TECHNICAL SPECIFICATION

**ISO/TS 18625**

First edition
2017-10

# Freight containers — Container Tracking and Monitoring Systems (CTMS): Requirements

*Conteneurs de fret — Système de suivi et de surveillance : Exigences*



Reference number
ISO/TS 18625:2017(E)



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

# 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 on 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 the following URL: www.iso.org/iso/foreword.html.



This document was prepared by Technical Committee ISO/TC 104, *Freight containers*, Subcommittee SC 4, *Identification and communication*.



 

# Introduction

Through communication with a broad range of potential Container Tracking and Monitoring System (CTMS) users, much has been learned about needed capabilities and the timeline for providing certain solution levels. Initially, it was assumed that the most immediate needs would be for high-tier (i.e. high-capability) solutions to protect dangerous or valuable cargoes. Potential users made clear that point solutions for dangerous or valuable cargoes have already been developed for these needs. These point solutions are in use today. Instead, the most immediate potential demand seems to be for "low-tier" solutions that deliver a minimal but important capability at low cost, capable of being broadly deployed and used. Starting at the low tier reflects a building block approach that can be expanded as technology and requirements permit.

This document summarizes the aforementioned discussions. This document provides a systemic approach for automatic identification, tracking and monitoring for freight containers. Specifically, it provides guidance for the requirements (operational and otherwise) for a system, and its enabling devices, used to track, monitor and/or report the status of the container according to the needs, requirements and specifications determined by the user. The CTMS would provide

a) an unambiguous unique identification of the container,

b) location of the container with a selectable degree of precision as defined by the user of the system (there are various options for accuracy and it is left to the user to determine what is best for the application), and

c) status, where applicable, of container condition parameters as defined by the user of the system which may include parameters related to container environment, container condition, container integrity, container load status, etc.



The collection of this information is done through one or more selectable communications interfaces. The format, frequency and granularity in which the information is accessed and presented will be defined by the user of the system and is outside the scope of this document.



Though not used in this document, recognition is given to the standardization work of

— ISO/IEC JTC 1/SC 31 in the area related to air interface, data semantic and syntax construction, conformance and identification, location and security of items,

— ISO/IEC/TR 24729-4, and

— ISO/TC 104 in the area of freight container security, including electronic seals [(e-seals) ISO 18185 (all parts)] and container identification.

# Freight containers — Container Tracking and Monitoring Systems (CTMS): Requirements

## 1 Scope

This document is intended to be applicable to freight containers as defined in ISO 668 as well as to other freight containers not defined in ISO 668 and to container ancillary equipment such as road and terminal chassis, generator sets and power packs.

This document provides guidance for the requirements (operational and otherwise) for a system, and its enabling devices, used to track, monitor and/or report the status of the container, hereinafter referred to as the Container Tracking and Monitoring System (CTMS). The use of a CTMS is optional. The party opting to use a CTMS is hereafter referred to as the "user of the system" or just the "user". The user, which can be, e.g. a shipper, a consolidator, a logistics service provider or a container owner or operator, will identify and specify its specific requirements and usages of the CTMS pursuant to specific use cases defined by that party (see Clause 6). This document establishes a tiered approach to the CTMS. The tiered approach is described in 5.2 and 5.3.

A CTMS in conformance with this document, provides for interoperability in regard to both data transfer and data interpretation neither of which may be hindered by systems claiming such conformance.



The CTMS elements addressed in this document include the following:

a) a set of requirements for transferring information to and from a container tracking device to/from an automatic data processing systems by, e.g. air interface through RF or optical means;



b) data for transmission to/from automatic data processing systems;

c) functional requirements necessary to ensure consistent and reliable operation of the CTMS;

d) features to inhibit malicious or unintentional alteration and/or deletion of the information content of the CTMS.

Specifically excluded from the scope of this document is the processing and display of data by the users' information system hereinafter referred to as the Operator Information Management system (OIMS). Also specifically excluded is the specific identification, tracking and monitoring of cargo packed or filled in the container.

