ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1381 (03/2023)

SERIES X: Data networks, open system communications and security

Secure applications and services (2) – Intelligent transportation system (ITS) security

---

Security guidelines for Ethernet-based in-vehicle networks

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security (1)	X.1140–X.1149
Application Security (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1350–X.1369
Intelligent transportation system (ITS) security	**X.1370–X.1399**
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
Cyber Defence	X.1590–X.1599
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1381

Security guidelines for Ethernet-based in-vehicle networks

Summary

Recommendation ITU-T X.1381 provides security guidelines for Ethernet-based in-vehicle networks (IVNs). The current trend in electrical and electronic (E/E) architecture is to integrate the Ethernet with legacy IVNs such as the controller area network (CAN), local interconnect network (LIN), media-oriented systems transport (MOST) and FlexRay. In the past, the Ethernet was considered only as a connection between vehicles with external environments. Standard protocols that enable Internet protocol-based connections over the Ethernet (e.g., diagnostic communication over Internet protocol or universal measurement and calibration protocol) have been used to enable communications between the external environment and vehicles. These use cases generally do not need to meet stringent real-time constraints. However, in-vehicle applications using Ethernet communication require characteristics that include high time sensitivity and reliability.

Current developments in in-vehicle communication technologies require increased bandwidth in the network. Compared to the Ethernet, legacy IVNs are insufficient to meet the bandwidth requirements of current in-vehicle applications. Therefore, now and in the future, Ethernet-based IVNs are a major part of E/E architecture.

However, countermeasures known from common computer networks cannot be suitable for an automotive application because they were not designed with regard to automotive requirements and capabilities.

To address this demand, this Recommendation provides security guidelines for automotive Ethernet technology. This Recommendation includes a reference model of automotive Ethernet and analysis of threat and vulnerability for Ethernet-based IVNs. In addition, this Recommendation provides security requirements and use cases of Ethernet-based IVNs.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1381	2023-03-03	17	11.1002/1000/15107

Keywords

Automotive ethernet security, ITS security.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

		Page
1	Scope	1
1.1	Applicability statements	1
1.2	Validation of security guidelines over the timeline	1
2	References	1
3	Definitions	2
3.1	Terms defined elsewhere	2
3.2	Terms defined in this Recommendation	3
4	Abbreviations and acronyms	3
5	Conventions	5
6	Overview of automotive Ethernet-based and evolving in-vehicle architectures	5
6.1	Electrical and electronic computing and network architecture in a vehicle	6
6.2	Comparison of future and current electrical and electronic architecture security	7
6.3	Communication services using the Ethernet in automotive applications	9
7	Analysis of threats	11
7.1	Approach methodology for analysis of threats	11
7.2	Security assets	11
7.3	Security objectives	12
7.4	Identified threats	13
8	Security requirements	16
8.1	Confidentiality	16
8.2	Integrity	17
8.3	Availability	17
8.4	Authenticity	17
9	Implementation of Ethernet-based in-vehicle networks with security	18
9.1	Implementation related considerations in advance	18
9.2	Automotive Ethernet associated security gateway functions	19
9.3	Secure VLAN configuration	19
9.4	Security for Ethernet switches in automotive context	20
Appendix I – Description of some Ethernet-based in-vehicle network protocols with communication endpoints located in AUTOSAR or non-AUTOSAR compute nodes		22
I.1	Overview and scope	22
I.2	AUTOSAR secure onboard communication inclusive lower protocol layer security protocols	22
I.3	Diagnostic communication over Internet protocol	25
I.4	Media access control security	25
Appendix II – Vehicle gateways with Ethernet, IP or Internet connectivity		26

Page

II.1 Motivation 26
II.2 Purpose of this appendix 26
II.3 Selected vehicle gateway Recommendations with security information 26
Appendix III – Intra-vehicle intelligent transport system security 27
III.1 Background 27
III.2 ITS in-vehicle networks 27
III.3 ITS security 27
Bibliography 28

Recommendation ITU-T X.1381

Security guidelines for Ethernet-based in-vehicle networks

1 Scope

This Recommendation provides security guidelines for Ethernet-based in-vehicle networks (IVNs). It covers:

1) security threat analysis;

2) security requirements; and

3) use cases,

from a cyber-security perspective. Cybersecurity indicates that the technical communication architecture concerned is or can be an integral part of cyber-physical systems (e.g., Ethernet communication protocol stacks integrated in embedded systems).

1.1 Applicability statements

Networks in general and those on the Ethernet in particular are used for communication services. The security context in this Recommendation consequently focuses on communication security, but not necessarily on information security as such for compute nodes with Ethernet connectivity.

The security guidelines in this Recommendation therefore cover network engineering of Ethernet-based networks as used in automotive applications, from the security engineering perspective. Thus, the associated layered communication architectures with their layered protocol stacks are a fundamental part of such security considerations.

1.2 Validation of security guidelines over the timeline

Security for communication architectures as required for in-vehicle Ethernet networks is fundamentally evolving, primarily due to

1) possible changes in network topologies (driven by the evolving distributed computing architectures, using that communication networks, e.g., in direction of vehicle automation);

2) layered protocol architectures: current Ethernet and non-Ethernet protocol stacks in use can change, get extensions, etc.;

3) protocol evolution: current information and communication technology (ICT) protocols (as owned by standards development organizations like IEEE, IETF, ITU-T, ETSI, 3GPP) in use are still subject to ongoing maintenance activities and extensions, reflected by protocol profiling (e.g., IEEE time-sensitive networking (TSN) for automotive applications) [b-IEEE 1722-2016] or protocol versioning;

NOTE – Further, protocol specification-associated security considerations may be also subject to update.

1) evolution of security means and solutions in the context of communication security.

Future revisions of this Recommendation are therefore expected.

This Recommendation focuses in particular on initial security guidelines, given by a first set of use cases. The primary scope is first generation(s) Ethernet-based IVNs, leading to best current security practices and security guidelines at the time of publication of this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the

editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1371] Recommendation ITU-T X.1371 (2020), *Security Threats to Connected Vehicles*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 accountability [b-ITU-T X.800]: The property that ensures that the actions of an entity may be traced uniquely to the entity.

3.1.2 authentication [b-ITU-T X.1252]: Formalized process of verification that, if successful, results in an authenticated identity for an entity.

NOTE – Use of the term authentication in an identity management context is taken to mean entity authentication.

3.1.3 authenticity [b-ITU-T X.641]: Protection for mutual authentication and data origin authentication.

3.1.4 authorization [b-ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.5 availability [b-ITU-T X.800]: The property of being accessible and useable upon demand by an authorized entity.

3.1.6 confidentiality [b-ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.7 data integrity [b-ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.8 firewall [b-ITU-T X.1039]: Type of security barrier placed between network environments – consisting of a dedicated device or a composite of several components and techniques – through which all traffic from one network environment traverses to another, and vice versa, and only authorized traffic, as defined by the local security policy, is allowed to pass.

3.1.9 security gateway [b-ITU-T X.1039]: Point of connection between networks, or between subgroups within networks, or between software applications within different security domains intended to protect a network according to a given security policy.

3.1.10 vehicle gateway (VG) [b-ITU-T F.749.1]: A VG is a device in a vehicle that enables communications between a device in the vehicle and another device which may be physically located either inside the vehicle or outside the vehicle (e.g., roadside station, cloud-based server, etc.). A VG provides standardized interfaces and protocols, communications across heterogeneous networks, optimized network selection based on application needs and network QoS, arbitration and integration of network communications, security and switching network connections to maintain service continuity.

NOTE 1 – The term central gateway (as introduced in this Recommendation) is typically synonymous with vehicle gateway in abstracted in-vehicle networks (IVNs), or vehicle border gateways in more detailed IVN architectures.

NOTE 2 – The term vehicle intelligent transport system (ITS) gateway is basically synonymous with vehicle gateway.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 electrical and electronic architecture (E/E architecture): A coupled, two-plane vehicular architecture, consisting of: 1) an electrical energy or power distribution network plane; and 2) an information processing and communication network architectural plane.

NOTE – A third tag is sometimes added to E/E to indicate the vehicular propulsion technology, i.e., E^3;the third E indicates an electric vehicle.

3.2.2 vehicle border gateway: A vehicle gateway positioned at the border of and in vehicle internal network domain(s) and vehicle external network domain(s). Consequently, all vehicle-to-everything (V2X) communication traffic is routed via such a vehicle gateway type.

NOTE 1 – The term vehicle gateway also covers this meaning, and might therefore be sufficient for in-vehicle network (IVN) architectures with only a single vehicle gateway deployed. However, IVNs can also use vehicle gateways for internal interconnection and interworking purposes only. Such network contexts can lead to the need to differentiate between gateway types in a more detailed manner.

NOTE 2 – The specific interworking functions as supported by a particular *gateway* type are often expressed by an extended gateway name, indicating, for example, the location in a network hierarchy (such as access or core network level), the border or interconnection type of inter-networking (such as security domains), specific network interfaces or communication technologies.

NOTE 3 – A communication control unit is understood as a technical component that belongs to the category of vehicle border gateway (functions).

NOTE 4 – V2X communication covers all traffic types, e.g., that from telematic, ITS or diagnostic services.

3.2.3 zone-oriented electrical and electronic architecture: An electrical and electronic (E/E) architecture grouping in-vehicle components (Note 1) such as sensors, actuators and compute nodes, by their location (Note 2) in network subdomains. Each subdomain, a so-called zone (Note 3), has a distinguished zone-related vehicle compute node (known as a zone controller in automotive applications), connected to all intra-subdomains in-vehicle components. Zone controllers of each zone again are interconnected with a superior high-performance in-vehicle compute node. Thus, there is a resulting processing hierarchy between zones and the overall in-vehicle network (IVN) domain, from the perspective of distributed computing architecture.

NOTE 1 – Scoping on the computing and networking components in context of IVNs.

NOTE 2 – "Location" is understood as the network location at the physical or virtual IVN topological level.

