INTERNATIONAL STANDARD

ISO 13400-2

Second edition
2019-12

Road vehicles — Diagnostic communication over Internet Protocol (DoIP) —

Part 2: Transport protocol and network layer services

Véhicules routiers — Communication de diagnostic au travers du protocole internet (DoIP) —

Partie 2: Protocole de transport et services de la couche réseau

Reference number
ISO 13400-2:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 31, *Data communication*.

This second edition cancels and replaces the first edition (ISO 13400-2:2012), which has been technically revised.

The main changes compared to the previous edition are as follows:

— addition of TLS (Transport Layer Security);

— major restructuring of document content.

A list of all parts in the ISO 13400 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Vehicle diagnostic communication has been developed starting with the introduction of the first legislated emissions-related diagnostics and has evolved over the years, now covering various use cases ranging from emission-related diagnostics to vehicle-manufacturer-specific applications like calibration or electronic component software updates.

With the introduction of new in-vehicle network communication technologies, the interface between the vehicle's servers and the client DoIP entity has been adapted several times to address the specific characteristics of each new network communication technology requiring optimized data link layer definitions and transport protocol developments in order to make the new in-vehicle networks usable for diagnostic communication.

With increasing memory size of servers, the demand to update this increasing amount of software and an increasing number of functions provided by these control units, technology of the connecting network and buses has been driven to a level of complexity and speed similar to computer networks. Various applications (x-by-wire, infotainment) require high band-width and real-time networks (like FlexRay, MOST), which cannot be adapted to provide the direct interface to a vehicle. This requires gateways to route and convert messages between the in-vehicle networks and the vehicle interface to client DoIP entity.

All parts of ISO 13400 are applicable to vehicle diagnostic systems implemented on an IP communication network.

The ISO 13400 series has been established in order to define common requirements for vehicle diagnostic systems implemented on an IP communication link.

Although primarily intended for diagnostic systems, ISO 13400 has been developed to also meet requirements from other IP-based systems needing a transport protocol and network layer services.

The intent of the ISO 13400 series is to describe a standardized vehicle interface which

— separates in-vehicle network technology from the client DoIP entity vehicle interface requirements to allow for a long-term stable external vehicle communication interface,

— utilizes existing industry standards to define a long-term stable state-of-the-art communication standard usable for legislated diagnostic communication as well as for manufacturer-specific use cases,

— can easily be adapted to new physical and data link layers, including wired and wireless connections, by using existing adaptation layers, and

— allows connections of vehicle-internal and vehicle-external DoIP entities.

To achieve this, it is based on the Open Systems Interconnection (OSI) Basic Reference Model specified in ISO/IEC 7498-1 and ISO/IEC 10731[1], which structures communication systems into seven layers.

Figure 1 illustrates an overview of communication frameworks beyond the scope of this document including related standards:

— Vehicle diagnostic communication framework, which is composed of ISO 14229-1[3], ISO 14229-2[4], and ISO 14229-5[5].

— Presentation layer standards, for example vehicle manufacturer- (VM-) specific or ISO 22901 ODX[6].

— OSI lower layers framework, which is composed of ISO 13400-3 and ISO 13400-4[2].

The ISO 13400 series and ISO 14229-5[5] are based on the conventions specified in the OSI Service Conventions (ISO/IEC 10731)[1] as they apply for all layers and the diagnostic services.