## 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 17712, *Freight containers — Mechanical seals*

ISO 18185-2, *Freight containers — Electronic seals — Part 2: Application requirements*

ISO 18185-3, *Freight containers — Electronic seals — Part 3: Environmental characteristics*

ISO/IEC 19762, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

IEC 60533, *Electrical and electronic installations in ships — Electromagnetic compatibility (EMC) — Ships with a metallic hull*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 and ISO 17712 apply.

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

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

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

## 4 Abbreviated terms

BLE Bluetooth Low Energy

CTD Container Tracking Device

CTMS Container Tracking and Monitoring System

EMI Electro-magnetic Interference

FCL Full Container Load

IMO International Maritime Organization

OIMS Operator Information Management system

NFC Near Field Communications

RFI Radio Frequency Interference

RFID Radio Frequency Identification

SOLAS Safety of Life at Sea Convention



## 5 General information

### 5.1 System architecture

A CTMS architecture is comprised of the following components shown in Figure 1:

a) a tag or device attached to or an integral part of the container and referred to as a Container Tracking Device (CTD);

b) Tag-to-Reader Interface and Tag-to-Tag Interface (air or wired interface) that can be, e.g. an RF or an optical connection between the CTD and Reader;

c) readers (transceivers) — a device for collecting information from the tag or CTD, e.g. a reader located away from the freight container, cell towers, satellite system, optical readers, smart phone, etc.;

d) Operator Information Management system (OIMS). The OIMS could be any user or provider system that accepts data from the CTMS.

The CTMS consists of both permanent and removable container-carried tracking devices (CTDs) with various levels of capability and a variety of infrastructure elements with which CTDs communicate. Some tag technologies can communicate with each other as data transfer nodes. The reader communicates with the tag to read or write data and interface to the back-end OIMS. Both the CTD-to-CTD and CTD-to-reader involve the air interface protocols.

The data generated in or collected by the CTMS, which can include video and pictures, shall be transferrable to the OIMS, labelled as item 4 in Figure 1. The configuration of the information system

 

depends on the CTD sophistication, e.g. if encryption is a feature of the CTD, then the key management might be conducted at the OIMS level to communicate with the CTD. The primary focus in this document will be the elements of the CTMS, which are labelled as 1 to 3. There are numerous standards on how information systems are configured and secured.

For the purpose of this document, the only recommendation is a basic set of data elements that would have value to any user. However, data elements beyond those defined in this document may be needed. This document does not define a data format to allow standardization in parsing the data elements provided to the OIMS; such definition would be the purview of an international standard proper.

