

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/>.

© ITU 2023

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

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., E³; 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.

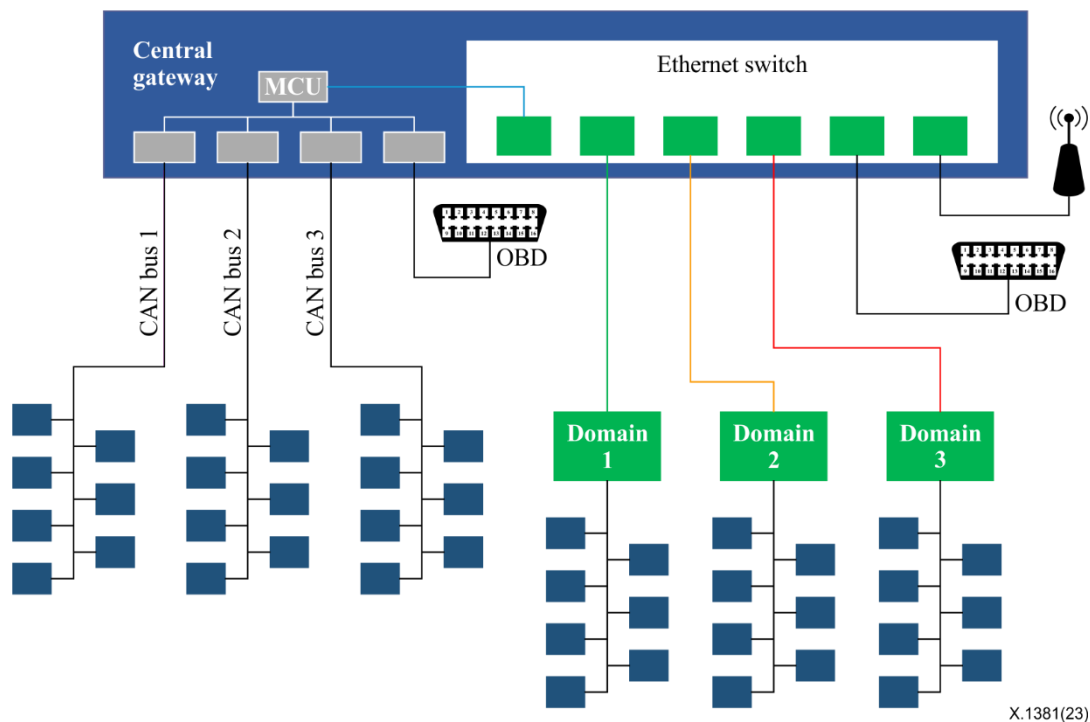


Figure 1 – The current heterogeneity of a typical in-vehicle network, based on legacy protocols and the automotive Ethernet

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).