NOTE 3 – The notion of zone here is primarily related to the concept of network domains in the context of E/E architectures. Such a zone does not necessarily include the concept of security zone, trusted zone or demilitarized zone as used in other security-related ITU-T Recommendations (like e.g., [b-ITU-T Y.2770]).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ADAS	Advanced Driver Assistance System
ARP	Address Resolution Protocol
AUTOSAR	Automotive Open System Architecture
AVB	Audio Video Bridging
CAN	Controller Area Network
CGW	Central Gateway
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check

DHCP	Dynamic Host Configuration Protocol
DoIP	Diagnostic communication over Internet Protocol
DoS	Denial of Service
DTLS	Datagram Transport Layer Security
ECU	Electronic Control Unit
E/E	Electrical and Electronic
FDB	Forwarding Database
FIB	Forwarding Information Base
HSM	Hardware Security Module
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technology
ID	Identifier
IDS	Intrusion Detection System
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITS	Intelligent Transport System
IVN	In-Vehicle Network
LIN	Local Interconnect Network
MAC	Media Access Control
MACsec	Media Access Control security
MCU	Microcontroller Unit
MOST	Media Oriented Systems Transport
MPU	Multipoint Control Unit
OBD	On-Board Diagnostic
OEM	Original Equipment Manufacturer
PDU	Protocol Data Unit
PVID	Port VLAN ID
QoS	Quality of Service
SecOC	Secure Onboard Communication
SR	Security Recommendation
TARA	Threat Analysis and Risk Assessment
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TP	Transport Protocol
TSN	Time-Sensitive Networking

UDP	User Datagram Protocol
UDS	Unified Diagnostic Service
V2X	Vehicle to Everything
VG	Vehicle Gateway
VID	VLAN Identifier
VLAN	Virtual Local Area Network

5 Conventions

This Recommendation provides a list of security requirements, labelled [SR-*x*], where *x* is a number. Such SRs use the following phrases with meanings prescribed as follows.

The phrase "**is recommended**" or "should" indicate a requirement that is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformity.

The phrase "**can optionally**" indicates an optional requirement that is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can optionally be enabled by the network operator or service provider. Rather, it means the vendor may optionally provide the feature and still claim conformity to this Recommendation.

6 Overview of automotive Ethernet-based and evolving in-vehicle architectures

The automotive Ethernet is a physical network that is used to connect components within a vehicle using a wired network. The automotive Ethernet is also used as the name for the entire in-vehicle Ethernet network as such, comprising all protocol layers and protocols used in that network domain. It is designed to meet the needs of the automotive market, including meeting electrical requirements (electromagnetic interference/radio frequency interference emissions and susceptibility), bandwidth requirements, latency requirements, synchronization and network management requirements. As an autonomous vehicle and advanced driver assistance system (ADAS) technologies are getting a lot of attention, modern vehicles are usually equipped with multiple cameras, on-board diagnostics (OBDs) and infotainment systems that require high bandwidth. In addition, as the number of functions increases, the number of interconnected computing nodes (such as electronic control units (ECUs)) in a vehicle increases. It leads to an increase in the wiring harness and the mass of the vehicle, which degrade its performance and fuel efficiency. The zone-oriented E/E architecture is a prominent example of a particular in-vehicle computing and network architecture, where Ethernet is also used at the top network hierarchy level, used for the interconnection of all zones (a so-called backbone network) in the entire architecture. When a legacy IVN, including a controller area network (CAN), local interconnect network (LIN), media-oriented systems transport (MOST) or FlexRay, is integrated with the Ethernet, standardized Ethernet cables can be used to significantly reduce mass and reduce costs. In addition, because of the high bandwidth, the number of control systems can be reduced, as well as the complexity.

However, not every IVN domain, such as powertrain, body and chassis, will change to the automotive Ethernet. It means that domains, for example, a body that needs a low quantity of data and bandwidth does not need to change networking protocols with additional resources and efforts.

Figure 1 shows a mixed IVN with legacy IVN protocols, such as CAN, and the automotive Ethernet. Communications requiring low bandwidth can still use legacy IVN protocols, while communications requiring high bandwidth, such as autonomous or ADAS functions, can be changed to an Ethernet-based IVN.

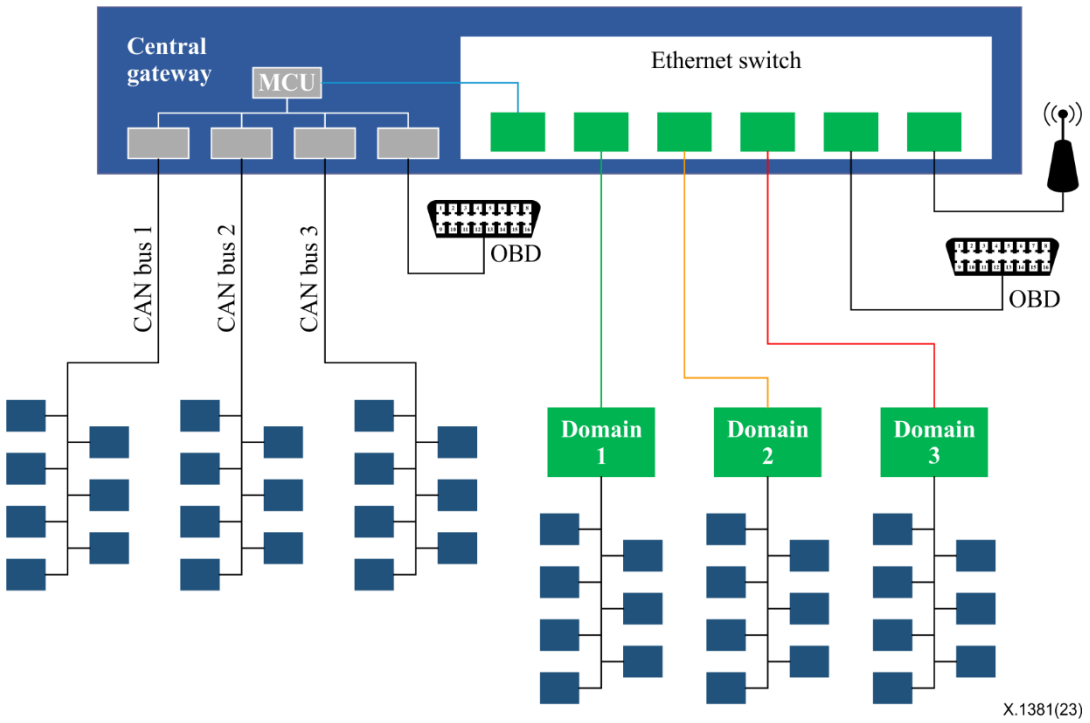

Figure 1 – The current heterogeneity of a typical in-vehicle network, based on legacy protocols and the automotive Ethernet

It is recognized that there is an expected evolution of Ethernet-based IVNs over the timeline. Such network evolutions are accompanied typically by communication architecture (given by communication topologies, layered protocol stacks, etc.) changes, which again will most likely impact associated communication security architectures.

Security concepts for classical E/E architectures, i.e., based on CAN/FlexRay/LIN and sometimes MOST, have been already discussed in the past and some proposed mechanisms have already made their way to standardization. The Ethernet and its related upper-layer protocols will not only be a simple, but also a faster replacement of legacy automotive bus systems; as well as likely changing fundamental concepts of current E/E architectures.

The introduction of the Ethernet is a huge chance to improve in-vehicle security because many demanding security issues in automotive applications have been already addressed for Ethernet, e.g., in so-called carrier-grade ICT business (e.g., Ethernet-based metropolitan area networks, Ethernet-based terrestrial radio access networks), but also classical information technology business (i.e., the Ethernet as baseline connectivity in private, enterprise local area networks). However, it also yields huge challenges, including those due to the constraints of automotive or embedded systems, to ensure at least the same security as currently expected for existing security-enhanced E/E architectures.

6.1 Electrical and electronic computing and network architecture in a vehicle

Former E/E architectures consider a central gateway (CGW; also known as a VG or vehicle ITS gateway in that type of IVN) for in-vehicle communication and interconnection between different subdomains. There are thus end-to-end connections, which are routed across such VGs.

NOTE 1 – "Routed" in this context is the generic traffic routing function, not other routing such as that for the IP. Current Ethernet-based IVNs do not use IP router entities, only IP-type gateways. Such a usage of IP and the Ethernet leads to something like a switched IP network (for IP-based communication services).

This aspect is crucial from the communication security perspective because it reduces IP-related security objectives (e.g., there will be no security threats due to IP routing protocols).

The targeted Ethernet-based communication is expected to meet the requirement of high real-time performance and reliable communication, and to benefit from a mature, widely used, and proven communication technology and technique.

NOTE 2 – [b-IEEE 802.1], especially [b-IEEE 802.1CB], allows reliable communication, which includes a ring architecture including a layer 2 redundancy feature (R-Tag).

In particular, CAN, FlexRay, LIN and MOST are natively used for in-vehicle communication; CAN is the most popular. A CGW, VGs in general and a vehicle border gateway in particular as such are crucial network and security elements in intra-vehicle networks and communication architectures. Appendices II and III provide some complementary information which might be beneficial from the communication security perspective.

In the past, it was not possible to access a vehicle remotely (e.g., using workshop connectivity for diagnosis purposes or the variety of all kinds of V2X communication options). In-vehicle ECUs were connected to each other via one or more of the native, automotive optimized field buses.

Legal access after production was only possible by direct and cable-based physical connectivity. Thus, point-to-point connection over a short distance is used exclusively for diagnostic services that require a connection to the OBD port via the CAN protocol. Original equipment manufacturers (OEMs) were aware of the enhanced security risk of the diagnostic functionality and the native CAN protocol that does not provide any security functionality. [b-Autosar 654] has focused on the authenticity and integrity of CAN messages and suitable security concepts mainly use message authentication codes.

