TECHNICAL SPECIFICATION

ISO/TS 20684-2

First edition

Intelligent transport systems — Roadside modules SNMP data interface —

Part 2: Generalized field device basic management

Systèmes de transport intelligents — Interface de données SNMP pour les modules en bord de route —

Partie 2: A Gestion de base d'ppareil de terrain généralisé

PROOF/ÉPREUVE

Reference number
ISO/TS 20684-2:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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 204, *Intelligent transport systems.*

A list of all parts in the ISO 20684 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

0.1 Background

The need for standardized communication with ITS field devices is growing around the world. Several countries have adopted SNMP-based field device communication standards.

There is a growing view and empirical evidence that standardizing this activity will result in improved ITS performance, reduced cost, reduced deployment time, and improved maintainability. The ISO 20684 series extends ISO 15784-2 by defining the management information necessary to monitor, configure and control features of field devices. The data elements in all parts of the ISO 20684 series may be used with any protocol, but were designed with an expectation that they would be used with one of the ISO 15784-2 protocols.

By using this approach, agencies can specify open procurements and systems can be expanded geographically in an open and non-proprietary manner which reduces costs, speeds up deployment and simplifies integration.

0.2 Overview

SNMP is a collection of well thought-out and well-proven concepts and principles. SNMP employs the sound principles of abstraction and standardization. This has led to SNMP being widely accepted as the prime choice for communication between management systems and devices on the Internet and other communications networks.

The original implementation of SNMP was used to manage network devices such as routers and switches. Since then, the use of SNMP has grown into many areas of application on the Internet and has also been used successfully over various serial communications networks.

This document defines management information for ITS field devices following the SNMP conventions.

0.3 Document approach and layout

This document defines:

a) Conformance tables for this document (Clause 5);

b) User needs that are deemed to be common to many types of field devices (Clause 5);

c) Requirements for implementing the identified user needs, organized by major feature (Clause 6);

d) Design elements that are to be used in implementing the requirements (Clause 7);

e) The management information base (MIB) for the features defined by this document (Annex A);

f) A requirements traceability table that traces requirements to the design elements (Annex B);

g) Encoding examples (Annex C).

In addition, a simplified version of the conformance table and the MIBs are available electronically at https://standards.iso.org/iso/20684/-2.

Intelligent transport systems — Roadside modules SNMP data interface —

Part 2: Generalized field device basic management

1 Scope

Field devices are a key component in intelligent transport systems (ITS). Field devices include traffic signals, message signs, weather stations, traffic sensors, roadside equipment for connected ITS (C-ITS) environments, etc.

Field devices often need to exchange information with other external entities (managers). Field devices can be quite complex necessitating the standardization of many data concepts for exchange. As such, the ISO 20684 series is divided several individual parts.

This part of the ISO 20684 series identifies basic user needs for the management of virtually any field device and traces these needs to interoperable designs. This includes the ability to identify the device, its capabilities, and its status.

NOTE This document is similar to portions of NTCIP 1103 v03 and NTCIP 1201 v03.

ISO 20684-1 provides additional details about how the ISO 20684 series relates to the overall ITS architecture.

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 20684-1:—[1)], *Intelligent transport systems — Roadside modules SNMP data interface — Part 1: Overview*

IETF RFC 2578, *Structure of Management Information Version 2 (SMIv2), April 1999*

IETF RFC 2579, *Textual Conventions for SMIv2, April 1999*.

IETF RFC 2580, *Conformance Statements for SMIv2, April 1999*.

IETF RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, December 2002*

IETF RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), December 2002*

IETF RFC 6933, *Entity MIB (Version 4), May 2013*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 20684-1 apply.

1) Under preparation. Stage at the time of publication: ISO/FDIS 20684:2021.

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/

4 Symbols and abbreviated terms

AC	alternating current
C-ITS	connected intelligent transport systems
I/O	input/output
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITS	intelligent transport systems
MIB	management information base
NTCIP	national transportation communications for ITS protocol
RFC	request for comments
RTM	requirements traceability matrix
SNMP	simple network management protocol

5 Conformance

This conformance section follows the rules defined in ISO 20684-1. Table 1 traces each user need to a set of software features. Table 2 traces each feature to a set of requirements. Table 3 defines terms that are used as predicates in the conformance codes listed in Tables 1 and 2. For a full understanding of these tables and codes, see ISO 20684-1.