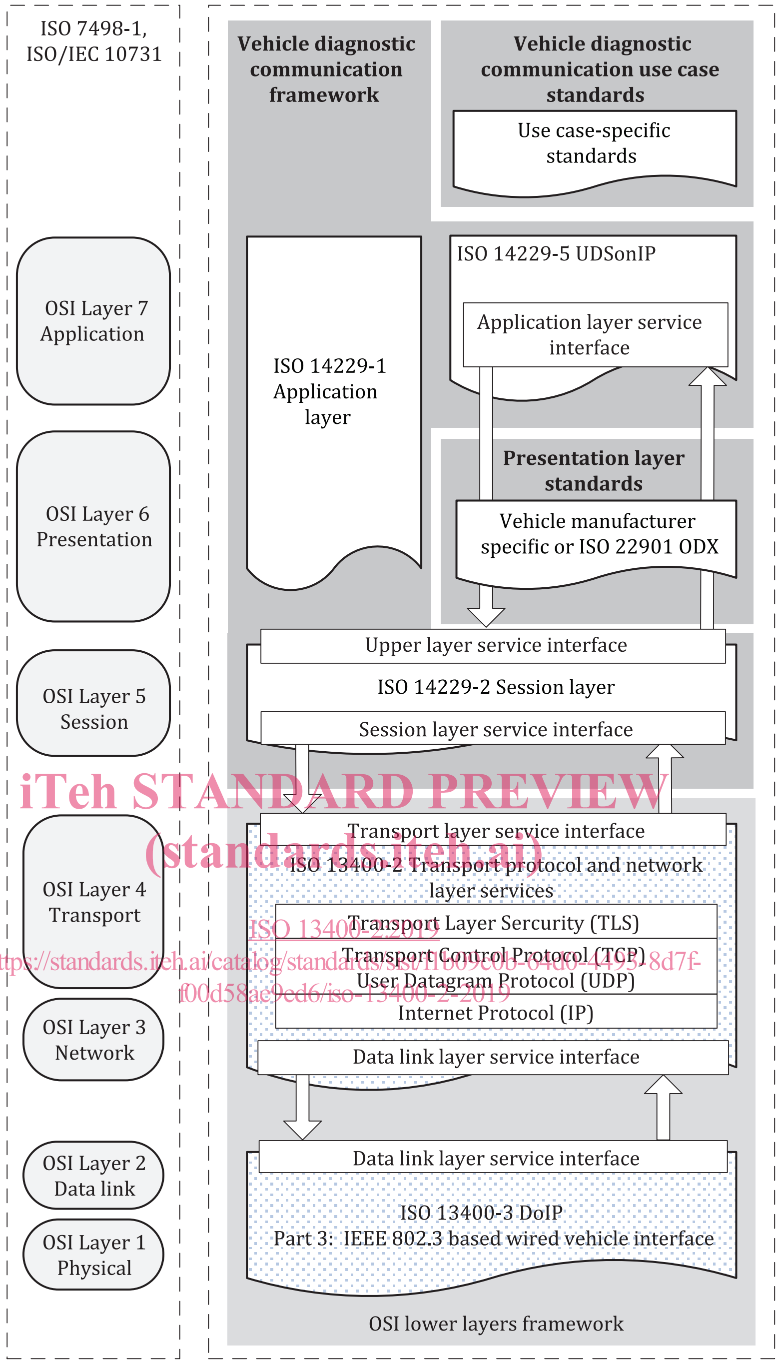
ISO 7498-1,
ISO/IEC 10731
Vehicle diagnostic communication framework
Vehicle diagnostic communication use case standards
Use case-specific standards
OSI Layer 7
Application
ISO 14229-1
Application
layer
ISO 14229-5 UDSonIP
Application layer service interface
OSI Layer 6
Presentation
Presentation layer standards
Vehicle manufacturer specific or ISO 22901 ODX
OSI Layer 5
Session
Upper layer service interface
ISO 14229-2 Session layer
Session layer service interface
OSI Layer 4
Transport
Transport layer service interface
ISO 13400-2 Transport protocol and network layer services
Transport Layer Sercurity (TLS)
Transport Control Protocol (TCP)
User Datagram Protocol (UDP)
OSI Layer 3
Network
Internet Protocol (IP)
Data link layer service interface
OSI Layer 2
Data link
OSI Layer 1
Physical
Data link layer service interface
ISO 13400-3 DoIP
Part 3: IEEE 802.3 based wired vehicle interface
OSI lower layers framework

Figure 1 — DoIP document reference according to OSI model

Figure 2 illustrates vehicle network architecture schematics from a functional viewpoint.

