un conjunto de VID, ni debe configurarse en ninguna entrada de base de datos de retransmisión (FDB) o utilizarse en operaciones de gestión.
1	El valor de PVID predeterminado utilizado para clasificar tramas en el momento de su ingreso a través de un puerto de puente. El valor de PVID de un puerto puede ser modificado con una operación de gestión.
FFF	Reservado para su uso en implementaciones. Este valor de VID no debería configurarse como PVID o miembro de un VID ni ser transmitido en un encabezado de rótulo. Este valor de VID se puede utilizar para indicar una concordancia de comodín para el VID en operaciones de gestión o entradas de la FDB.

Un atacante puede vigilar el tráfico Ethernet mediante un acceso no autorizado desde otra VLAN con un ataque por "desplazamiento sucesivo de VLAN". Para mitigar este ataque, se debería establecer la configuración de manera que las tramas que no están rotuladas con VLAN sean abandonadas. Sin embargo, se pueden producir las excepciones siguientes. Cuando se realiza una sincronización temporal, los mensajes se envían a través del protocolo de tiempo de precisión, que requiere que las tramas se transmitan sin rótulos de VLAN de acuerdo con lo dispuesto en [b-IEEE 802.1AS].

Un atacante que se encuentra en una VLAN nativa puede ejecutar un ataque de doble rotulado utilizando un ID de VLAN nativa predeterminado. El atacante añade dos rótulos a la trama: el primero contiene el ID de VLAN nativa predeterminado y el segundo, el ID de VLAN objetivo del atacante. Cuando la trama con rótulos añadidos pasa por el primer conmutador, se elimina el primer rótulo y la trama con el segundo rótulo se retransmite al siguiente conmutador, que a continuación reenvía la trama a la VLAN objetivo utilizando el segundo rótulo restante. De esta forma, el atacante puede enviar el mensaje a la VLAN objetivo. Por consiguiente, se debería cambiar el ID de VLAN nativa predeterminado para evitar este ataque.

9.4 Seguridad para conmutadores Ethernet en el contexto de la automoción

El puente Ethernet IEEE, también denominado conmutador Ethernet, proporciona intrínsecamente una base de información de retransmisión (FIB) que posibilita el proceso de conmutación y retransmisión de manera nativa. Esta FIB incluye una tabla de direcciones MAC.

NOTA 1 – En esta Recomendación se utiliza un modelo de conmutador Ethernet muy abstracto y se centra únicamente en las funciones de red que pueden ser objeto de procedimientos de seguridad. Se puede consultar una presentación completa de todas las funciones básicas del conmutador Ethernet en [b-IEEE Std 802.1Q].

NOTA 2 – Por ejemplo, en [b-IEEE 802.1Q] se especifica un modelo de normas (de políticas) para procesamiento de tramas MAC Ethernet, que se divide en normas de ingreso, de retransmisión y de egreso. Este modelo resulta especialmente interesante, por ejemplo, en el contexto de las VLAN.

Los conmutadores Ethernet habituales proporcionan mecanismos de aprendizaje de direcciones dinámicas para las redes que requieren flexibilidad. Cuando se conecta una ECU nueva al puerto del conmutador, se añade automáticamente una entrada para la dirección MAC de un nodo final Ethernet a la tabla de direcciones MAC de manera que se pueda comunicar con otras ECU en todo el dominio de red Ethernet, a través de esa etapa de conmutador.

NOTA 3 – El trayecto de comunicación extremo a extremo puede contener más de un conmutador Ethernet.

La función de aprendizaje de direcciones MAC dinámicas facilita el acceso no autorizado a la red y debería estar desactivado. En ocasiones, será necesario utilizar esta función, cuando se requieran dispositivos de diagnóstico externos para fines de mantenimiento o diagnóstico, en cuyo caso el conmutador debería admitir la capacidad de limitar el tiempo de validez de las direcciones MAC aprendidas de manera dinámica. Es evidente que estas dos recomendaciones son contradictorias, pero en realidad dependen del contexto operativo específico de la red Ethernet intravehicular (con o sin conectividad externa a, por ejemplo, un dominio de red Ethernet para DoIP). Estas dependencias del contexto operativo de la red pueden traducirse en recomendaciones de seguridad condicionadas, por ejemplo, en este caso se establecería un intervalo de tiempo limitado y restringido para habilitar el aprendizaje de direcciones dinámicas.