Current developments enable Ethernet-based communication from external devices to the vehicle. Usually, a dedicated ECU within the vehicle serves as an access point for some type of external communication. If required, the ECU routes relevant information to other ECUs via common automotive networks or forwards the traffic via an Ethernet-based connection to a CGW for routing to other, commonly attached ECUs.

6.2 Comparison of future and current electrical and electronic architecture security

Due to a number of different misuse cases involving in-vehicle components, there are established security mechanisms for current E/E architectures. Regarding communication systems, authentication mechanisms for the predominant CAN network have been published, standardized and will be partially applied within future vehicle generations. Automotive open system architecture (AUTOSAR) specifies a secure on-board communication module that focuses on the authenticity and integrity of in-vehicle communication. Please note that an authentication mechanism not only refers to the authenticity of transmitted messages. but also ensures the authenticity of the communication partners.

Moreover, CAN as a physical layer bus technology transmits messages only as broadcast.

NOTE 1 – The fundamental nature of a shared physical media communication like a bus topology is, therefore, contrary to the approach of a switched Ethernet network design.

Therefore each participant is able to read all traffic transmitted via the CAN bus. Different bus-based network domains as well as further subdomains separate traffic that is safety related from other types, e.g., infotainment or comfort. Communication between network domains is only possible via a CGW that usually implements policy rule enforcement (such as filter-related rules) mechanisms to prevent flooding attacks and to ensure availability of the network.

NOTE 2 – Vehicle gateways (like the CGW) provide a set of network functions, where a particular subset is related to communication security. There are consequently not only security, but also non-security, specific policy rules enforced (e.g., for VLAN interworking, IP forwarding or setting TSN-driven QoS actions).

The Ethernet is an established standard for network communication with a wide range of applications. It is used for common machine-type communication (e.g., computer) networks, covering multiple scales of area network (e.g., small, local, metropolitan) as well as terrestrial radio access networks for

mobile communication. Given that history and network background, there might be network security patterns for reuse.

Due to its prevalent usage, there are several attacks on Ethernet-based communication (inclusive the upper layer protocols) but countermeasures exist for different use cases. For example, within the Internet, for transport services based on the transmission control protocol (TCP) (only), the usage of transport layer security (TLS) is strongly recommended to ensure the authenticity, integrity and confidentiality of the communication. It is also recommended to use the complimentary transport security protocol datagram transport layer security (DTLS) for transport services based on the user datagram protocol (UDP). The usage of the Ethernet as the established and prevalent standard for in-vehicle communication can re-use the Internet protocol (IP) stack-associated security mechanisms. However, countermeasures known from common computer networks cannot be suitable for an automotive application because they were not designed specifically for its requirements and capabilities. For example, they may not provide real-time assurances and require enhanced performance that cannot be provided by resource constraint-embedded devices. Therefore, there is no consideration of the integration of security mechanisms for time-sensitive Ethernet-based communication protocols at the time of publication.

The separation of in-vehicle communication is crucial for safety reasons. At the moment, OEMs consider the logical isolation of Ethernet traffic using network virtualization, which relates to a virtual local area network (VLAN) as a layer 2 virtual private network in the case of the Ethernet. Note that in-vehicle traffic separation can also be achieved by other means, such as VPNs of layer 1 (by physically separate Ethernet networks) or layer 3 (using a known VPN solution for IP-over-Ethernet communication services).

A VLAN is a well-established practice for providing logical isolation on the data link layer in common computer networks. VLANs are commonly used to separate physical networks into different logical networks. The in-vehicle application of VLAN is mainly based on the fact that VLAN enables traffic prioritization (e.g., by mapping VLAN priority code points directly to TSN traffic classes).

NOTE 3 – Security considerations of hierarchical VLANs, which might be in the scope of future IVNs for specific V2X interconnection models, lie outside the scope of this edition of this Recommendation. Thus, there is a hypothesis here of single-tagged or port-based VLANs only.

The application of the widespread Ethernet standard for in-vehicle communication offers some possibilities on one hand; however, special care needs to be taken on the other. In addition to the lack of a security mechanism application, no special equipment is recommended to connect an external device via the Ethernet to the vehicle.

Even users can be interested in trying to plug-in their laptops or using their smartphones to enhance access to IVNs. Using an Ethernet switch as an additional component can allow a specially trained unauthorized person to have an interesting attack vector. The attackers can execute known attacks from the Internet or published exploits for common Ethernet switches. Similar to communication security, countermeasures for common Ethernet switches exist. However, further exploration and investigation of automotive environments are required.

Table 1 shows differences between legacy, fieldbus-oriented IVN protocols and those based on the Ethernet at a very abstract level. The first column of each comparison target is the maturity of respective criteria, which is represented by its symbol such as bad (−), neutral (0), good (+), best (++). Note that Table 1 is intentionally a simplification; a more serious protocol evaluation would require a comparison of Ethernet against each individual fieldbus or vehicle bus communication technology.

Table 1 – Comparison of legacy and Ethernet-based communication architectures in a vehicle

Criteria	Fieldbus-oriented IVN protocols (Note 1)		Ethernet-based IVN	
Simplicity	–	Complex, heterogeneous, multi-protocol gateway	++	Very homogenous with (mostly) layer 2 switches
Flexibility	–	Difficult to extend/adapt new subnet (within subnets easy)	++	Easy to extend/adapt new or within subnets
Performance	+	Depends on the bus type	++	Up to several gigabits per second
Real-time	++	Well proven over decades	–	Capable but not invented for
Mass of network-related physical material	–	Individual wiring per bus	+	One twisted pair for all
Costs (investment, not operation)	–	Small-batch automotive-specific production	+	Global mass production also for non-automotive
Degree of standardization	–	Standard with large diversity	+	Standard with little diversity
Connectivity models at physical and data link layer (NOTE 2)	–	Only point-to-multipoint communication models due to shared physical media usage ("bus")	+	Ethernet supports both communication models, point-to-point and point-to-multipoint (NOTE 3).
Message integrity (NOTE 4)	+	Cyclic redundancy check (CRC) + bus specific measures	+	CRC, block codes
Security measures (NOTE 5)	–	Virtually none	0	Add-ons (Internet protocol version 4 (IPv4)), Internet protocol security (IPsec) (Internet protocol version 6 (IPv6))

NOTE 1 – Evaluations against the listed criteria reflect typical protocol design, but are not valid for every case of fieldbus-oriented communication technologies, e.g., CAN does not provide inherent protocol means to support real-time communication.

NOTE 2 – Assumption here: in-vehicle applications typically require communication services with communication topologies of the types point-to-point or point-to-multipoint. Such topologies have to be served by logical connection topologies, which implies here the consideration of link layer connection topologies as the common denominator "protocol layer" of the communication technologies discussed.

NOTE 3 – In-vehicle Ethernet networks will be deployed and operated in "switched mode" only (primarily driven by quality of service (QoS) objectives), which implies support of point-to-point connection models only at the Ethernet physical media layer. The physical media is not shared, rather each Ethernet layer 1 endpoint has exclusive access to the physical layer resources. However, point-to-multipoint communication topologies are also supported: either directly by the native Ethernet embedded multi- and broadcast capability by the data link layer forwarding functions or indirectly by upper layer protocols (such as the IP and its multi-, any- or broadcast type of network address).

NOTE 4 – The security relevant integrity covers here both: a) bit integrity; b) data integrity, i.e., either an integrity scope on individual bits of a protocol data unit (PDU) or the entire PDU as such (at specific protocol layers).

NOTE 5 – The security measures are evaluated whether the respective protocol specification has inherent security features or not.

The comparison criteria outlined cover basic network engineering and communication service engineering as well as security-specific aspects.

6.3 Communication services using the Ethernet in automotive applications

These days, the automotive Ethernet is mainly used in diagnostics and transmission of the multimedia stream such as video data from camera sensors for the ADAS. Furthermore, it started in the mid-2010s to allow compute nodes (like ECUs) in vehicles to communicate over the Ethernet.

6.3.1 Diagnostics

The conventional diagnostic method on a vehicle is to connect a diagnostic tool to an OBD-II Port and communicate with the target ECU via a unified diagnostic service (UDS) protocol. UDS is an automotive industry-elaborated application level protocol that lets diagnostic systems communicate with the ECUs to diagnose faults and reprogram the ECUs accordingly (see [b-ISO 14229-5]).

The diagnostic communication over Internet protocol (DoIP) is based on the IP (see [b-ISO 13400-2]). The DoIP enables the transmission of UDS messages between a vehicle and external test equipment over the Ethernet and it becomes possible to retrieve diagnostic data from a vehicle remotely, without requiring physical connectivity to the vehicle. The DoIP provides an encapsulation of UDS messages within TCP packets or UDP datagrams as shown in Figure 2.

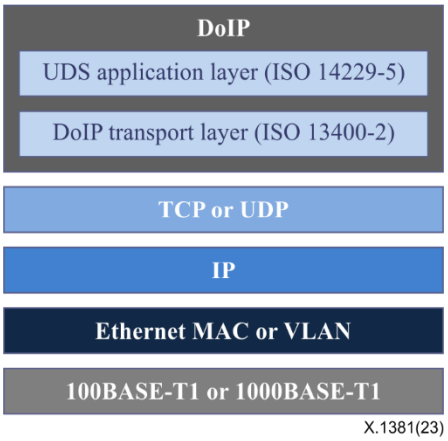

Figure 2 – Protocol stack for the diagnostic communication over Internet protocol application

The DoIP itself does not consider any mechanisms for communication security. Messages are generally not authenticated or encrypted in any way. The DoIP considers an authentication in the upper layer(s) but this is not mandatory.

6.3.2 Media streams in context of multimedia services

For the ADAS, highly automated and fully autonomous vehicles have to deploy a lot of sensors like high-definition cameras and connectivity functions to get sufficient information in order to perceive the vehicle environment. In addition, many vehicles are equipped with devices that use or transmit streams of application-level media (not to be mixed with physical media (sub-)layers in the case of the Ethernet) that are used in infotainment systems, around view monitoring systems, parking assistance systems, line keeping assistance systems, night vision and so on. In the case of cameras, relatively large media streams (in terms of traffic volume) are generated with application-driven QoS objectives of low-latency and high-quality transmission. If the protocol is CAN, the preceding requirements are impossible to achieve due to protocol design inherent limitations, e.g., payload size range.