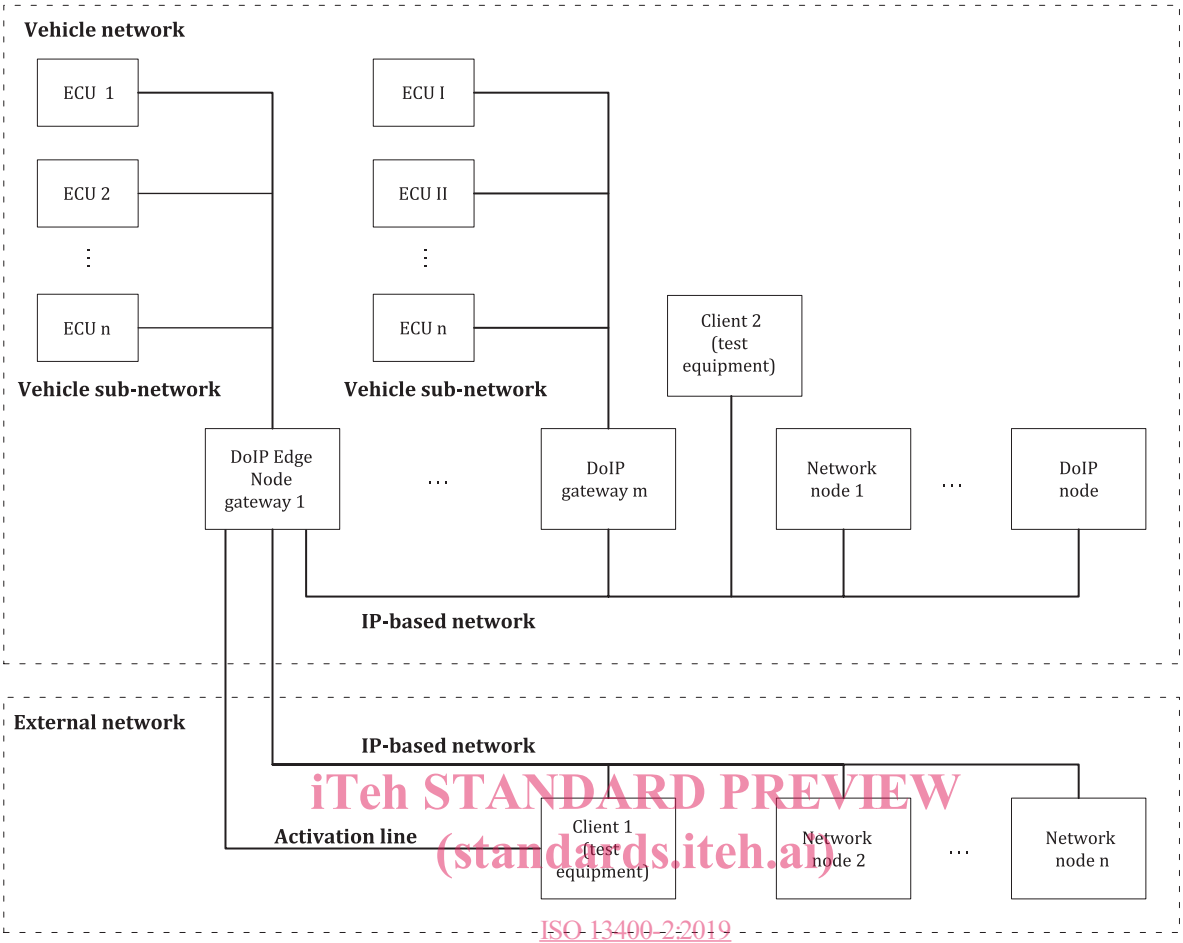

Figure 2 — Vehicle network architecture schematics (functional view)

This protocol standard is implemented by one or more DoIP entities, depending on the vehicle's network architecture. Figure 2 illustrates a client 1 (external client), which is connected to the DoIP edge node and a client 2 (internal client) in the vehicle's internal network. If not stated otherwise, the DoIP client entities are assumed to behave the same regardless to which network they are connected.

If necessary, this document distinguishes between an "internal client" and "external client" to apply a requirement or statement.

In this document, the requirements are assigned a unique number of the form "**X.DoIP-yyy**", allowing for easier requirement tracking and reference.

— X = OSI layer number; and

— DoIP-yyy = requirement number; and

— xL = x = OSI layer abbrevation[8 = APP, 7 = AL, 6 = PL, 5 = SL, 4 = TL, 3 = NL, 2 = DLL, 1 = PHY, 0 = SPP].