La inundación de direcciones MAC es un ataque conocido contra redes informáticas que puede ejecutarse en situaciones de ataque a vehículos. Para proteger la IVN, si se utiliza una variante de acceso, se debería garantizar la autenticación y fiabilidad de los dispositivos conectados utilizando el control de acceso a redes mediante puerto. Con un control de este tipo se autentican los componentes antes de concederles acceso a la red. El conmutador Ethernet se comunica con la red únicamente si la autenticación es satisfactoria.

A fin de mitigar los ataques DoS, el conmutador debería prevenir las tormentas de difusión y admitir límites de velocidad basados en puertos para la recepción de paquetes (véase el control de parámetros del tráfico Ethernet de [b-UIT-T Y.1222]).

En lo que respecta a la seguridad del conmutador, se debería garantizar la integridad de los datos de gestión de configuración del conmutador, y la única manera de hacerlo sería utilizando un mecanismo de programación seguro o un protocolo de gestión seguro para las actualizaciones.

– En general, las funciones de seguridad requeridas para el funcionamiento y la gestión de los conmutadores Ethernet en las aplicaciones de automoción que tienen integrado un procesador propio son las siguientes: Almacenamiento seguro

  El almacenamiento seguro garantiza la confidencialidad e integridad de los datos almacenados. Se deberían proteger los datos, como las claves y el MAC, utilizando almacenamiento seguro como un HSM.

– Arranque seguro

  El arranque seguro verifica la integridad del *software* en cada ciclo de arranque. Con el arranque inicial, se genera un código de autenticación de mensaje de la imagen de *software*, que se conserva en un almacenamiento seguro. Con el siguiente arranque, si el código de autenticación de mensaje recién generado coincide con el código almacenado, se garantiza la integridad del *software*.

– Interfaz de depuración segura

  Una interfaz de depuración segura impide el acceso no autorizado a la interfaz de depuración. Por regla general, se recomienda eliminar las interfaces de depuración para que no se pueda conectar ninguna entidad de depuración. No obstante, si es preciso utilizar las interfaces para la garantía o el mantenimiento del producto, se debería permitir el acceso a las entidades autorizadas únicamente.

– Actualización segura de *software*

  Una actualización segura de *software* permite reprogramar un *software* únicamente si se ha verificado la autenticidad del *software*. El proveedor del *software* utiliza su clave privada para generar una firma digital que envía junto con la imagen de *software*. Cuando el receptor comprueba que la firma digital ha sido generada por el proveedor utilizando la clave pública del proveedor, se garantiza la autenticidad del *software*.

Apéndice I

Descripción de algunos protocolos de red intravehicular basada en Ethernet con puntos extremo ubicados en nodos de cálculo AUTOSAR o no AUTOSAR

(Este apéndice no forma parte de la presente Recomendación.)

Existen varios protocolos de comunicación para las redes basadas en Ethernet, y muchos casos de uso utilizados en la comunicación intravehicular basada en Ethernet emplean uno de ellos o una combinación de varios. Además, los nodos de cálculo de las IVN no solo pueden utilizarse con sistemas que presentan arquitecturas de *software* basadas en AUTOSAR (como la AUTOSAR Classic Platform o la AUTOSAR Adaptive Platform), sino que también utilizan arquitecturas de comunicación basadas en *software* no AUTOSAR.

Por tanto, básicamente se presupone que una IVN está compuesta por una combinación de nodos de cálculo AUTORSAR y no AUTOSAR en el contexto de la ingeniería de IVN por Internet y Ethernet.

I.1 Descripción y alcance

En este Apéndice se explican brevemente los protocolos que se pueden utilizar en la comunicación intravehicular basada en Ethernet, como se muestra en la Figura I.1.

