TECHNICAL SPECIFICATION

ISO/TS 20684-4

First edition
2022-10

Intelligent transport systems — Roadside modules SNMP data interface —

Part 4: Notifications

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

Partie 4: Notifications

Reference number
ISO/TS 20684-4:2022(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) a set of custom dialogues for notification management (Clause 7);

e) security considerations for the information defined in this document (Clause 8);

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

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

Intelligent transport systems — Roadside modules SNMP data interface —

Part 4: Notifications

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 needs, requirements and design for the field device to send notifications to one or more managers. It relies upon the definition of triggers as defined in ISO/TS 20684-3.

NOTE 1 There are similarities between certain portions of NTCIP 1103 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*

ISO/TS 20684-7:2022, *Intelligent transport systems — Roadside modules SNMP data interface — Part 7: Support features*

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*

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. 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
5.1.1: Real-time notifications user need		
	6.2: Notification channel	M
	6.3: Notification event	M
	6.4: Notification factory	M
	6.5: Notification packet	M
	20684-7 6.5: SNMP target	M
	20684-7 6.6: SNMP target parameters	M
	6.1: Notification aggregator	O
	20684-7 6.4: Object group	O

Table 2 — Requirement conformance

Feature	Requirement	Conformance
6.1: Notification aggregator		
	6.1.4.1: Aggregating logic	M
	6.1.4.2: Sending aggregated notifications	M
6.2: Notification channel		
	6.2.2.1: Determine notification channel capabilities	M
	6.2.2.2: Configure a notification channel	M
	6.2.2.3: Verify notification channel configuration	M
	6.2.2.4: Retrieve notification channel statistics	M
	6.2.2.5: Clear notification channel queue	M
	6.2.2.6: Delete a notification channel	M
	6.2.2.7: Toggle enabled status for all notifications	M
	6.2.2.8: Send notifications to target	M
	6.2.3.1: Notification packet size	M
	6.2.4.1: Process incoming data	M
	6.2.4.2: Sending non-queueable notifications	M
	6.2.4.3: Sending queueable notifications	queue:M
	6.2.4.4: Adding messages to the notification queue	queue:M
6.3: Notification event		
	6.3.2: Notification event contents	M
	6.3.3: Maximum data size	M
	6.3.4: Timestamp latency	M
	6.3.5: Timestamp resolution	M
6.4: Notification factory		
	6.4.2.1: Determine notification factory capabilities	M
	6.4.2.2: Configure a notification factory	M
	6.4.2.3: Verify notification manager factory	M

Table 2 *(continued)*

Feature	Requirement	Conformance
	6.4.2.4: Retrieve notification factory statistics	M
	6.4.2.5: Retrieve notification factory status	M
	6.4.2.6: Toggle notification factory	M
	6.4.2.7: Delete notification factory	M
	6.4.3.1.1: Support for unacknowledged notifications	M
	6.4.3.1.2: Support for acknowledged notifications	O
	6.4.3.2.1: Support for non-queueable notifications	M
	6.4.3.2.2: Support for queueable notifications	O
	6.4.3.3.1: Support for non-aggregated notifications	M
	6.4.3.3.2: Support for aggregated notifications	O
	6.4.4: Generate a notification	M
6.5: Notification packet		
	6.5.2.1: Retrieve last notification contents	M
	6.5.3: Notification packet contents	M
	6.5.4.1: Maximum packet size	M
	6.5.4.2: Maximum number of events	M

Table 3 — External standard reference

Predicate	Subclause
queue	6.4.3.2.2

5 User needs

5.1 Monitor user-defined exceptions in real-time

5.1.1 Real-time notifications user need

When user-defined triggers fire, a manager needs to receive real-time notifications containing user-defined information. This will allow a manager to immediately become aware of information that can potentially affect its operation or security without burdening the communications channel with frequent polling for data that seldom changes. Multiple triggers can need to be monitored with different systems being notified based on the type of condition.

EXAMPLE 1 A manager wants to be immediately notified when the cabinet door opens so that an appropriate response can be initiated if the access is unauthorized.

EXAMPLE 2 A manager wants to have the maintenance system notified when the cabinet door opens and have the traffic management system notified when a new message is displayed on a sign.