The automotive Ethernet can meet these requirements using the IEEE audio video bridging (AVB) framework.

NOTE – The term AVB denotes a set of [b-IEEE 802.1] standards, including [b-IEEE 802.1Qav], [b-IEEE 802.1AS] and [b-IEEE 802.1Qat]. Therefore in 2012, the IEEE AVB task group changed the name to TSN Task Group, which now includes the AVB standards.

AVB can satisfy more generalized TSN requirements, opening up the possibility of a single network that handles infotainment, body control, driver assistance and even safety-critical functions.

In the case of an around view monitoring system, an array of cameras provide a synchronized 360° surround view of the vehicle environment. This video-type media stream can be sent to the driver

awareness system such as head-up display system or video navigation system. It can also be synchronized additional sensor data and related ECUs via the AVB network

6.3.3 Backbone of in-vehicle network

Modern vehicles could have more than 100 ECUs. An ECU or vehicle compute node relates to a network node in the Ethernet IVN topology, with one or multiple endnodes (dependent on the number of physical, logical or virtual Ethernet connection interfaces per compute node). Moreover, the number of ECUs could still increase. Further the ADAS and autonomous vehicles start to demand a large IVN transport capacity (colloquially called bandwidth) of the IVN.

In addition, legacy IVN protocols use the wiring harness system, which is heavy and a significant cost factor. If the Ethernet is used as a backbone of the IVN, up to 80% in-vehicle connection costs and 30% in-vehicle wiring mass can be reduced.

As shown in Figure 1, there are several domains in the Ethernet-based IVN. Legacy IVN protocols are used within each domain and the Ethernet is used for inter-domain communication, i.e., at the core network level (when comparing it with ICT networks), colloquially also termed a backbone network.

The automotive Ethernet is different from the topology of a bus system. There is no bus conductor that is connected to numerous ECUs, sensors and actuators. Instead, they are connected with an Ethernet switch in a point-to-point manner. If communication messages have to send from one domain to another, it can be easily handled by network interworking functions, such as those provided by Ethernet switches, VLAN gateways, possibly also IP routers and IP gateway in the Ethernet-based IVN. In contrast, legacy in-vehicle fieldbus protocols require network and possibly also service interwork support, typically located in gateways, when communicating with Ethernet network-located endpoints.

7 Analysis of threats

7.1 Approach methodology for analysis of threats

This clause analyses of security threat scenarios in the context of in-vehicle Ethernet networks. Overall identified threats in connected vehicles are described in [ITU-T X.1371].

To derive the security concept, security goals should be developed. A threat analysis and risk assessment (TARA) is performed to determine the treatment method for the risk at the security goal phase. In order to perform a TARA, security assets and security objectives should be identified, as well as related threats. The security concept can be determined if the treatment method for respective risks is decided through impact rating and attack feasibility rating based on identified security assets, security objectives and threats, see [b-ISO/SAE 21434] for more information. According to the threat analysis approach of [b-ISO/SAE 21434], security assets and related security objectives are identified, and then security threats are also identified in this clause.

The process of impact rating, attack feasibility rating and risk decision lie outside the scope of this Recommendation and are for further study.

7.2 Security assets

A security asset means any data object, function, or resource that should be protected. From a consideration of Ethernet-based IVNs, the extracted security assets are listed in Table 2.

Table 2 – Security assets

Asset	Description
Management data	Management data covers the two categories (Note 1) of: configuration data, that characterizes the functional behaviour of network elements or network functions with Ethernet connectivity, such as a gateway, Ethernet switch, intrusion detection system (IDS), and firewall; operational state data, describing not only the actual behaviour of those network entities, but also all management services using notifications [b-ITU-T M.3702] such as alarm reporting [b-ITU-T M.3703] as part of fault management. The management data flows for both categories between the managing and managed entity are basically subject to security protection. However, the security impact, e.g., by manipulating configuration data, should usually be much higher than on operational state data. On the other side, e.g., the intended suppression of an alarm, issued by an Ethernet network element, might worsen the current faulty situation
Ethernet communication related layer 2 protocol data units	Ethernet traffic is constituted by the data link layer traffic, i.e., the Ethernet media access control (MAC) frames (as layer 2 PDUs) being transferred to the Ethernet-based automotive IVN
Management data generated by logging (Note 2)	The successful detection of, and associated information on, security events can be audited
Cryptographic material	Keys and certificates for symmetric and asymmetric schemes, including other credentials, such as password
Firmware or software image	The compiled code to be run on vehicle computing nodes such as ECUs
NOTE 1 – See the Ethernet applicable network management framework, e.g., as described in [b-ITU-T M.3010, b-ITU-T X.703, b-ITU-T G.8013, b-ITU-T Y.1730]. Management data for Ethernet network entities is based on YANG [b-IETF RFC 6020] as specification and management data modelling language. The IEEE 802 (as technology owner of the Ethernet) provides YANG-based management data models for all the various Ethernet entities, i.e., the main management data reference for this Recommendation. NOTE 2 – The management of logging functions [b-ITU-T M.3705] is not covered by this table. Logging concerns here the system event caused by management information flows that are recorded by logging functions (see [b-ITU-T G.7710] on network equipment internal management data flows). NOTE 3 – Such a detection function belongs to the category of statistical hypothesis testing, primarily due to uncertainties in the event description or the policy rule condition description for the unambiguous identification of such events. Thus, successful detection provides inherently probabilistic results only, including false positives besides true positives. The grade of detection quality should be consequently qualified and quantified, e.g., by estimating the expected non-true-positive ratio.	

7.3 Security objectives

Security assets (see clause 7.1) are analysed regarding a list of security objectives as outlined in Table 3.

Table 3 – Security objectives

Security asset	Security objective	Explanation
Management data	Integrity, confidentiality	Data that determines the functional behaviour of Ethernet network elements such as vehicle gateway, Ethernet switch, IDS and firewall shoud not be manipulated

Table 3 – Security objectives

Security asset	Security objective	Explanation
Ethernet communication related layer 2 protocol data units	Confidentiality	Prevent discosure of layer-specific protocol data units ((Lx)-PDU) transferred to an Ethernet-based automotive IVN.
	Availability	Communications services across the Ethernet-based automotive IVN shoud be possible whenever needed given that well-defined, communication service-related constraints are met
	Authenticity	Communications on the Ethernet-based automotive IVN shoud detect and reject imposters of other components
	Integrity	Prevent manipulation of communication data exchanged on the Ethernet-based automotive.
Management data generated by logging	Integrity	Prevent manipulation of the proof of and information about logged security events that can be audited without detection. Integrity covers bit and data integrity with scope on logged information
Cryptographic material	Confidentiality	Prevent disclosure of secrets and private keys, as well as user credentials like passwords.
	Integrity	Prevent manupulation of keys and certificates without detection
Firmware or, software image	Confidentiality	Prenvent disclosure of the contents of firmware and software such as compiled code and calibration data related to intellectual property to unauthorized entities
	Integrity	Prevent manipulation of firmware and software images, e.g., as the subject of capability change procedures (e.g., via firmware over the air, software over the air or software management in general)

7.4 Identified threats

7.4.1 Threats to confidentiality

– Unauthorized exposure of Ethernet communication traffic (as constituted by Ethernet physical layer (L1) or data link layer (L2) PDUs)

An attacker can sniff Ethernet communication traffic by connecting the component that is responsible for external communication with the Ethernet switch. The attacker then analyses communication traffic information by sniffing Ethernet related PDUs.

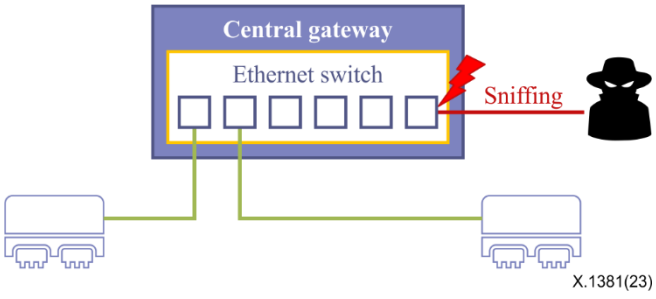

Figure 3 – Threats to confidentiality by sniffing

– Unauthorized exposure of cryptographic materials

An attacker can sniff cryptographic materials by:

- obtaining cryptographic material by physically opening the casing of the storage;
- reading the cryptographic material from the memory of each component where the cryptographic material is used;
- modifying the firmware and altering the control flow to expose the cryptographic material.

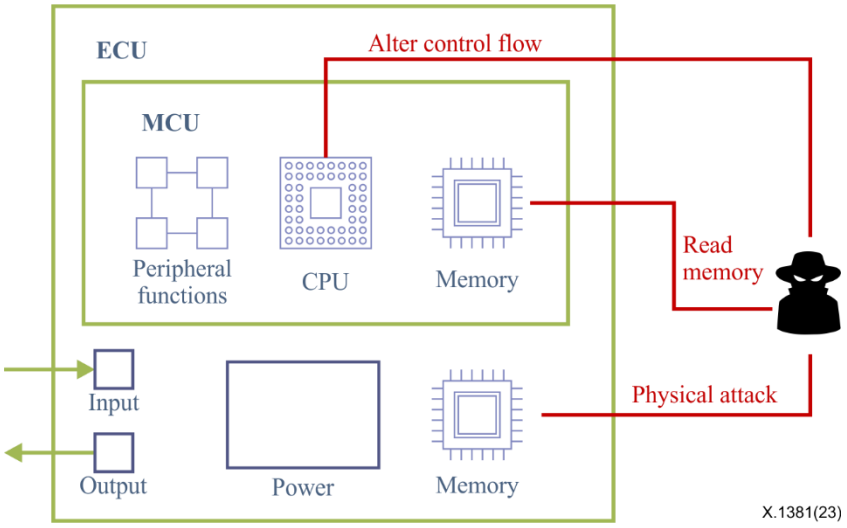

Figure 4 – Threats to confidentiality of cryptographic materials

7.4.2 Threats to integrity

The context of integrity is limited to data objects in general, given here by specific security use cases.

