TECHNICAL SPECIFICATION

ISO/TS 20684-6

First edition
2022-09

Intelligent transport systems — Roadside modules SNMP data interface —

Part 6: Commands

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

Partie 6: Commandes

Reference number
ISO/TS 20684-6:2022(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 Simple Network Management Protocol (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 defined in all parts of 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) the conformance requirements for this document (Clause 4);

b) a set of user needs for user-defined trigger conditions that can “fire” to initiate actions (Clause 5);

c) a set of detailed requirements for the identified user needs (Clause 6);

d) security considerations for the information defined in this document (Clause 7);

e) the management information bases that define the data for the defined requirements (Annex A);

f) the requirements traceability matrix (RTM) that traces the requirements to the design elements (Annex B).

Intelligent transport systems — Roadside modules SNMP data interface —

Part 6: Commands

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 document specifies the user needs, requirements and design elements that are used to issue an SNMP set-request in response to a trigger firing. This allows a manager to configure the field device to implement simple responses to conditions in the field.

NOTE 1 There are similarities between certain portions of the Event MIB defined in IETF RFC 2981 and this document.

NOTE 2 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 20684-1:2021, *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*.

3 Terms and definitions

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

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

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

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

4 Conformance

This clause 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. For a full understanding of these tables and codes, see ISO 20684-1.

Table 1 — User need and feature conformance

Need	Requirement	Conformance
5.1: Issue trigger-based commands		M
	6.1: Command factory	M
	20684-7 6.5: SNMP target	M
	20684-7 6.6: SNMP target parameters	M

Table 2 — Requirement conformance

Feature	Requirement	Conformance
6.1: Command factory		
	6.1.2.1: Determine command factory capabilities	M
	6.1.2.2: Configure a command factory	M
	6.1.2.3: Verify command factory configuration	M
	6.1.2.4: Retrieve command factory statistics	M
	6.1.2.5: Retrieve command factory status	M
	6.1.2.6: Toggle a command factory	M
	6.1.2.7: Delete command factory	M
	6.1.3.1: Size of variable bindings list	M
	6.1.3.2: Issue a command	M

5 User needs

5.1 Issue trigger-based commands

5.1.1 Automatically respond to user-defined exceptions user need

A manager needs to be able to configure a field device ("field manager") to send a command to a remote field device ("target") when user-defined conditions are detected by the field manager. This will allow the field manager to alter the state of other devices (targets) in response to exceptional conditions in a timely manner without burdening the communications channel between the centre and field location.

NOTE The field manager and target can be the same field device.

EXAMPLE A manager wants to configure a field manager to automatically display a message whenever ice is detected on the roadway.

5.1.2 Automatically respond to user-defined exceptions overview

5.1.2.1 Required features

In the simplest case, the “automatically respond to user-defined exceptions” user need shall support the following features.

a) A mechanism to trigger the command factory to generate a command. For example, this functionality can be provided by the trigger, as specified by ISO/TS 20684-3.

b) A command factory, as defined by this document, which defines details about the command(s) to be generated when the event occurs.

c) An SNMP target, as specified by ISO/TS 20684-7 and RFC 3413, which defines the SNMP agent to which the command should be sent. It may also be used to identify a remote device from which to obtain data used in the trigger logic.

d) SNMP target parameters, as specified by ISO/TS 20684-7 and RFC 3413, which defines the parameters used to communicate with the SNMP target.

5.1.3 Graphical relationships

The relationships among these features are depicted in Figure 1.