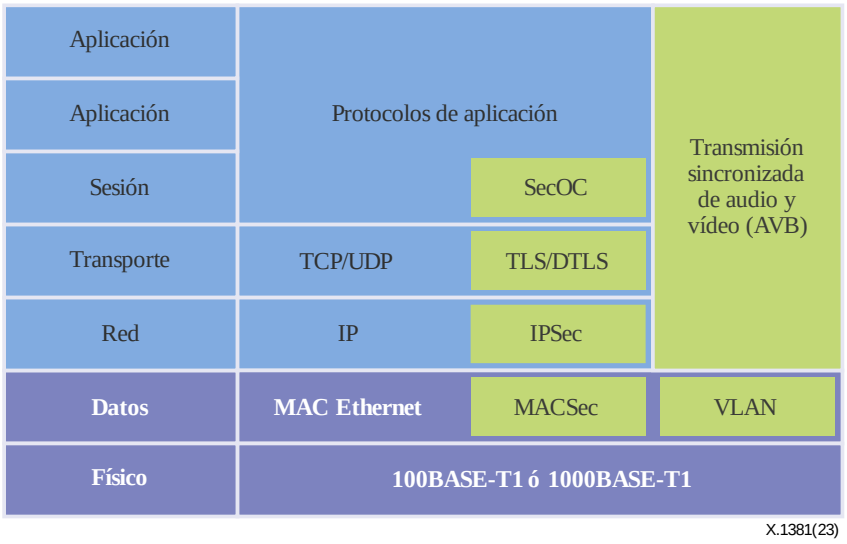

Figura I.1 – Servicios de comunicación por Ethernet, basados en el protocolo Internet y sin protocolo Internet, con los protocolos de seguridad de capa específica asociados que son el objetivo de las redes intravehiculares

Es importante destacar que la Figura I.1 se centra en los servicios de transporte de comunicaciones, no en los protocolos de la capa de aplicación y sesión. Por ejemplo, el protocolo de AUTOSAR "Scalable Service-Oriented Middleware over IP" (SOME/IP), que es un protocolo de la capa de presentación y sesión para comunicaciones orientadas a servicios y basadas en IP, es ajeno al alcance de la presente Recomendación.

I.2 Protocolos de seguridad de capas inferiores con comunicación a bordo segura de AUTOSAR

Es importante recordar que AUTOSAR determina la arquitectura de *software* y, por tanto, excluye las arquitecturas de despliegue. Así, existen múltiples opciones para correlacionar el sistema de

software siguiente con elementos de procesador (concurrencia, paralelismo, sustitución de la pila de comunicación definida en AUTOSAR por una pila comercial integrada, etc.)

La Ethernet forma parte de su norma desde AUTOSAR Classic 4.0 [b-Autosar 654]. En la arquitectura AUTOSAR, la pila de comunicación Ethernet está ubicada en paralelo (en la arquitectura de *software*) con las instancias de pila CAN, LIN y FlexRay.

El encaminador PDU AUTOSAR es responsable del encaminamiento interno del nodo de cálculo en las PDU AUTOSAR entre las aplicaciones AUTOSAR y las interfaces de red asociadas de punto extremo de la comunicación.

NOTA 1 – Por consiguiente, la función de encaminador de la PDU AUTOSAR se superpone, pero no debe confundirse con las funciones de enrutamiento de tráfico heredadas de los puntos extremo de comunicación no AUTOSAR.

El mensaje generado por la aplicación se envía al enrutador PDU, que transmite un mensaje al módulo de interfaz o protocolo de transporte (TP) correspondiente. Cada interfaz/TP transmite el mensaje a una interfaz de red a través de un controlador pertinente. En el caso de la Ethernet, el enrutador PDU envía un mensaje al adaptador de conector (esto es, el punto de acceso de servicio de capa 4 para la comunicación basada en TCP o UDP), que se transmite a la interfaz Ethernet a través del módulo TCP/IP. En la Figura I.2 se muestra el flujo de control y datos en la pila de comunicación AUTOSAR ampliada.