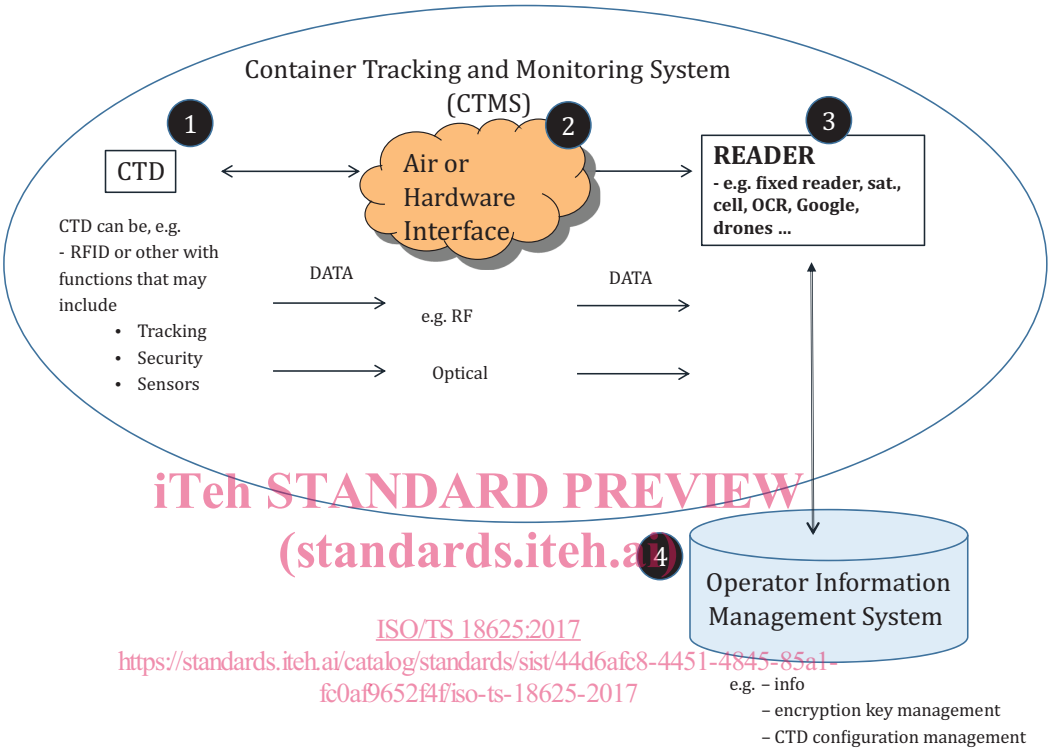




**Figure 1 — System level architecture components for CTMS**

## 5.2 System functions

CTDs will exist at different levels ("tiers") of capability to be matched to the needs of specific container journeys as defined by the user. These tiers allow for consistent categorization and matching of the features of a CTD and a CTMS. The tiered structure is shown in Figure 2.

The container-installed (or container-carried) CTD incorporates an inherent identification and — except for Tier 0 — a location-finding capability, and may also include the ability to monitor one or more container sensors. For example, a sensor could include detection of door openings on the container, temperature within the container, humidity, and /or shock or vibration that the container experiences. (For Tier 0, the CTMS would infer the location from the reader that collected the data from a Tier 0 CTD). The CTMS is capable of reporting identification, location and container sensor status, if so equipped, using one or more communication modes. Higher level tiers have functions of the lower level tiers. Tiers 1 and 2 have the ability for add-on sensors and memory as optional inputs and storage. It is up to the users to determine the appropriate tier and any add-on capabilities.