Table 1 — User need and feature conformance

Need	Requirement	Conformance
7.1: Monitor the field device		M
	8.1: Field device requirements	M
	8.3: Cabinet	M
7.2: Monitor and control single-value inputs and outputs		O
	8.2: General-purpose I/O	M
7.3.1: Monitor cabinet doors		O
	8.2: General-purpose I/O	M
	8.4: Cabinet doors	M
7.3.2: Monitor and control cabinet fans		O
	8.2: General-purpose I/O	M
	8.5: Cabinet fans	M
7.3.3: Monitor and control cabinet heaters		O

Table 1 *(continued)*

Need	Requirement	Conformance
	8.2: General-purpose I/O	M
	8.6: Cabinet heaters	M
7.3.4: Monitor cabinet humidity		O
	8.2: General-purpose I/O	M
	8.7: Cabinet humidity	M
7.3.5: Monitor cabinet temperature		O
	8.2: General-purpose I/O	M
	8.8: Cabinet temperature	M
7.3.6: Monitor cabinet mains power		0.1 (1..*)
	8.2: General-purpose I/O	M
	8.9: Cabinet mains power	M
7.3.7: Monitor cabinet battery power		0.1 (1..*)
	8.2: General-purpose I/O	M
	8.10: Cabinet battery	M
7.3.8: Monitor cabinet generator power		0.1 (1..*)
	8.2: General-purpose I/O	M
	8.11: Cabinet generator	M
7.3.9: Monitor cabinet solar power		0.1 (1..*)
	8.2: General-purpose I/O	M
	8.12: Cabinet solar power	M
7.3.10: Monitor cabinet wind power		0.1 (1..*)
	8.2: General-purpose I/O	M
	8.13: Cabinet wind power	M

Annex D provides additional user needs that were considered but not included in this document.

Table 2 traces each feature to a set of requirements and defines under what conditions those requirements could be mandatory in order to claim conformance to this document.

Table 2 — Requirement conformance

Feature	Requirement	Conformance
8.1: Field device requirements		
	8.1.2.1: Discover basic capabilities of the field device	M
	8.1.2.2: Discover SNMP capabilities of the field device	M
	8.1.2.3: Configure the field device's identity	M
	8.1.2.4: Identify the field device	M
	8.1.2.5: Identify the SNMP engine	M
	8.1.2.6: Monitor the field device configuration identifier	M
	8.1.2.7: Monitor controller operation	M
	8.1.2.8: Monitor controller up time	M
	8.1.2.9: Monitor watchdog failure count	M
	8.1.2.10: Reset the controller	M
	8.1.3.1: Field device performance requirements	M
	8.1.3.2: Support maximum message size	M

Table 2 *(continued)*

Feature	Requirement	Conformance
	8.1.3.3: Support changeable memory	O.2 (1..*)
	8.1.3.4: Support volatile memory	O.2 (1..*)
	8.1.4.1: Control access	M
	8.1.4.2: Coordinate multiple managers	M
8.2: General-purpose I/O		
	8.2.2.1: Discover general-purpose I/O capabilities	M
	8.2.2.2: Configure general-purpose I/O	M
	8.2.2.3: Retrieve configuration of general-purpose I/O	M
	8.2.2.4: Monitor value from general-purpose I/O port	input: M; bi-directional: M
	8.2.2.5: Monitor status of general-purpose I/O port	M
	8.2.2.6: Monitor status of general-purpose I/O type	M
	8.2.2.7: Control output value of general-purpose I/O port	output: M; bi-directional: M
	8.2.2.8: Confirm output setting for general-purpose I/O port	output: M; bi-directional: M
	8.2.3.1: General-purpose I/O port capabilities	M
8.3: Cabinet		
	8.3.2.1: Configure the cabinet's physical components	M
	8.3.2.2: Identify the cabinet's physical components	M
	8.3.2.3: Determine power source	O
	8.3.3.1.a) Mainline (alternating current) power	ac:M
	8.3.3.1.b) Battery power	battery:M
	8.3.3.1.c) Generator power	generator:M
	8.3.3.1.d) Solar power	solar:M
	8.3.3.1.e) Wind power	wind:M
	8.3.3.2: Support UPS power	O
8.4: Cabinet doors		
	8.4.3.1: Cabinet doors monitored	M
	8.4.4.1: Cabinet doors monitored through general-purpose I/O	M
8.5: Cabinet fans		
	8.5.3.1: Cabinet fans actively monitored	O.3 (1..*)
	8.5.3.2: Cabinet fan control	O.3 (1..*)
	8.5.4.1: Cabinet fans managed through general-purpose I/O	M
8.6: Cabinet heaters		
	8.6.3.1: Cabinet heaters actively monitored	O.4 (1..*)
	8.6.3.2: Cabinet heater control	O.4 (1..*)
	8.6.4.1: Cabinet heaters managed through general-purpose I/O	M
8.7: Cabinet humidity		
	8.7.3.1: Cabinet humidity monitored	M
	8.7.4.1: Cabinet humidity monitored through general-purpose I/O	M
8.8: Cabinet temperature		
	8.8.3.1: Cabinet temperature monitored	M
	8.8.4.1: Cabinet temperature monitored through general-purpose I/O	M
8.9: Cabinet mains power		