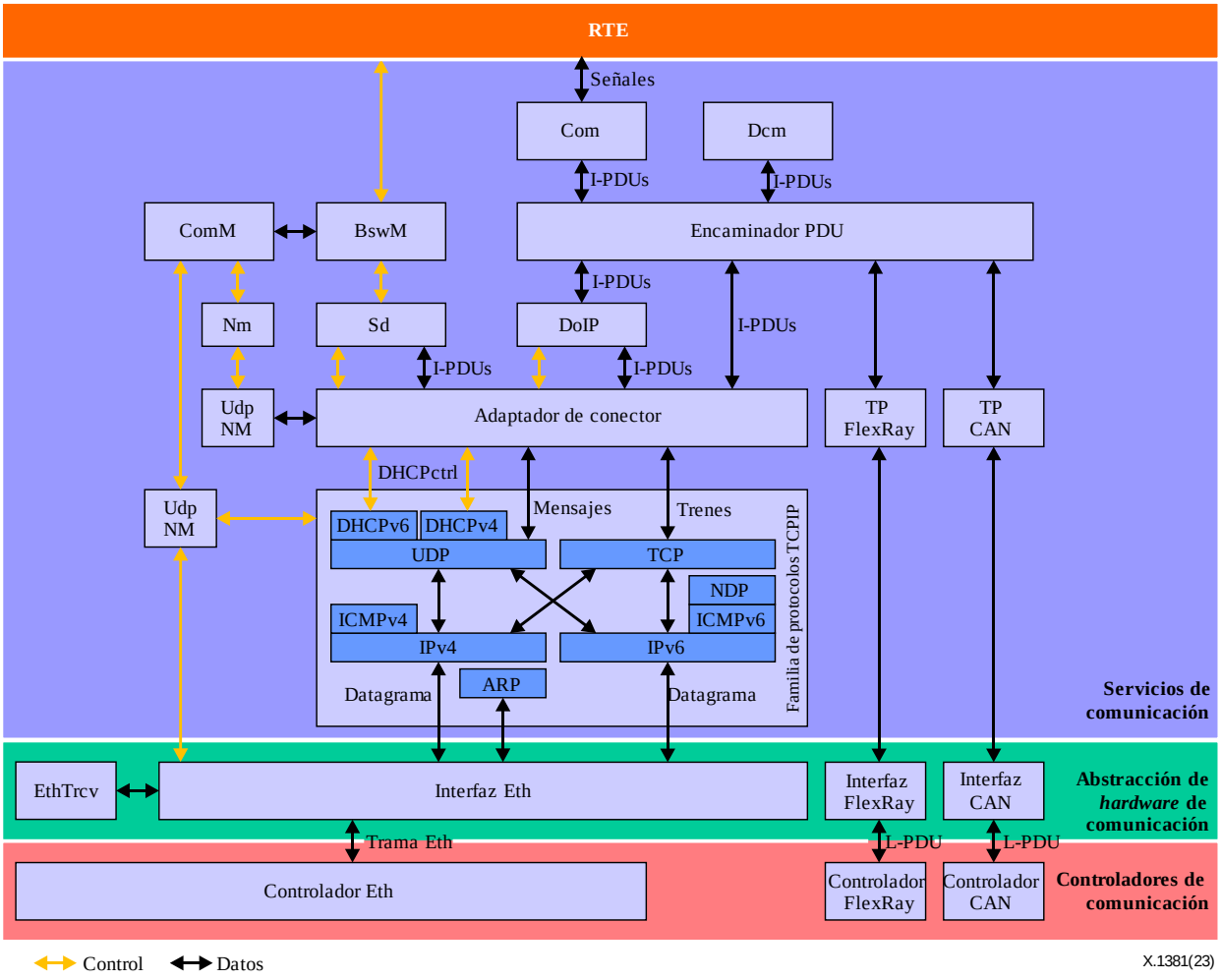

Figura I.2 – Pila de comunicación AUTOSAR ampliada (arquitectura de *software* únicamente) (Fuente: [b-AUTOSAR 617])

NOTA 2 – AUTOSAR introdujo una notación de PDU distinta de la semántica de PDU heredada utilizada en las TIC (como se especifica en [b-UIT-T X.200]). Las I-PDU, N-PDU o L-PDU internas del sistema de *software* AUTOSAR están correlacionadas o se muestran en las interfaces de comunicación de red utilizadas como PDU de capa *x*, en general (L*x*)-PDU, dependiendo de la pila de protocolo específica utilizada.

I.2.1 Comunicación a bordo segura

Los servicios criptográficos de AUTOSAR vienen prestados por el servicio de criptografía, la capa abstracta del *hardware* de seguridad y el controlador criptográfico, que se denominan colectivamente pila de criptación. El controlador criptográfico depende del microcontrolador y proporciona la interfaz para acceder al *hardware*. La capa abstracta del *hardware* de seguridad proporciona una interfaz común como programa intermedio entre el servicio de criptografía y el *hardware* de seguridad. La interfaz común proporciona independencia entre un controlador criptográfico que depende del *hardware* de seguridad y un servicio de criptografía como servicio de capa superior. El único módulo que se incluye en un servicio de criptografía es el gestor de servicios criptográficos (CSM).

La comunicación a bordo segura (SecOC) es un servicio del CSM que ofrece integridad para los mensajes de comunicación.

El objetivo de SecOC es facilitar mecanismos de autenticación que son prácticos y que hacen un uso eficaz de los recursos para el nivel de *software* (o capa de protocolo) de una PDU. Este tipo de mecanismo de autenticación utiliza un código de autenticación de mensaje basado en un algoritmo criptográfico simétrico porque es necesario minimizar el consumo de recursos que se añade a los sistemas heredados.