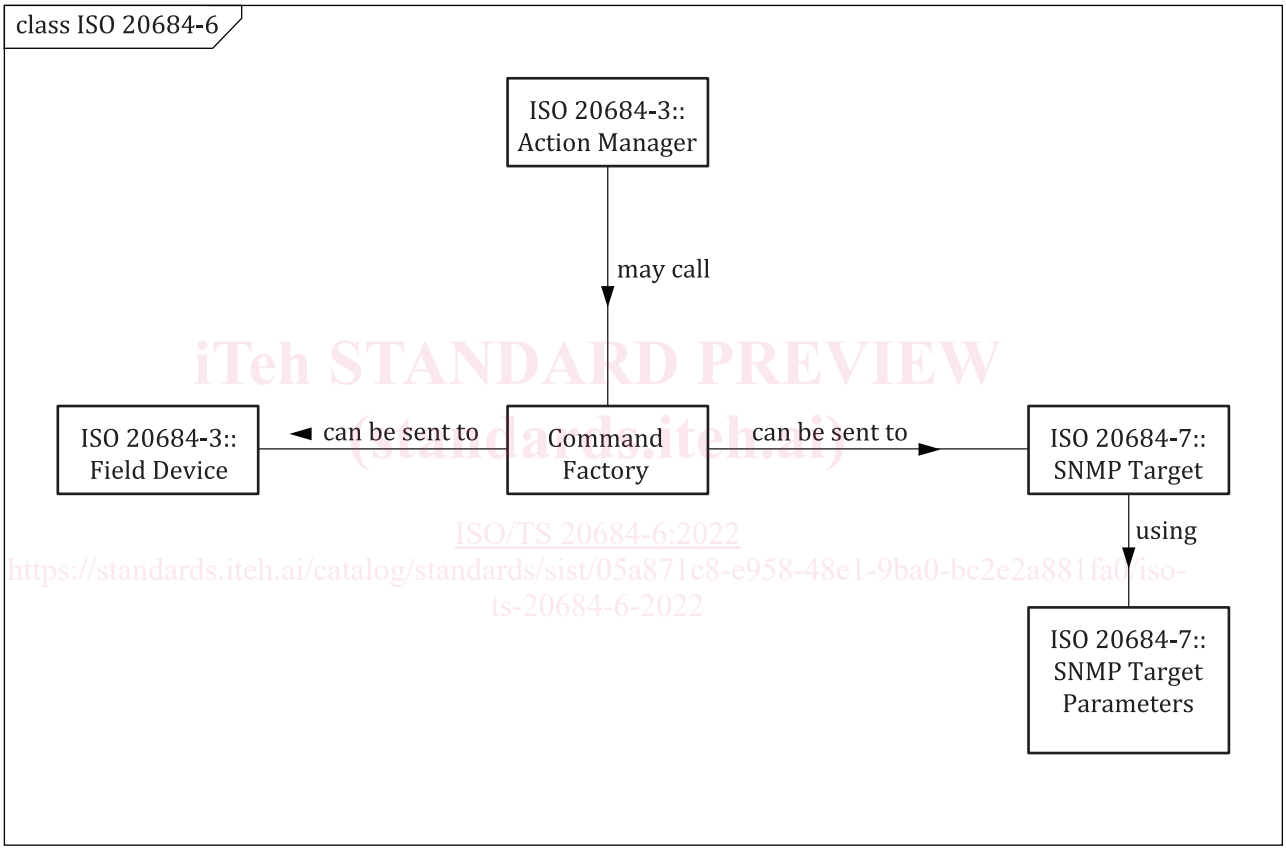

Figure 1 — Conceptual overview of commands

The mechanism by which the command factory is called is outside the scope of this document, but it is possible for it to be called by an entry in the fdActionTable, as specified in ISO/TS 20684-3.

When the command factory is called, the field manager sends the configured SNMP set request to the identified SNMP target using the configured SNMP target parameters.

6 Requirements

6.1 Command factory

6.1.1 Command factory definition

The command factory generates a SET request for a target when activated. The target may be the host field device or a remote field device.

6.1.2 Command factory data exchange requirements

6.1.2.1 Determine command factory capabilities

The field device shall allow a manager to determine the maximum size (number of octets) allowed for the variable binding list associated with any fdCommandFactoryEntry.

6.1.2.2 Configure a command factory

The field device shall allow a manager to configure the command and the target(s) to which the command should be sent along with a description for the entry.

6.1.2.3 Verify command factory configuration

The field device shall allow a manager to verify the configuration of a command factory.

6.1.2.4 Retrieve command factory statistics

The field device shall allow a manager to retrieve statistics about the issuance of commands by the command factory.

6.1.2.5 Retrieve command factory status

The field device shall allow a manager to retrieve the status of the command factory.

6.1.2.6 Toggle a command factory

The field device shall allow a manager to toggle the enabled status of a command factory.

6.1.2.7 Delete command factory

The field device shall allow a manager to delete a command factory configuration.

6.1.3 Command factory capability requirements

6.1.3.1 Size of variable bindings list

The field device shall support a variable binding list of at least 64 octets for each supported command.

6.1.3.2 Issue a command

The field device shall transmit a Set Request to the associated target, using the associated SNMP target parameters, each time the command factory is called (e.g. due to logic defined in ISO/TS 20684-3).

7 Security vulnerabilities

There are data elements defined in this document with a MAX-ACCESS clause of read-write and/or read-create. These and other data elements are sensitive and need to be protected from malicious and inadvertent manipulation and/or disclosure. The support for requests in a non-secure environment without proper protection can have a negative effect on network operations. A sampling of the vulnerabilities includes:

a) the ability to change when commands are sent;

b) the ability to delete commands;

c) the ability to create additional commands; and

d) the ability to monitor current configurations.

To overcome these vulnerabilities, it is highly recommended that SNMPv3 with TLS support, as defined in RFC 6353, is used to exchange the data.