– Manipulation of configuration data

An attacker can manipulate the configuration data of the Ethernet switch.

– Manipulation of log data

An attacker can delete, modify log data, and especially audit logs of security events from the IDS, firewall, and over-the-air system.

– Manipulation of cryptographic materials

An attacker can change valid cryptographic materials on their own.

– Manipulation of firmware

An attacker can change the firmware into malicious firmware.

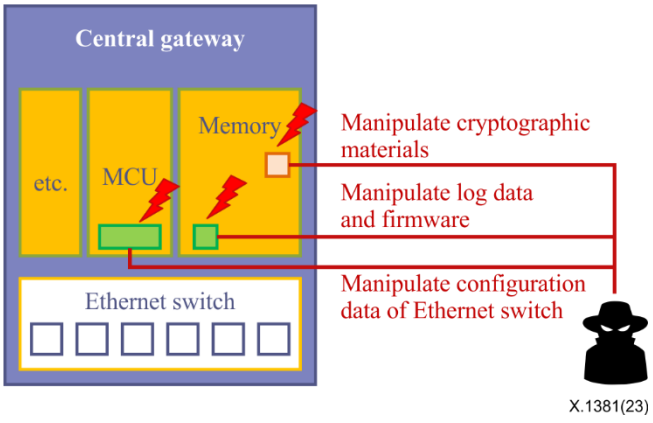

Figure 5 – Threats to integrity of data units under communication

7.4.3 Threats to availability

System quality attribute availability relates here to communication service availability for Ethernet-based communications, which transforms in network and layer-specific connection availability requirements in general, which again might lead to e.g., Ethernet path availability in case of a path redundant Ethernet IVN.

– Availability-specific threats: Denial of service (DoS) attack on Ethernet-based IVN

An attacker can perform a DoS attack in order to obstruct the functionality of a specific ECU including a CGW, vehicle border gateway or connectivity control unit.

As shown in Figure 6, an attacker can make a specific ECU and CGW unavailable to the desired counter ECUs using well-known DoS attack techniques such as IP transport protocol specific attacks like TCP SYN flood or teardrop attacks for the TCP. In addition, an attacker can make resources of IVN exhausted using attacks such as a layer 2 broadcast storms so that normal Ethernet MAC frames (as layer 2 PDUs) can no longer be exchanged.

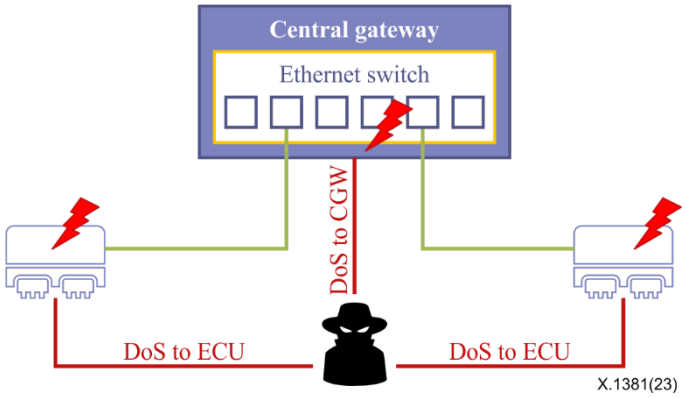

Figure 6 – Threats to availability

7.4.4 Threats to authenticity

– Impersonation of vehicle compute nodes (like ECUs)

An attacker can impersonate a valid component such as an ECU and send malicious messages to other components. An attacker can pretend to be a valid communication endpoint (e.g., hosted by an ECU) and send malicious messages or acquire transmitted communication traffic. In the example shown in Figure 7, the normal situation is given by upper layer connections between ECUs A and B (e.g., point-to-point IP transport connections), with the result that ECU-A sends Ethernet traffic to ECU-B (and possibly *vice versa*). An attacker pretends to be ECU-A using attack methods such as address resolution protocol (ARP) spoofing or IP spoofing (see e.g., [b-IETF RFC 2827][b-IETF RFC 4953][b-IETF RFC 6575][b-IETF RFC 6959]), and then sends a malicious message to ECU-B.

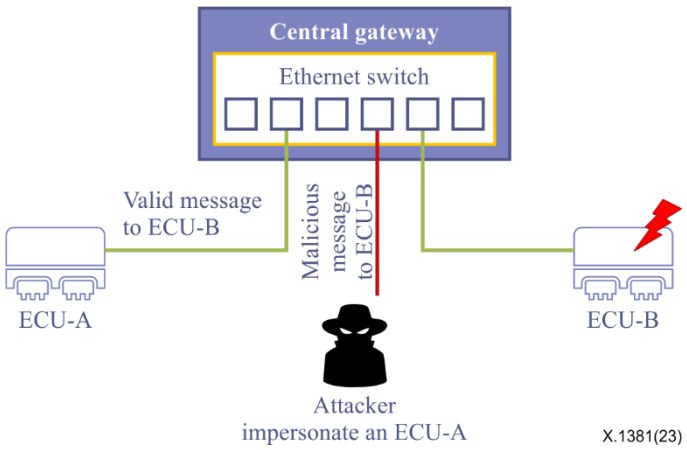

Figure 7 – Threats to authenticity

8 Security requirements

This clause describes security requirements to address the identified threats in Ethernet-based IVN environments.

8.1 Confidentiality

– [SR-01] An ECU that stores and uses cryptographic materials is recommended to use secure storage such as a hardware security module (HSM) in order to store the cryptographic materials securely.

– [SR-02] Well-known algorithms and protocols specified, for example, by international standard organizations are recommended for deployment.

– [SR-03] Security mechanisms to prevent eavesdropping are recommended for employment in the message in Ethernet communication.

Various layer specific security protocols can optionally be applied to the corresponding protocol layer to encrypt it and the protocol specific PDU (entirely or partially) as part of Ethernet-based communication traffic in a vehicle. Examples of such communication security protocols include media access control security (MACsec), IPsec, TLS and DTLS.

– [SR-04] An unauthorized entity is prevented from disclosing sensitive cryptographic materials.

The security mechanism in a vehicle is no longer secure when the cryptographic materials are exposed to unauthorized entities.

– [SR-05] Only authorized personnel and equipment according to an access control policy in a vehicle are recommended to handle cryptographic materials in the production phase.

– [SR-06] The MAC address table of the Ethernet switch is recommended to be statically configured.

Pre-defined ECUs can access an Ethernet in a vehicle by configuring the MAC address table in the Ethernet switch statically.

Dynamic MAC addresses can cause security problems like spoofing and MAC flooding. The switch can broadcast the data frame to all network ports when a large number of MAC addresses are stored in the table. In the case of a vehicle, the MAC address table can be statically configured to prevent these security issues, since the ECU that communicates with the switch is already specified.

– [SR-07] It is recommended that the dynamic learning function of a MAC address table in an Ethernet switch be disabled.

Deactivating the dynamic learning function of the MAC address table, a MAC flooding which can cause the transmission of Ethernet messages to unintentional destinations, can be prevented.

Nevertheless, if it is essential to the operation or maintenance of the vehicle, the switch should not store learned MAC address for a limited time only.

– [SR-08] It is recommended that IP network interfaces of IP host functions (e.g., hosted by ECUs) using the Ethernet get fixed IP addresses assigned by the responsible network management function.

NOTE – The specific network management functions here are identity management, including network address management. Such management functions may be performed during different lifecycle and operational phases of the Ethernet-based IVN, e.g., fully static a-priori, mix of static and dynamic configuration management, also dependent on the usage or not of network operational protocols for the Ethernet and Internet layers.

This SR applies not only to single ECUs as a whole but also each partition or node within an Ethernet network (e.g., each virtual machine).

8.2 Integrity

– [SR-09] It is recommended that logging and configuration data of an Ethernet switch be protected against unauthorized modification and deletion.

– [SR-10] It is recommended that updates of configuration data be only performed by authorized entities.

– [SR-11] It is recommended that an ECU employ secure boot features along with an integrity check of firmware.

The firmware of an ECU and an Ethernet switch data stored in the memory of the ECU should be checked for integrity before or during execution. An integrity check of the configuration and input parameters of the firmware can be used for secure boot.

8.3 Availability

The meaning of availability in this context relates to network availability of Ethernet domains, i.e., the communication service available. Security attacks can impact such availability objectives, but also other kinds of non-security specific events (like a component outage or communication failure).

Thus, availability requirements (in this clause) are actually security requirements with potential impact on availability targets.

– [SR-12] It is recommended that DoS attacks against Ethernet-based IVN be considered at the design phase of a vehicle.

– [SR-13] It is recommended that an switch detect and protect against a DoS attack through Ethernet communication messages.

The monitoring and controlling of traffic flows between ECUs are crucial in order to minimize the risks from the DoS attacks in an IVN.

– [SR-14] Safety-critical functions are recommended for isolation from other networks in a vehicle.

8.4 Authenticity

Authenticity means the ability to ensure that the given information is without modification or forgery and was in fact produced by the entity who claims to have given the information.

– [SR-15] It is recommended that countermeasures be provided for Ethernet communication messages to be protected against impersonation attacks.

– [SR-16] It is recommended that physical Ethernet network interfaces of IVN network elements, which are not intended for use in a production vehicle, provide the ability of temporal administrative state changes (enable, disable), using a default configuration value of "disabled".

NOTE – Such a network management-related requirement obviously implies the support of a correspondent fine granular management data model for the Ethernet.

This requirement limits the attack surface by reducing the number of available entry points.