Table 2 *(continued)*

Feature	Requirement	Conformance
	8.9.3.1: Cabinet mains power voltage	M
	8.9.3.2: Cabinet mains power current	O
	8.9.4.1: Cabinet mains power voltage monitored through general-purpose I/O	M
	8.9.4.2: Cabinet mains power current monitored through general-purpose I/O	M
8.10: Cabinet battery		
	8.10.3.1: Cabinet battery voltage	M
	8.10.3.2: Cabinet battery current	M
	8.10.3.3: Cabinet battery charge	M
	8.10.4.1: Cabinet battery voltage monitored through general-purpose I/O	M
	8.10.4.2: Cabinet battery current monitored through general-purpose I/O	M
	8.10.4.3: Cabinet battery charge monitored through general-purpose I/O	M
8.11: Cabinet generator		
	8.11.3.1: Cabinet generator voltage	M
	8.11.3.2: Cabinet generator current	M
	8.11.3.3: Cabinet generator engine speed	M
	8.11.3.4: Cabinet generator fuel level	M
	8.11.4.1: Cabinet generator voltage monitored through general-purpose I/O	M
	8.11.4.2: Cabinet generator current monitored through general-purpose I/O	M
	8.11.4.3: Cabinet generator engine speed monitored through general-purpose I/O	M
	8.11.4.4: Cabinet generator fuel level monitored through general-purpose I/O	M
8.12: Cabinet solar power		
	8.12.3.1: Cabinet solar power voltage	M
	8.12.3.2: Cabinet solar power current	M
	8.12.4.1: Cabinet solar power voltage monitored through general-purpose I/O	M
	8.12.4.2: Cabinet solar power current monitored through general-purpose I/O	M
8.13: Cabinet wind power		
	8.13.3.1: Cabinet wind power voltage	M
	8.13.3.2: Cabinet wind power current	M
	8.13.4.1: Cabinet wind power voltage monitored through general-purpose I/O	M
	8.13.4.2: Cabinet wind power current monitored through general-purpose I/O	M

Table 3 provides the formal reference to clauses where the predicates used in Tables 1 and 2 are defined.

Table 3 — External standard reference

Predicate	Clause
ac	7.3.6
battery	7.3.7
bi-directional	8.2.3.1.c
generator	7.3.8
input	8.2.3.1.a
output	8.2.3.1.b
solar	7.3.9
wind	7.3.10

Each requirement specifying a need for a data exchange traces to one dialogue and one or more data elements that an implementation claiming conformance to the requirement shall support. The traceability from requirements to dialogues and data elements is defined in the Requirements Traceability Matrix (RTM) as contained in Annex B. Annex B may include references to dialogues and data elements defined in other documents; any locally defined dialogues shall be defined in the body of the standard while all data elements shall be defined in accordance with Annex A of this document using a Management Information Base (MIB) conforming to the format defined in IETF RFC 2578.

If the implementation supports SNMP, all supported data element instances (i.e., SNMP objects) shall be accessible via any dialogue that meets the requirements of SNMP and the data element definition.

NOTE The dialogues defined in this document are specified to promote a common interface for testing purposes and are not intended to restrict otherwise allowable requests or notifications.

6 Architecture

6.1 General

This document defines data for management and control of roadside field devices. Figure 1 depicts the physical view of this interface using the graphical conventions defined by the architecture reference for cooperative and intelligent transportation (ARC-IT, http://arc-it.net) and also documented in ISO 14813-5:2020, Annex B.

The manager of the field device is shown in grey indicating that it can be any type of physical object, such as a central system, another field device, a maintenance laptop or any other device that supports the defined interface.