NOTE Requirements in this document are not numbered sequentially because the order of individual requirements changed during document development.

Requirements formulated as "The vehicle shall implement …" imply that this is a requirement for all DoIP entities to implement the required functionality if not explicitly stated otherwise. If multiple DoIP entities are present on a vehicle network, implementation details may differ slightly for each DoIP entity (e.g. for identification purposes), so that the client DoIP entity is able to identify the individual DoIP gateways that support this protocol standard.

Where reference is made to RFC documents, note that the forms “shall/shall not” are used to express requirements in these documents.

Road vehicles — Diagnostic communication over Internet Protocol (DoIP) —

Part 2: Transport protocol and network layer services

1 Scope

This document specifies the requirements for secured and unsecured diagnostic communication between client DoIP entity and server(s) installed in the vehicle using Internet protocol (IP) as well as the transmission control protocol (TCP) and user datagram protocol (UDP). This includes the definition of vehicle gateway requirements (e.g. for integration into an existing computer network) and test equipment (client DoIP entity) requirements (e.g. to detect and establish communication with a vehicle).

This document specifies features that are used to detect a vehicle in a network and enable communication with the vehicle gateway as well as with its sub-components during the various vehicle states. These features are separated into two types: mandatory and optional.

This document specifies the following mandatory features:

— vehicle network integration (IP address assignment);

— vehicle announcement and vehicle discovery;

— vehicle basic status information retrieval (e.g. diagnostic power mode);

— connection establishment (e.g. concurrent communication attempts), connection maintenance and vehicle gateway control;

— data routing to and from the vehicle's sub-components;

— error handling (e.g. physical network disconnect).

This document specifies the following optional features:

— DoIP entity status monitoring;

— transport layer security (TLS);

— DoIP entity firewall capabilities.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7498-1:1994, *Information processing systems — Open systems interconnection — Basic reference model*

ISO 13400-3, *Road vehicles — Diagnostic communication over Internet Protocol (DoIP) — Part 3: Wired vehicle interface based on IEEE 802.3*

ISO/IEC/IEEE 8802-3, *Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 3: Standard for Ethernet*

IETF RFC 768, *User Datagram Protocol*

IETF RFC 791:1981, *Internet Protocol — DARPA Internet Program — Protocol Specification*

IETF RFC 792, *Internet Control Message Protocol — DARPA Internet Program — Protocol Specification*

IETF RFC 793, *Transmission Control Protocol — DARPA Internet Program — Protocol Specification*

IETF RFC 826, *An Ethernet Address Resolution Protocol*

IETF RFC 1122, *Requirements for Internet Hosts — Communication Layers*

IETF RFC 2131, *Dynamic Host Configuration Protocol*

IETF RFC 2132, *DHCP Options and BOOTP Vendor Extensions*

IETF RFC 2460, *Internet Protocol, Version 6 (IPv6) — Specification*

IETF RFC 2375, *IPv6 Multicast Address Assignments*

IETF RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

IETF RFC 3484, *Default Address Selection for Internet Protocol version 6 (IPv6)*

IETF RFC 3927, *Dynamic Configuration of IPv4 Link-Local Addresses*

IETF RFC 4291, *IP Version 6 Addressing Architecture*

IETF RFC 4443, *Internet Control Message Protocol (ICMP v6) for the Internet Protocol Version 6 (IPv6) Specification*

IETF RFC 4492, *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)*

IETF RFC 4702, *The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option*

IETF RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*

IETF RFC 4862, *IPv6 Stateless Address Autoconfiguration*

IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*

IETF RFC 8446:2018, *The Transport Layer Security (TLS) Protocol Version 1.3*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 7498-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
diagnostic power mode
abstract vehicle internal power supply state, which affects the diagnostic capabilities of all servers on the in-vehicle networks and which identifies the state of all servers of all gateway sub-networks that allow diagnostic communication

Note 1 to entry: The intent is to provide information to the client DoIP entity about whether diagnostics can be performed on the connected vehicle or whether the vehicle needs to be put into a different diagnostic power mode (i.e. technician interaction required). In this document, the following states are relevant: Not Ready (not all servers accessible via DoIP can communicate), Ready (all servers accessible via DoIP can communicate) and Not Supported (the Diagnostic Information Power Mode Information Request message is not supported).