– [SR-17] It is recommended that access communication interface, either realized in the hardware or software domain, be limited according to the principle of least privilege.

– [SR-18] It is recommended that a debug interface in an ECU be configured for protection against unauthorized entities. That requirement covers vehicle compute node local debug interfaces as well as remote debug interfaces with IVN-based access to such a network node.

Table 4 shows the mapping between the threats identified in clause 7 and the security requirements in clause 8.

Table 4 – Mapping of security requirements and threats

Threats	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Unauthorized exposure of an Ethernet communication message	–	Y	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y
Unauthorized exposure of cryptographic materials	Y	Y	–	Y	Y	–	–	–	–	–	–	–	–	–	–	–	–	Y
Manipulation of configuration data	Y	Y	–	–	–	Y	Y	–	Y	Y	Y	–	–	–	–	–	–	Y
Manipulation of log data	Y	Y	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–	Y
Manipulation of cryptographic materials	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y
DoS attack on Ethernet-based IVN	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–
Impersonation of ECU	–	Y	–	–	–	Y	Y	Y	–	–	–	–	–	Y	Y	Y	Y	Y

Each identified threat can be addressed by satisfying the corresponding security requirements marked with Y. For example, the security requirements for the first threat, unauthorized exposure of an Ethernet communication message, are [SR-2], [SR-3], and [SR-18].

9 Implementation of Ethernet-based in-vehicle networks with security

9.1 Implementation related considerations in advance

This Recommendation provides implementation-related considerations in order to:

- outline security aspects that are driven by technical constraints;
- illustrate implementation-specific security issues in a typical technical IVN architecture.

The value of such security information is inherently tightly coupled to the specific technical view only, thus might be obsolete in future, e.g., if technical IVN system architectures change.

However, there are not yet any applicable, non-technical reference models and reference architectures for IVNs that might be used as baseline for the discussion of implementation-specific security aspects. This Recommendation therefore provides at least some security considerations by looking at example technical IVN systems (as introduced by clause 6).

9.2 Automotive Ethernet associated security gateway functions

Monitoring and controlling the flow of communication between different logical network domains (e.g., VLAN, IPv4 subnet, IPv6 prefix defined subnet; each logical network domain represents a specific security domain by its security attributes) is important to minimize the risk from unauthorized access and DoS attacks in Ethernet-based IVNs. Firewalls specifically or security gateways in general are used to allow or deny communication data according to predetermined rules at the IVN or at the junction of the in-vehicle and external networks to increase the vehicle security level.

The following technical components that can monitor communication messages coming from outside the vehicle or IVN are recommended for the implementation of such security gateway functions (like firewalls), as known in current, typical in-vehicle technical E/E architecture.

– Ethernet switch.

NOTE 1 – The logical Ethernet switch component represents a network node type, not an end node. There are two IVN implementation options. an Ethernet switch as stand-alone technical component or monolithically integrated as front or end node into an vehicle compute node.

– Vehicle border gateway.

NOTE 2 – The native choice because that technical component represents the single observation point for regular V2X communication traffic.

– ECU: when ECU has direct external communication.

NOTE 3 – A vehicle compute node might provide additional communication interfaces for direct, vehicle external communication (i.e., bypassing the vehicle border gateway), e.g., for diagnostic purposes.

The firewall uses several mechanisms for packet filtering, including static packet filtering, stateless or stateful packet inspection, shallow, medium-depth or even deep packet inspection.

NOTE 4 – The metaphorical terms "shallow", "deep", etc. need to be mapped and associated with: a) protocol layer; and b) PDU context type of information (see e.g., [b-ITU-T Y.2770][b-ITU-T Y.2771]) in order to be unambiguous, e.g., "shallow packet inspection" would be typically be a L3,4 header inspection in the case of Internet traffic.

In particular, static packet filtering mechanism is based on predefined policy rules. Therefore, a specific policy rule setting is recommended according to the vehicle E/E architecture and the communication protocol applied. Additionally, the firewall policy applies to the whitelist method as default, which basically blocks all communication that is not explicitly allowed.

One firewall main feature is defence against DoS attacks. Firewalls can protect the network from DoS attacks by setting thresholds using pre-stored values, such as counters, or by applying frequency filters.

Another complementary feature of the firewall is the logging function (i.e., the firewall network element as a managed entity provides an integrated log management function according to [b-ITU-T M.3705]). Security related events are expected to be subject of logging services in general. Thus, firewalls, IDSs or security gateways in general log information when a security event occurs, which not only helps forensic specialists to analyse the event situation, but also enhances the precision of the firewall policy through studies such as blocking records. Therefore, when storing the log, it is necessary to use the cryptographic mechanism to ensure integrity.

9.3 Secure VLAN configuration

Configuring a secure VLAN is very important for the communication security of the IVN to address [SR-14] and [SR-17] OEMs are expected to be responsible authority for the specification of that VLAN because VLAN configuration is dependent on the OEMs chosen vehicle E/E architecture.

Each VLAN has a unique value called a VLAN identifier (ID). According to the specification of the VLAN, the VLAN ID (VID) can be used from 0 to 4094, but predefined VLAN ID described in

Table 5 should not be used. VLAN ID 1 can also be used for attacks using double tagging, so switch should change VLAN ID 1 into another VLAN ID.

Table 5 – Reserved VLAN ID

VID value (hexadecimal)	Meaning/Use
0	The null VID indicates that the tag header contains only priority information; no VID is present in the frame. This VID value should not be configured as a port VLAN ID (PVID) or a member of a VID set, or configured in any forwarding database (FDB) entry, or used in any management operation.
1	The default PVID value used for classifying frames on ingress through a bridge port. The PVID value of a port can be changed by management.
FFF	Reserved for implementation use. This VID value should not be configured as a PVID or a member of a VID or transmitted in a tag header. This VID value can be used to indicate a wildcard match for the VID in management operations or FDB entries.

An attacker can monitor Ethernet traffic by unauthorized access from another VLAN through a "VLAN hopping" attack. To mitigate this attack, frames that are not tagged with VLANs should be configured to be dropped. However, the following exceptions can exist. For time synchronization, messages are sent via the precision time protocol, that requires frames to be transmitted without VLAN tags according to [b-IEEE 802.1AS].

An attacker who is included in a native VLAN can perform a double tagging attack using a default native VLAN ID. The attacker adds two tags to the frame: the first contains the default native VLAN ID; and the second the attacker's target VLAN ID. When the frame with tags added passes through the first switch, the first tag is removed and the frame with the second is forwarded to the next switch. That switch thenforwards the frame to the target VLAN using the remaining second tag. In this way, the attacker can send the message to the target VLAN. Therefore, the default native VLAN ID should be changed in order to prevent this attack.

9.4 Security for Ethernet switches in automotive context

The IEEE Ethernet bridge, also commonly known as Ethernet switch, provides inherently a forwarding information base (FIB) as native means for the forwarding and switching process. Such a FIB includes a MAC address table.

NOTE 1 – This Recommendation uses a very abstract Ethernet switch model, focusing only on network functions that are potentially subject to security s. A comprehensive overview of all basic Ethernet switch functions is outlined in [b-IEEE Std 802.1Q].

NOTE 2 – For instance, [b-IEEE 802.1Q] specifies a (policy) rule Ethernet MAC frame processing model, divided into ingress, forwarding and egress rules. That is of particular interest, e.g., in the VLAN context.

Typical Ethernet switches provide dynamic address learning mechanisms for networks that require flexibility. When a new ECU is connected to the switch port, an entry for the MAC address of an Ethernet endnode is automatically added to the MAC address table so that it can communicate with other ECUs in the entire Ethernet network domain, via that switch stage.

NOTE 3 – There might be more than one Ethernet switch in the end-to-end communication path.

The dynamic MAC address learning feature facilitates unauthorized access to the network and should be disabled. This feature can be required if external diagnostic devices are required for maintenance or diagnostic purposes. In this case, the switch should support the ability to limit the validity time of dynamically learned MAC addresses. It is obvious that these two recommendations are contradictory, but actually depend on a specific operational context of the in-vehicle Ethernet network: without or with external connectivity to, for example, a DoIP Ethernet network domain. Such network

operational context dependencies can lead to conditional security recommendations, e.g., here a limited, restricted time window with enabled dynamic address learning or the like.

MAC address spoofing is a well-known attack on computer networks that can be implemented into vehicle attack scenarios. To protect the IVN, authentication and reliability of connected devices using port-based network access control should be guaranteed if an access variant is used. Such a control authenticates a component before granting access to the network. The Ethernet switch communicates with the network only if the authentication is successful.

To mitigate DoS attacks, the switch should prevent broadcast storms and support port-based rate-limits on receiving packets (see the Ethernet traffic parameter control in [b-ITU-T Y.1222]).

For the security of the switch, the integrity of the switch configuration management data should be ensured and it should be possible only through a secure programming mechanism or secure management protocol for updates for updates.

– Generally, security functions required for the operation and management of Ethernet switches in automotive applications that integrate an own processor are as follows: Secure storage

  Secure storage enssures the confidentiality and integrity of the stored data. Data such as keys and MAC should be protected using secure storage such as an HSM.

– Secure boot

  Secure boot checks the integrity of the software every boot cycle. On an initial boot, a message authentication code of the software image is generated and stored in secure storage. On the next boot, if the newly generated message authentication code is the same as that stored, the integrity of the software is ensured.

– Secure debug interface

  A secure debug interface prevents unauthorized access to the debug interface. Debug interfaces are usually recommended for removal so that any debugging entities cannot be connected. Nevertheless, if the interfaces are necessary for product assurance or maintenance, the access should be allowed to authorized entities only.

– Secure software update

  A secure software update allows a software re-programming only if the authenticity of the software is assured. The software supplier generates a digital signature using their private key and sends the digital signature and software image together. When the receiver verifies that the digital signature is generated by the supplier using the supplier's public key, the authenticity of the software is assured.