SecOC utiliza un CSM para generar y verificar el código de autenticación de mensaje. Un CSM puede acelerar el cálculo del código de autenticación de mensaje utilizando un HSM.

La Figura I.3 es una presentación funcional de SecOC.

Un remitente genera una PDU segura y le añade un rótulo de autenticación que contiene un código de autenticación de mensaje y el valor de antigüedad. El valor de antigüedad puede ser un valor de contador o un sello de tiempo.

Un receptor verifica el rótulo de autenticación en la PDU segura recibida, es decir, un receptor genera un código de autenticación de mensaje basado en los datos de la PDU segura recibida y lo compara con el código de autenticación de mensaje recibido.

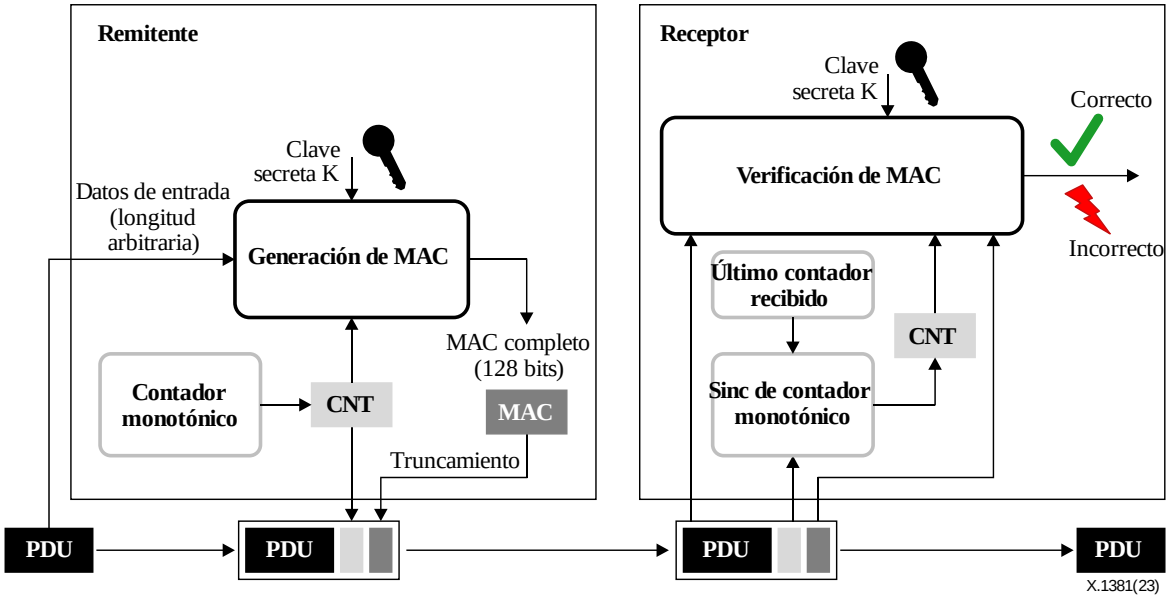

Figura I.3 – Autenticación de mensajes y verificación de antigüedad [b-Autosar 654]

I.2.2 Seguridad de la capa de transporte

TLS proporciona servicios de comunicación segura de extremo a extremo para TP fiables, como TCP.

AUTOSAR no admite las versiones de TLS anteriores a TLS 1.2.

NOTA – Véase también [b-IETF RFC 8996] sobre la desaprobación de TLS 1.0 y TLS 1.1.

Para utilizar TLS en AUTOSAR, el gestor de servicios criptográficos permite ejecutar los trabajos de criptografía y las operaciones clave utilizadas por el submódulo de TLS e IPsec. Se pueden consultar los requisitos detallados y las especificaciones en [b-AUTOSAR 617].

I.2.3 Seguridad de la capa de transporte de datagramas

Este tema se estudiará con más detalle en una edición futura de la presente Recomendación.

I.2.4 Seguridad del protocolo Internet

IPsec es básicamente el protocolo de seguridad de capa de red nativo de las redes basadas en IP y admite la autenticación y el cifrado. IPsec es opcional para IPv4, pero obligatorio para IPv6. El despliegue de IPsec en las TIC suele estar limitado, si acaso, a una zona pequeña, pero no se utiliza en redes IP de zonas grandes porque la conectividad IP de extremo a extrema es rigurosa, aunque limitada (por ejemplo, interrupciones debidas a las pasarelas de ocultación de la topología de IP o a las pasarelas de seguridad IP).