5.1.2 Monitor user-defined exceptions in real-time overview

5.1.2.1 Required features

In the simplest case, the “real-time notifications” user need shall support the following features

a) A mechanism to call a specific notification factory to generate a new notification event. This document is written based on the assumption that the call will be made by one of the mechanisms specified in ISO/TS 20684-3, which may conclude with a specific action calling a specific notification factory, but this document does not prohibit calling a notification factory by other mechanisms.

b) Notification factory, as defined in this document, which specifies details about the specific notification event and the type of notification packet that should be used to send the notification event.

c) Notification event, which represents the information to be reported to a manager when a call is made to the notification factory.

d) Notification packet, as defined in this document, which represents the contents of a single SNMP notification message, which contains one or more notification events. There are four types of notification packet: one-off traps (not acknowledged), one-off informs (acknowledged), aggregated traps and aggregated informs.

e) Notification channel, as defined in this document, which constructs, manages, and transits notification packets.

f) SNMP target, as specified in ISO/TS 20684-7 and RFC 3413, which defines the SNMP manager to which the notification channel should send notification packets.

g) SNMP target parameters, as specified in ISO/TS 20684-7 and RFC 3413, which define the parameters used to communicate with the target.

5.1.2.2 Aggregate notification option

An implementation may support the notification aggregator, as defined in this document, which manages the aggregation of individual notification events into a single notification packet. Without this feature, all notification packets contain a single notification event and are passed to the notification channel immediately.

5.1.3 Graphical relationships

The relationships among these features are depicted in Figure 1.