The field device is shown in orange, indicating that it is located in the field (e.g. along the roadside). It shall have a connection to the manager and may have any number of connections to other ITS-S or external systems.

The figure indicates two information transfers between these physical objects. The first is the "configuration and commands" information flow from the manager to the field device. The second is "status and notifications" information flow from the field device to the manager. Both flows are shown in green indicating that authentication is required and both are shown with a single arrowhead indicating a unicast transfer.

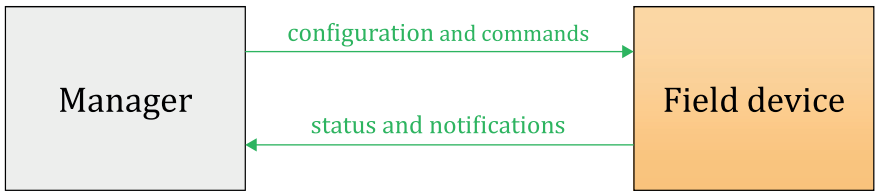

Figure 1 — Physical view of interface

6.2 Architecture reference

This document addresses technical details identified within the Harmonised Architecture Reference for Technical Standards (HARTS). The scope of this architecture is described at http://htg7.org/html/analysis/servicepackages.html.

6.3 Functional view of interface

This document is concerned with defining the data concepts used to manage a field device. The scope of this document does not define the logic used to manage the field device or the protocols used to exchange the defined data elements. However, the data concepts defined in this document have been defined with the assumption that they would be exchanged using an SNMP-like interface.

6.4 Physical view of interface

This document addresses interfaces between a “field device” and the physical objects that can potentially manage it, typically “centres” and other “field device” objects. Specific information flows considered within the scope of this document include:

— device identification: information used to initialize, configure, and control the field device.

This document also defines other flows as deemed necessary during the development of detailed designs.

6.5 Communications view of interface

6.5.1 Overview

This document addresses the data within the application and management entities of the ITS-S architecture reference model as depicted in Figure 2.

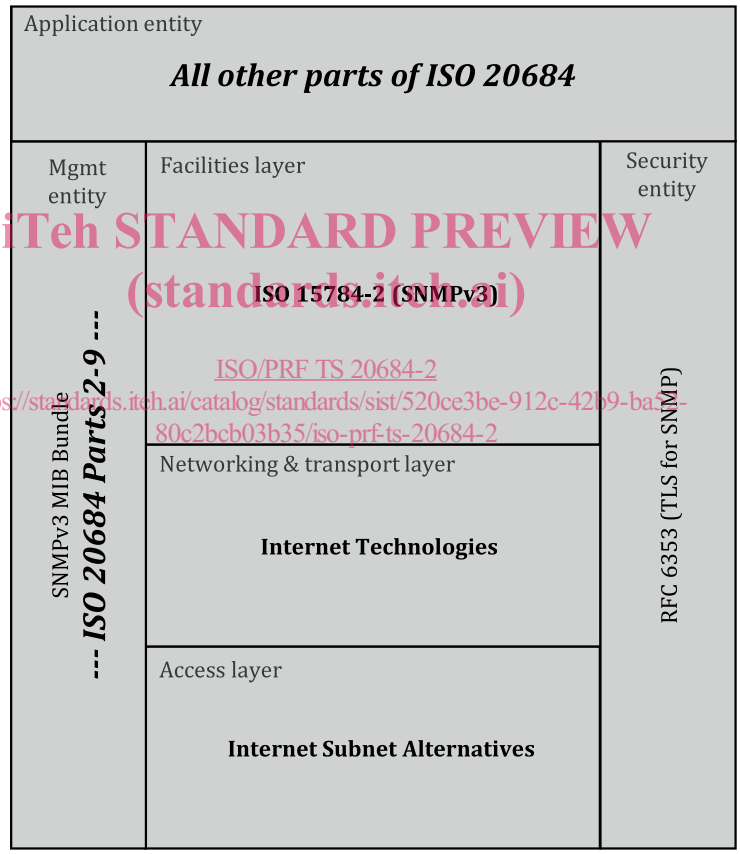

Figure 2 — Communications view of interface

6.5.2 Security and data protection

Authentication and authorization are dependent on Datagram Transport Layer Security (DTLS)/ Transport Layer Security (TLS) coupled with either X.509 or IEEE 1609.2 certificates. Encryption can be provided as needed using any encryption method with a registered OBJECT IDENTIFIER.