Sin embargo, las redes IP intravehiculares pertenecen más bien a la categoría de redes de área (muy) pequeña y están sujetas a una única autoridad de gestión de redes, lo que no debería impedir el uso de la IPsec, limitándola a los dominios de red IP intravehicular.

Según se indica en [b-AUTOSAR 617], el modo de túnel de IPsec no está disponible actualmente en AUTOSAR. Solo se puede utilizar el modo de transporte. Tampoco admite la IPv6 o la multidifusión. Se pueden consultar los requisitos detallados y las especificaciones en [b-AUTOSAR 970].

NOTA – En la presente edición de esta Recomendación no se proporcionan consideraciones de seguridad específicas de versión IP para el protocolo IPsec.

I.3 Comunicación de diagnóstico a través del protocolo Internet

La DoIP se utiliza con fines diagnósticos, sin medios de seguridad incorporados.

La DoIP es un TP basado en IP que está definido en [b-ISO 13400-2]. La DoIP puede transferir mensajes entre los UDS de un vehículo y el equipo de prueba externa a través de la Ethernet. La DoIP depende de los protocolos siguientes:

– DHCP;

– ICMP;

– búsqueda de dirección MAC basada en la dirección IP (IPv4: ARP, IPv6: protocolo de descubrimiento de vecino).

En el UDP, cada datagrama contiene un solo mensaje DoIP. Para los datos basados en TCP, el encabezado separa los mensajes DoIP individuales dentro del flujo de datos.

Se debería utilizar el puerto TCP 13400, de uso demostrado y registrado por la IANA (autoridad de asignación de números de Internet), para la comunicación DoIP (peticiones y respuestas de diagnóstico) entre el equipo de diagnóstico externo y la ECU del vehículo.

La DoIP no tiene en cuenta ningún mecanismo de seguridad de las comunicaciones. Los mensajes no se autentican ni encriptan de ninguna manera. Por lo tanto, al diseñar servicios DoIP, los arquitectos de seguridad deben considerar la posibilidad de utilizar diferentes capas de protocolos de seguridad.

I.4 Seguridad de control de acceso a los medios

MACsec es un protocolo de seguridad habitual [b-IEEE 802.1AE] que proporciona comunicación segura para todo el tráfico de la capa de enlace de datos. MACsec admite la seguridad extremo a extremo o por tramos en el nivel de conexión de capa 2 Ethernet (es decir, "enlaces" de extremo a extremo o enlaces locales) entre nodos de conmutador o nodos finales Ethernet. MACsec incluye autenticación y cifrado o descifrado, lo que permite identificar y prevenir la mayoría de las amenazas a la seguridad, como DoS, intrusiones, ataques de intermediario, simulaciones, escuchas pasivas y ataques por repetición.

Apéndice II

Pasarelas de vehículo con conectividad Ethernet, IP o Internet

(Este apéndice no forma parte de la presente Recomendación.)

II.1 Motivos

Una CGW, una pasarela de vehículo limítrofe o las VG en general desempeñan una función crucial en la arquitectura de la seguridad de la comunicación intravehicular, en especial en lo que respecta a los servicios de comunicación y los dominios de red basados en IP y Ethernet. La ubicación topológica de red de una CGW como pasarela de vehículo limítrofe implica y determina una función de pasarela de seguridad entre los dominios de red internos y externos del vehículo.

La especificación y normalización de estos tipos de elementos de red se asocian normalmente a consideraciones de seguridad explícitas o, incluso, a directrices y especificaciones de seguridad.

II.2 Finalidad del presente apéndice

En este apéndice se proporciona una lista no exhaustiva de normas de VG pertinentes para la seguridad que podrían resultar beneficiosas (por ejemplo, debido a la información adicional de seguridad de las comunicaciones) y que están dentro del ámbito de esta Recomendación. Este Apéndice puede ser objeto de actualización en ediciones futuras de esta Recomendación.

II.3 Recomendaciones sobre pasarelas de vehículo seleccionadas con información de seguridad

En este apartado se enumeran las Recomendaciones de interés para la seguridad, sin ningún tipo de valoración.

– [b-ITU-T F.749.1]: establece los requisitos de seguridad funcionales;

– [b-ITU-T F.749.2]: contiene apartados dedicados a los requisitos de seguridad de las comunicaciones y los requisitos de seguridad de capa superior;

– [b-ITU-T H.550]: aspectos de seguridad relacionados principalmente con la gestión de la seguridad en las VG;

– [b-ITU-T H.560]: aspectos de seguridad relacionados principalmente con la interfaz de comunicaciones de las VG utilizadas para comunicación externa.