Appendix I

Description of some Ethernet-based in-vehicle network protocols with communication endpoints located in AUTOSAR or non-AUTOSAR compute nodes

(This appendix does not form an integral part of this Recommendation.)

There are several communication protocols for the Ethernet-based network, and many use cases employed in Ethernet-based in-vehicle communication deploy one or a combination of them. Furthermore, compute nodes in IVNs can not only be operated with a system according to AUTOSAR-based software architectures (like AUTOSAR Classic Platform, AUTOSAR Adaptive Platform), but also use non-AUTOSAR software-based communication architectures.

Thus, basically assume that an IVN is composed of a mix of AUTOSAR and non-AUTOSAR compute nodes in the context of Ethernet and Internet IVN engineering.

I.1 Overview and scope

This appendix briefly explains protocols that are intended for use in Ethernet-based in-vehicle communication, as shown in Figure I.1.

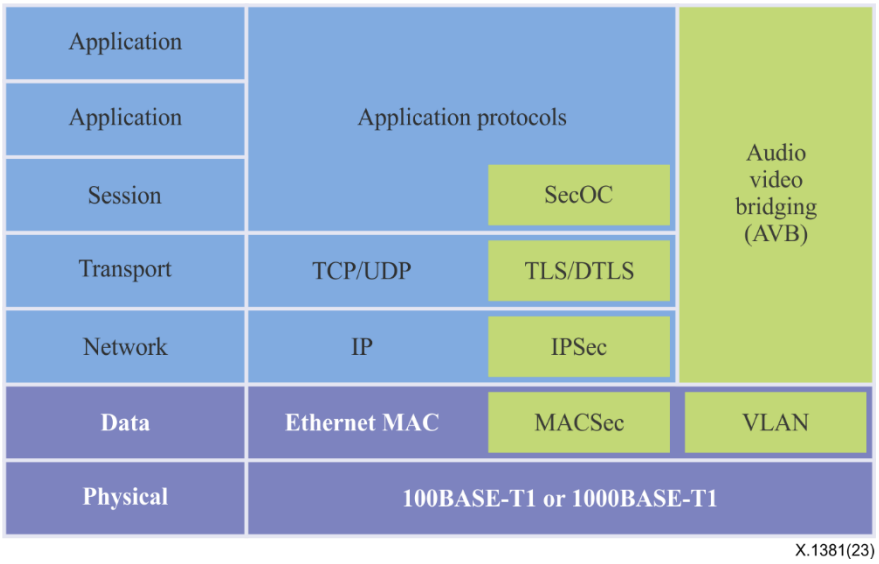

Figure I.1 – Internet protocol-based and Internet protocol-less communication services over Ethernet with associated, layer specific security protocols as targeted for in in-vehicle networks

Note that Figure I.1 focuses on communication transport services, rather than session and application layer protocols. For instance, the AUTOSAR-based scalable service-oriented middleware over IP, a session and presentation layer protocol for IP-based, service-oriented communication services, lies outside the scope of this Recommendation.

I.2 AUTOSAR secure onboard communication inclusive lower protocol layer security protocols

Recall that AUTOSAR determines a software architecture, thus excludes deployment architectures. There are thus many options for how the following software system could be mapped on processor elements (using concurrency, parallelism, replacing the AUTOSAR defined communication stack by a commercial off-the-shelf stack, etc.).

The Ethernet has been part of its standard since AUTOSAR classic release 4.0 [b-Autosar 654]. In the AUTOSAR architecture, the Ethernet communication stack is located in parallel (in the software architecture) with the CAN, LIN, and FlexRay stack instances.

The AUTOSAR PDU router is responsible for the compute node internal routing of AUTOSAR PDUs between the AUTOSAR applications and the communication endpoint associated network interfaces.

NOTE 1 – Thus, the AUTOSAR PDU router function is overlapping, but should not be confused with legacy traffic routing functions in non-AUTOSAR communication endpoints.

The message generated by the application is sent to the PDU router, which sends a message to a corresponding interface or transport protocol (TP) module. Each interface/TP transmits the message to a network interface through a relevant driver. In the case of the Ethernet, the PDU router sends a message to a socket adaptor (i.e., the layer 4 service access point for TCP- or UDP-based communication) and it is transmitted to the Ethernet interface via TCP/IP module. Figure I.2 shows the control and data flow in the extended AUTOSAR communication stack.

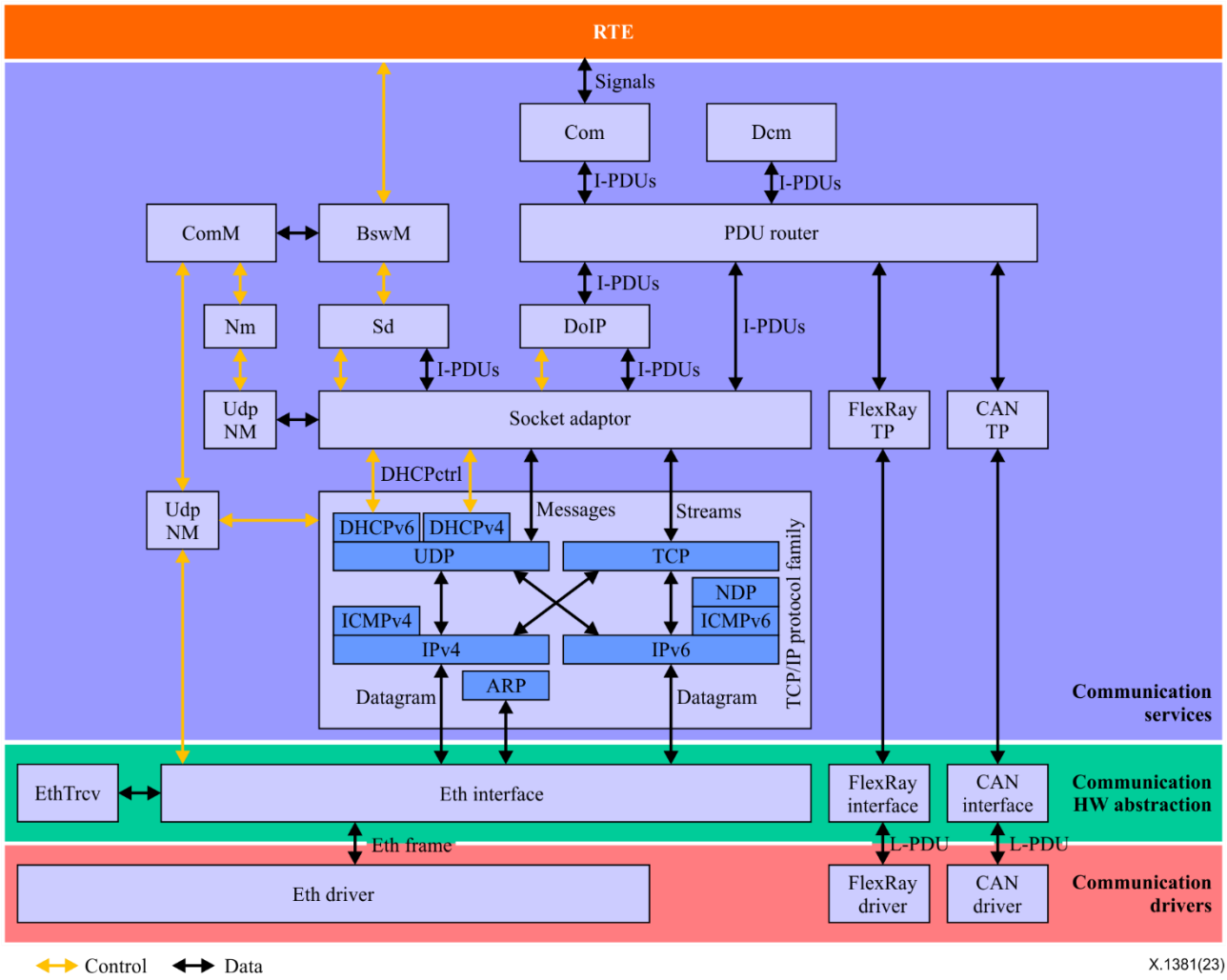

Figure I.2 – Extended AUTOSAR communication stack (software architecture only) (Source: [b-AUTOSAR 617])

NOTE 2 – The AUTOSAR introduced PDU notation that differs from legacy PDU semantics used in ICT (as specified in [b-ITU-T X.200]). The AUTOSAR software system internal I-PDU, N-PDU or L-PDU are mapped or appear at the used network communication interfaces as layer *x* PDU, in general (L*x*)-PDU, depending on the specific29 protocol stack used.

I.2.1 Secure onboard communication

Cryptographic services of AUTOSAR are provided by the crypto service, security hardware abstract and crypto driver, which collectively are called the crypt stack. The crypt driver depends on the microcontroller and provides the interface that can access hardware. The security hardware abstract provides a common interface as middleware between the crypto service and security hardware. The common interface provides independence between a crypto driver that depends on security hardware and a crypto service as an upper layer service. A crypto service manager (CSM) is the only module to be included in crypto service.

Secure onboard communication (SecOC) is a service of the CSM and provides integrity for communication messages.

The goal of SecOC is to provide the authentication mechanisms that are practical and resource effective for the software level (or protocol layer) of a PDU. This kind of authentication mechanism uses a message authentication code based on a symmetric cryptography algorithm because they should minimize resource consumption to add on legacy systems.

SecOC uses a CSM to generate and verify message authentication code. A CSM can accelerate the calculation of message authentication code using an HSM.

Figure I.3 ia a functional overview of SecOC.

A sender generates a secure PDU by adding an authentication tag that contains message authentication code and freshness value to the PDU. The freshness value can be a counter value or a time stamp.

A receiver verifies the authentication tag in the secure PDU received, i.e., a receiver generates message authentication code based on the data of the secure PDU received and compares it with the message authentication code received.