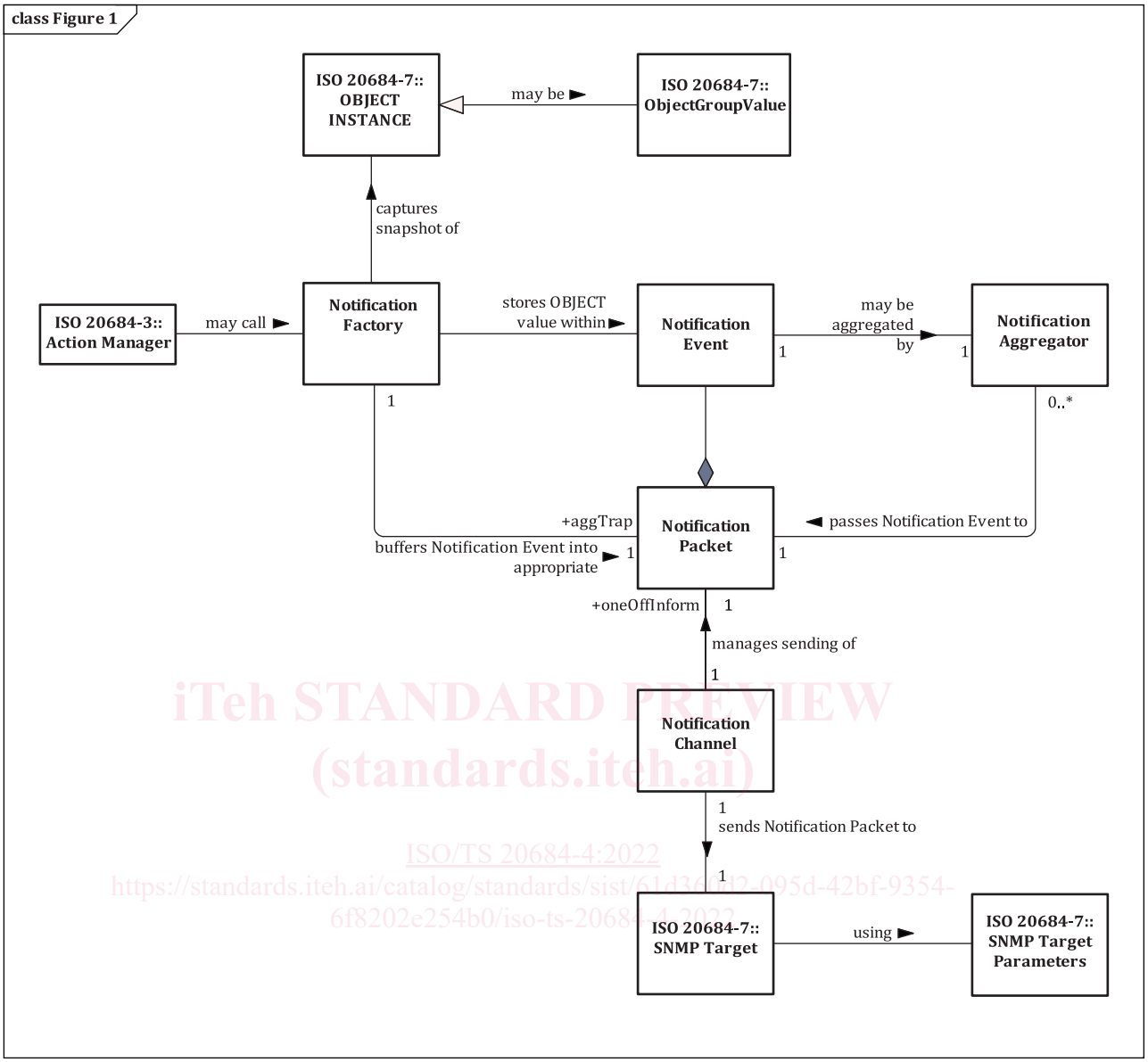

Figure 1 — Conceptual overview of notifications

When a trigger (specified in ISO/TS 20684-3) fires, it calls an action (ISO/TS 20684-3), which may direct the call to the notification factory. When called, the notification factory captures the current value of a specified object and stores this value in a notification event data structure along with an identifier of the condition that initiated the event and timestamp. The object value recorded may be an fdCompositeObjectValue (ISO/TS 20684-7), which can package the values of multiple subordinate objects in a compressed format. The notification factory then passes the Notification Event to the notification channel along with information about how the notification event is to be handled. Multiple notification factories may use the same notification channel.

If the notification event is flagged for aggregation, it is passed to the notification aggregator; otherwise the notification channel assigns the notification event to an appropriate one-off notification packet based on the rules defined in 6.1.4.1.

The optional notification aggregator combines notification events into a single notification packet, which serves to reduce overall communications overhead. The notification aggregator conceptually manages two aggregate notification packets: one that requires acknowledgements (i.e. an SNMP inform) and another that does not (i.e. a SNMP trap). Notification events from different notification

factories can be combined into a single notification packet. Once a notification packet is completed, it is sent back to the notification channel for transmission to the target.

Once a notification packet is ready to send, the notification channel sends the notification packet to the SNMP target while ensuring that the anti-streaming rate is not exceeded, which allows temporary queueing of notifications so that they do not overwhelm the communications channel.

Finally, as per the rules of SNMPv3, trap messages are unacknowledged and inform messages are acknowledged. The acknowledgement process is handled according to standard SNMPv3 rules (complete with timeout and retry logic).

6 Requirements

6.1 Notification aggregator

6.1.1 Notification aggregator definition

The notification aggregator combines multiple notification events into a single packet to reduce overall communication overhead.

6.1.2 Notification aggregator data exchange requirements

No data exchange requirements are defined for the notification aggregator.

6.1.3 Notification aggregator capability requirements

There are no explicit capability requirements for the notification aggregator.

6.1.4 Notification aggregator logic

6.1.4.1 Aggregating logic

Each notification channel shall be associated with its own notification aggregator. The notification aggregator shall store acknowledged and unacknowledged notification events in separate buffers. The aggregation logic for each buffer is independent of the other, but identical as follows.

a) If the number of events in the selected buffer (before adding the new event) is equal to or greater than the maximum configured value, the notification aggregator shall immediately send the aggregated notification according to the rules of 6.1.4.2 and then proceed to proceed to step c) of this subclause. If the number of events is zero (0) the logic proceeds to step c). If the number of events is greater than zero but less than the maximum configured value, the logic proceeds to step b).

b) The notification channel shall determine the length of a serialized notification packet containing the new notification event. If the length of the message exceeds the length of the maximum notification size, the notification aggregator shall immediately send the aggregated notification (omitting the new event) according to the rules of 6.1.4.2 and then proceed to proceed to step c) of this subclause. Otherwise, the logic simply proceeds to step c).

c) The notification aggregator shall add the new notification event to the selected buffer.

d) The notification aggregator shall update its local maximum number of events to aggregate to be the lesser of the previous value and the value associated with the new event.

e) If the number of notification events in the selected buffer (including the newly added event) is equal to or greater than the current local maximum, the notification aggregator shall immediately send the aggregated notification (including the new event) according to the rules of 6.1.4.2; the