Apéndice III

Seguridad del sistema de transporte inteligente intravehicular

(Este apéndice no forma parte de la presente Recomendación.)

III.1 Información general

El concepto de ITS incluye una arquitectura de comunicación vehicular que abarca el sistema de comunicación externo del vehículo y la interconexión con los sistemas y servicios de comunicaciones externos del vehículo. El elemento de comunicación y red más importante de la arquitectura general es la estación ITS intravehicular; véase, por ejemplo, [b-ETSI EN 302 665], [b-ETSI TR 101 607].

La estación ITS representa una red de comunicaciones intravehicular, que puede estar basada en Ethernet y que ofrece servicios de comunicación con o sin IP. Una solución técnica ITS de este tipo sería acorde con el alcance de esta Recomendación.

III.2 Redes ITS intravehiculares

Una arquitectura IVN especificada por el ITS está formada por los mismos elementos de red que se describen en la sección central de la presente Recomendación: pasarela ITS de vehículo, anfitrión ITS de vehículo, encaminador ITS de vehículo, pasarela o encaminador limítrofe ITS de vehículo, etc. En consecuencia, las directrices de seguridad del ITS también se aplican en gran medida a la presente Recomendación, especialmente cuando las tecnologías de comunicación (esto es, los protocolos y las pilas de protocolo) y la arquitectura de comunicación coinciden.

III.3 Seguridad ITS

El objetivo de esta Recomendación no es analizar la seguridad definida para el ITS. Sin embargo, el análisis de amenazas, vulnerabilidades y riesgos realizado en el marco del ITS, las directrices de seguridad ITS, los servicios de seguridad o la arquitectura de seguridad podrían constituir una lectura complementaria interesante, sobre todo en el caso de la seguridad de las comunicaciones. Véase [b-ETSI TS 102 731] para obtener más información y referencias de seguridad adicionales.

Bibliografía

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

[b-UIT-T F.749.2] Recomendación ITU-T F.749.2 (2017), *Service requirements for vehicle gateways*.

[b-UIT-T G.7710] Recomendación UIT-T G.7710/Y.1701 (2020), *Requisitos de las funciones comunes de gestión de equipos*.

[b-UIT-T G.8013] Recomendación UIT-T G.8013/Y.1731 (2015), *Funciones y mecanismos de operación, administración y mantenimiento para redes basadas en Ethernet.*

[b-UIT-T H.550] Recomendación UIT-T H.550 (2017), *Architecture and functional entities of vehicle gateway platforms*.

[b-UIT-T H.560] Recomendación UIT-T H.560 (2017), *Communications interface between external applications and a vehicle gateway platform*.

[b-UIT-T M.3010] Recomendación UIT-T M.3010 (2000), *Principios para una red de gestión de las telecomunicaciones.*

[b-UIT-T M.3702] Recomendación UIT-T M.3702 (2010), *Common management services – Notification management – Protocol neutral requirement and analysis*.

[b-UIT-T M.3703] Recomendación UIT-T M.3703 (2010), *Common management services – Alarm management – Protocol neutral requirement and analysis*.

[b-UIT-T M.3705] Recomendación UIT-T M.3705 (2013), *Common management services – Log management – Protocol neutral requirements and analysis*.

[b-UIT-T X.200] Recomendación UIT-T X.200 (1994), *Tecnología de la información – Interconexión de sistemas abiertos – Modelo de referencia básico: El modelo básico.*

[b-UIT-T X.641] Recomendación UIT-T X.641 (1997), *Tecnología de la información – Calidad de servicio: Marco*.

[b-UIT-T X.703] Recomendación UIT-T X.703 (1997), *Tecnología de la información – Arquitectura de gestión distribuida abierta.*

[b-UIT-T X.800] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT.*

[b-UIT-T X.1039] Recomendación UIT-T X.1039 (2016), *Technical security measures for implementation of ITU-T X.805 security dimensions*.