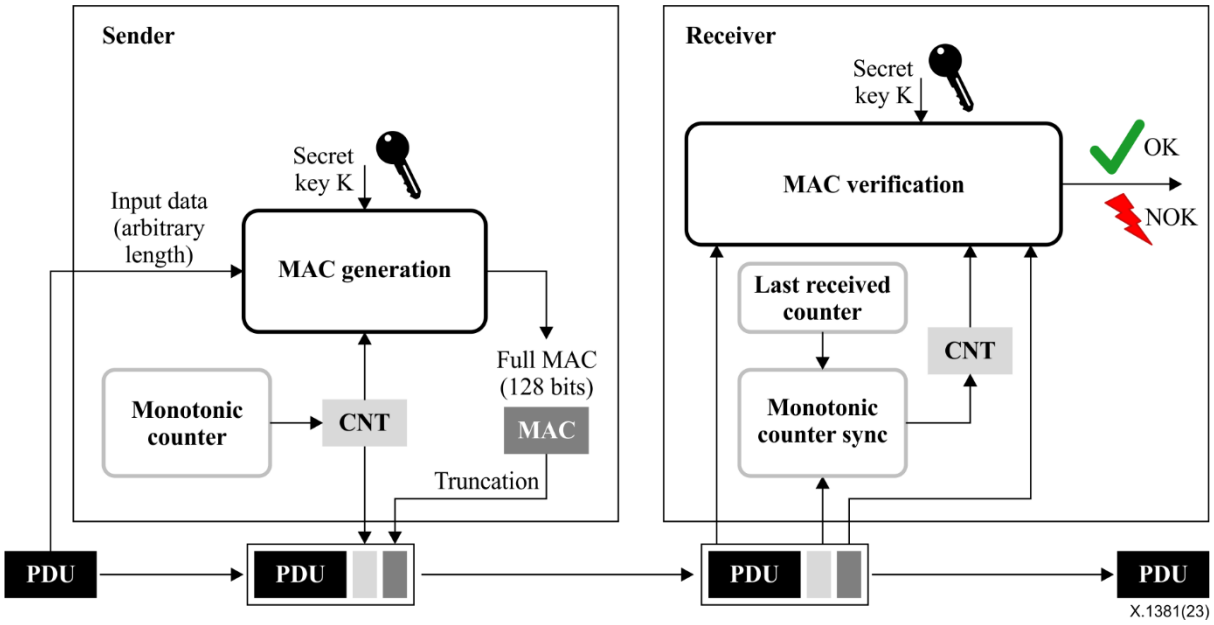

Figure I.3 – Message authentication and freshness verification [b-Autosar 654]

I.2.2 Transport layer security

TLS provides end-to-end secure communication services over reliable TPs such as TCP.

AUTOSAR does not support TLS versions lower than TLS 1.2.

NOTE – See also [b-IETF RFC 8996] concerning the deprecation of TLS 1.0 and TLS 1.1.

To use TLS in AUTOSAR, the crypto service manager allows crypto jobs and key operations used by the TLS and IPsec submodule to be performed. Detailed requirements and specifications can be found in [b-AUTOSAR 617].

I.2.3 Datagram transport layer security

This topic is for further study for a subsequent edition of this Recommendation.

I.2.4 Internet protocol security

IPsec is basically the native network layer security protocol for IP-based networks, supporting authentication and encryption. IPsec is optional for IPv4, but mandatory for IPv6. The deployment of IPsec in ICT is typically, if at all, limited to small area, but not used in large area, IP networks due to limited, completely thorough end-to-end IP connectivity (e.g., interruptions due to IP topology hiding gateways or IP security gateways).

However, in-vehicle IP networks belong rather to the category of (very) small area networks, and are subject to a single network management authority, which should not prevent the usage of IPsec, limited to the intra-vehicle IP network domain(s).

According to [b-AUTOSAR 617], the tunnel mode of IPsec is not currently available in AUTOSAR. Only the transport mode can be used. It also does not support IPv6 and multicast. Detailed requirements and specifications can be found in [b-AUTOSAR 970].

NOTE – This edition of this Recommendation does not provide IP version specific security considerations for the IPsec protocol.

I.3 Diagnostic communication over Internet protocol

The DoIP is for diagnostic purposes, without any built-in security means.

The DoIP is an IP-based TP specified in [b-ISO 13400-2]. DoIP can transfer messages between UDSs in a vehicle and external test equipment via the Ethernet. The DoIP depends on the following protocols:

– DHCP;

– ICMP;

– MAC address searching based on IP address (IPv4: ARP, IPv6: neighbour discovery protocol).

In UDP, each datagram contains only one DoIP message. For TCP-based data, the header separates the individual DoIP messages within the data stream.

The IANA-registered well-known TCP port 13400 should be used for DoIP communication (diagnostic requests and diagnostic responses) from external diagnostic equipment to the vehicle ECU.

The DoIP does not consider any mechanism for communication security. The messages are not authenticated or encrypted in any way. Therefore, when designing DoIP services, security architects should consider using different layers of security protocols.

I.4 Media access control security

MACsec is an [b-IEEE 802.1AE] standard security protocol that provides secure communication for all traffic on the data link layer. MACsec supports end-to-end or hop-to-hop security at the Ethernet layer 2 connection level (i.e., end-to end "links" or local links) between Ethernet end nodes or switch nodes. MACsec includes authentication and encryption or decryption, which allows identification and prevention of most security threats, including DoS, intrusion, man-in-the-middle, masquerading, passive wiretapping and playback attacks.

Appendix II

Vehicle gateways with Ethernet, IP or Internet connectivity

(This appendix does not form an integral part of this Recommendation.)

II.1 Motivation

A CGW, vehicle border gateway or VGs in general provide a crucial role in in-vehicle communication security architecture, particularly for Ethernet and IP-based network domains and communication services. The network topological location of a CGW as vehicle border gateway implies and determines a security gateway role between vehicle internal and external network domains.

The specification and standardization of such network element types is typically associated with explicit security considerations or even security guidelines and specifications.

II.2 Purpose of this appendix

This appendix provides a non-exhaustive list of security relevant VG standards, which might be beneficial, e.g., due to complementary communication security information, within the scope of this Recommendation. This appendix might be subject to updates in subsequent editions of this Recommendation.

II.3 Selected vehicle gateway Recommendations with security information

This clause lists Recommendations relevant to security, without any evaluation of their security specific Recommendations.

– [b-ITU-T F.749.1]: includes functional requirements for security;

– [b-ITU-T F.749.2]: provides dedicated clauses on communication security requirements and high-layer security requirements;

– [b-ITU-T H.550]: security aspects are primarily related to security management of VGs;

– [b-ITU-T H.560]: security aspects are primarily related to the communication interface of VGs used for external communication.

Appendix III

Intra-vehicle intelligent transport system security

(This appendix does not form an integral part of this Recommendation.)

III.1 Background

The notion of ITS includes a vehicle communication architecture that covers the vehicle internal communication system plus the interconnection to vehicle external communication systems and services. The most crucial network and communication element in the overall architecture is the in-vehicle located, so-called ITS station, see e.g., [b-ETSI EN 302 665][b-ETSI TR 101 607].

The ITS station represents an in-vehicle communication network, which might be Ethernet-based, offering IP-less and IP-based communication services. Such a technical ITS solution would match the scope of this Recommendation.

III.2 ITS in-vehicle networks

An ITS-specified IVN architecture is composed of the same network elements as described in the main body of this Recommendation: vehicle ITS gateway; vehicle ITS host; vehicle ITS router; vehicle ITS border router or gateway; etc. Consequently, ITS security guidelines apply also to this Recommendation to a very large extent, particularly whenever communication technologies (i.e., the protocols and protocol stacks) and communication architecture are the same.

III.3 ITS security

It is not the purpose of this Recommendation to evaluate ITS-defined security. However, threat, vulnerability and risk analysis conducted under ITS, ITS security guidelines, security services or security architecture might be beneficial complementary reading, especially in case of communication security. See [b-ETSI TS 102 731] for more information and further security references.

Bibliography

[b-ITU-T F.749.1] Recommendation ITU-T F.749.1 (2015), *Functional requirements for vehicle gateways*.

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

[b-ITU-T G.7710] Recommendation ITU-T G.7710/Y.1701 (2020), *Common equipment management function requirements*.

[b-ITU-T G.8013] Recommendation ITU-T G.8013/Y.1731 (2015), *Operations, administration and maintenance (OAM) functions and mechanisms for Ethernet-based networks*.

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

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

[b-ITU-T M.3010] Recommendation ITU-T M.3010 (2000), *Principles for a telecommunications management network*.

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

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

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

[b-ITU-T X.200] Recommendation ITU-T X.200 (1994), *Information technology – Open systems interconnection – Basic reference model: The basic model*.

[b-ITU-T X.641] Recommendation ITU-T X.641 (1997), *Information technology – Quality of service: framework*.

[b-ITU-T X.703] Recommendation ITU-T X.703 (1997), *Information technology – Open distributed management architecture*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

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

[b-ITU-T Y.1222] Recommendation ITU-T Y.1222 (2004), *Requirements for OAM functions in Ethernet-based networks and Ethernet services*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2021), *Baseline identity management terms and definitions*.

[b-ITU-T Y.1730] Recommendation ITU-T Y.1730 (2004), *Requirements for OAM functions in Ethernet-based networks and Ethernet services*.

[b-ITU-T Y.2770] Recommendation ITU-T Y.2770 (2012), *Requirements for deep packet inspection in next generation networks*.

[b-ITU-T Y.2771] Recommendation ITU-T Y.2771 (2014), *Framework for deep packet inspection*.

[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] European Standard ETSI EN 302 665 V1.1.1 (2010), *Intelligent transport systems (ITS); Communications architecture*.

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

[b-ETSI TS 102 731] Technical Specification 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*. Available [viewed 2022-06-30]: 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.* Available [viewed 2022-06-30]: 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).* Available [viewed 2022-06-30]: 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] International Standard ISO 13400-2:2019, *Road vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 2: Transport protocol and network layer services*.

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

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2023