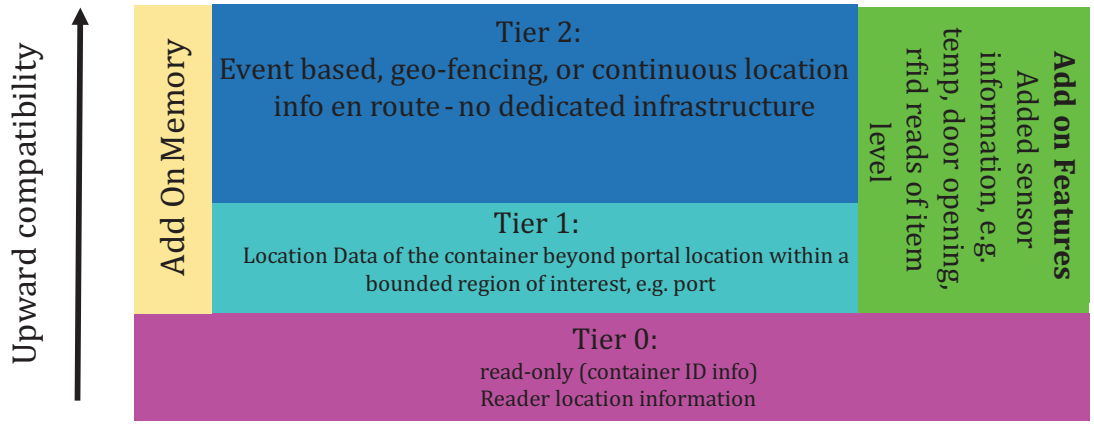


**Figure 2 — Tiered approaches to CTMS**

## 5.3 System operation

A container-installed (or container-carried) CTD is activated at the initial or subsequent container packing ("stuffing") point or when a Full Container Load (FCL) is realized. Initialization (activation) of the CTD is a user-defined event. The CTD at the lowest level provides a container ID and will, when communicating with a reader, provide a location associated with that reader. Higher level CTDs can have sensors and may provide location along the container journey. A higher Tier CTD can be programmed to report on a fixed or event-driven schedule or, alternatively, can be directed to report only when interrogated. Some CTDs will be capable of reporting via multiple media types and can be programmed to access media in a prioritized order. A Tier 1 or Tier 2 CTD may have the ability, if monitoring door openings or any other sensor, to clear events. For example, a CTD with a door opening sensor that is activated at the start the container journey, which will be consolidated at difference locations ("milk run"), can accept authorized inputs to allow for door openings without triggering an alert.



The CTMS tiers defined capabilities are:

a) Tier 0:

   1) maintaining the integrity of the freight container identification and other permanent related information;

   2) transmitting information using the appropriate interface protocol in a form suitable to the reader;

   3) being physically, electronically and radiographically secure and tamper-proof;

   4) being able to determine location of the reader and thus the tag at the time of information transfer;

   5) operating within the environmental conditions described in ISO 18185-3;

b) Tier 1:

   1) the capability of Tier 0;

   2) providing location data from the tag (but not necessarily in real time);

c) Tier 2:

   1) the capability of Tier 1;

   2) reporting without a reader using technologies such as satellite or cell phone;

3) utilizing geo-fencing;

4) integrating multiple sensors;

d) Optional add-on sensor:

1) integrating with Tier 1 to 2 CTDs

2) utilize IEEE 802.15.4-2006 and ISO/IEC IEEE 21451-7 protocols where applicable or other suitable protocols for the maritime environment

e) Optional memory capacity:

1) integrating with Tier 1 to 2 CTDs;

2) storing data to meet the requirements of the Tier in use to include read/write capability.

## 5.4 System interfaces

The CTMS, as shown in Figure 1, has multiple interfaces that include but are not limited to sensor to Tier 1 or 2 device, CTD to Reader; and Reader to OIMS. Devices used in CTMS are existing units that utilize existing protocols. Interfaces may be wired or air interfaces as appropriate. The system interfaces follow standard protocols that are appropriate for the mode of information delivery from the CTD to the reader to OMIS through various media types, e.g. RF, optical transmission, and data protocols. The system architecture refers to air interface and data protocols required to import into an OIMS without specifying them.



## 5.5 System data management



OIMS data management is at the discretion of the user. Data from the device to the infrastructure can be transmitted via different media types and shall be done in a standardized manner. The data also needs to be in a consistent format going into the OIMS. The development and use of an Application Programming Interface (API) for this purpose is strongly recommended. Transmission from the OIMS to other information systems is dependent on application and user needs and is outside the scope of this document. This document does not define a data format to allow standardization in parsing the data elements provided to the OIMS; such definition would be the purview of an international standard proper.

## 5.6 System data safeguard measures

Sensitive data may be exchanged/processed/saved by the CTMS. Data can be considered sensitive for a variety of reasons, including national security (e.g. data related to unauthorized access, public safety), content security (e.g. protection of high-value or pilferable cargoes), and business intelligence (e.g. identity of customers, cargoes, routing). All elements of the CTMS shall contribute to overall security. Data is most vulnerable when being transmitted (within wireless or wired networks) although close control of processing and data storage are also important.

Data vulnerabilities are further complicated by the allowed flexibility of communications media. The CTMS approach is not inventing new communications solutions; it is merely using known, deployed communication choices to move data. In an operational scenario, the system user's choice of communication media, pursuant to their needs and requirements, are driven by the media's performance (range and throughput), cost and ability to protect the information sent.

Since the system is required to live within the inherent security capabilities of the available media, additional security may, at the user's discretion, be included through processes such as encryption and authentication.

Additional information about system and device security can be found in ISO/IEC 29167 (all parts) and in 6.2 and 7.3.