[b-UIT-T Y.1222] Recomendación UIT-T Y.1222 (2004), *Traffic control and congestion control in Ethernet-based networks.*

[b-UIT-T X.1252] Recomendación UIT-T X.1252 (2021), *Términos y definiciones sobre gestión de identidad de referencia.*

[b-UIT-T Y.1730] Recomendación UIT-T Y.1730 (2004), *Requisitos de las funciones de operación, administración y mantenimiento en redes basadas en Ethernet y en servicios Ethernet.*

[b-UIT-T Y.2770] Recomendación UIT-T Y.2770 (2012), *Requisitos para la inspección detallada de paquetes en las redes de la próxima generación.*

[b-UIT-T Y.2771] Recomendación UIT-T Y.2771 (2014), *Marco para la inspección detallada de paquetes*.

[b-Autosar 617] AUTOSAR 617 (2021), *Specification of TCP/IP stack*, AUTOSAR CP R21-11.

[b-Autosar 654] AUTOSAR 654 (2017), *Specification of secure onboard communication*, AUTOSAR CP Release 4.3.1.

[b-Autosar 970] AUTOSAR 970 (2019), *Requirements on IPsec Protocol*, AUTOSAR FO R19-11.

[b-ETSI EN 302 665] Norma europea ETSI EN 302 665 V1.1.1 (2010), *Intelligent Transport Systems (ITS); Communications architecture*.

[b-ETSI TR 101 607] Informe técnico ETSI TR 101 607 V1.2.1 (2020), *Intelligent transport systems (ITS); Cooperative ITS (C-ITS); Release 1*.

[b-ETSI TS 102 731] Especificación técnica ETSI TS 102 731 V1.1.1 (2010), *Intelligent Transport Systems (ITS); Security; Security services and architecture*.

[b-IEEE 802.1] IEEE 802.1 (Internet). *Welcome to the IEEE 802.1 Working Group*. Disponible [último acceso: 30/06/2022]: https://1.ieee802.org/

[b-IEEE 802.1AE] IEEE 802.1AE-2018, *IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) security*.

[b-IEEE 802.1AS] IEEE 802.1AS (Internet), *Standard for Local and metropolitan area networks – Timing and synchronization for time-sensitive applications in bridged local area networks.* Disponible [último acceso: 30/06/2022]: https://www.ieee802.org/1/pages/802.1as.html

[b-IEEE 802.1CB] IEEE 802.1CB-2017, *IEEE Standard for local and metropolitan area networks – Frame replication and elimination for reliability*.

[b-IEEE 802.1Q] IEEE 802.1Q-2018, *IEEE Standard for local and metropolitan area network – Bridges and bridged networks*.

[b-IEEE 802.1Qat] IEEE 802.1Qat (Internet), *Standard for Local and metropolitan area networks – Virtual bridged local area networks – Amendment 9: Stream Reservation Protocol (SRP).* Dis ponible [último acceso: 30/06/2022]: https://www.ieee802.org/1/pages/802.1at.html

[b-IEEE 802.1Qav] IEEE 802.1Qav-2009, *IEEE Standard for Local and metropolitan area networks – Virtual bridged local area networks – Amendment 12: Forwarding and queuing enhancements for time-sensitive streams*.

[b-IEEE 1722-2016] IEEE 1722-2016, *Standard for a Transport Protocol for Time-Sensitive Applications in Bridged Local Area Networks*.

[b-IETF RFC 2827] IETF RFC 2827 (1997), *Network ingress filtering: Defeating IP source address spoofing denial of service attacks*.

[b-IETF RFC 4953] IETF RFC 4953 (2007), *Defending TCP against spoofing attacks.*

[b-IETF RFC 6020] IETF RFC 6020 (2010), *YANG – A data modeling language for the network configuration protocol (NETCONF)*.

[b-IETF RFC 6575] IETF RFC 6575 (2012), *Address resolution protocol (ARP) mediation for IP interworking of layer 2 VPNs*.

[b-IETF RFC 6959] IETF RFC 6959 (2013), *Source address validation improvement (SAVI) threat scope.*

[b-IETF RFC 8996] IETF RFC 8996 (2021), *Deprecating TLS 1.0 and TLS 1.1*.

[b-ISO 13400-2] Norma internacional ISO 13400-2:2019, *Road vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 2: Transport protocol and network layer services*.

[b-ISO 14229-5] Norma internacional ISO 14229-5:2022, *Road vehicles – Unified diagnostic services (UDS) – Part 5: Unified diagnostic services on Internet Protocol implementation (UDSonIP)*.

[b-ISO/SAE 21434] Norma internacional ISO/SAE 21434:2021, *Road vehicles – Cybersecurity engineering*.

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

Publicado en Suiza
Ginebra, 2023