3.2
DoIP edge node
host (3.4) inside the vehicle, where an Ethernet activation line in accordance with ISO 13400-3 is terminated and where the link from the first node/host in the external network is terminated

[SOURCE: ISO 13400-3:2011, 3.1.2, modified — definition editorially revised.]

3.3
DoIP entity certificate
certificate issued by an *intermediate CA* (3.5)to the DoIP entity presented during the TLS handshake to the client DoIP entity to verify the authenticity of this DoIP entity

3.4
host
node connected to the IP-based network

3.5
intermediate certificate authority
intermediate CA
authority, which issues subordinal certificates to another intermediate CA or DoIP entities

3.6
intermediate certificate
certificate either stored in the client DoIP entity or is presented during authentication together with the end node certificate to complete the chain of trust

3.7
invalid source address
address outside the reserved range for client(s) DoIP entity

3.8
logical address
address identifying a diagnostic application layer entity

3.9
network node
device connected to the IP-based network (e.g. Ethernet) and which communicates using Internet protocol but does not implement the DoIP protocol

Note 1 to entry: Some network nodes might also be connected to a *vehicle sub-network* (3.14), but they are not DoIP gateways as they don't implement the DoIP protocol. Consequently, these network nodes do not interact with (e.g. respond to) DoIP-compliant client DoIP entity.

3.10
root certificate authority
authority, which acts as the root of trust

Note 1 to entry: Typically issues *intermediate certificates* (3.6) to allow an *intermediate CA* (3.5) to further submit certificates.

3.11
root certificate
certificate created by the *root certificate authority* (3.10) and used as the trust anchor

Note 1 to entry: It is securely stored and used by all entities that wants to validate end node certificates (e.g. from the DoIP entity) together with all necessary *intermediate certificates* (3.6) in the chain of trust.

3.12
socket
unique identification, as defined in IETF RFC 147, to or from which information is transmitted in the network

3.13
unknown source address
address not listed in the connection table entry

3.14
vehicle sub-network
network not directly connected to the IP-based network

Note 1 to entry: Data can only be sent to and from a vehicle sub-network through the connecting DoIP gateway.

4 Symbols and abbreviated terms

4.1 Symbols

<d> payload length, given in bytes

<m> number of concurrent DoIP TCP sessions that the client DoIP entity is required to support in order to connect to one or more DoIP entities

<n> number of concurrent DoIP TCP sessions that the DoIP entity needs to support in order to accept 1 to N concurrent connections to one or more items of the client DoIP entity

<u>, <v> number of individual servers in a vehicle sub-network

<w> number of individual DoIP gateways in a vehicle network

<x> number of individual in-vehicle network nodes

<y> number of individual vehicle DoIP nodes in a vehicle network

<z> number of individual vehicle external network nodes

4.2 Abbreviated terms

AL application layer

Alt alternative

APP application

ARP address resolution protocol

ASCII American standard code for information interchange

Auto-MDI(X) automatic medium-dependent interface crossover

CA certificate authority

CAN	controller area network
CF	consecutive frame
DHCP	dynamic host control protocol
DLL	data link layer
DNS	domain name system
DoIP	diagnostic communication over Internet Protocol
EID	entity identification
FF	first frame
FMI	failure mode indicator
GID	group identification
GUI	graphical user interface
GW	gateway
IANA	Internet assigned numbers authority
ICMP	Internet control message protocol
IETF RFC	Internet Engineering Task Force Request for Comments
IP	Internet protocol
IPv4	Internet protocol version 4 (see IETF RFC 791)
IPv6	Internet protocol version 6 (see IETF RFC 2460)
MAC	media access control
MSC	message sequence chart
MTU	maximum transport unit
NDP	neighbour discovery protocol
NL	network layer
OSI	open systems interconnection
PKI	public key Infrastructure
SA	source address
SDU	service data unit
SF	single frame
SPN	suspect parameter number
SPP	service primitive parameter
TA	target address