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.

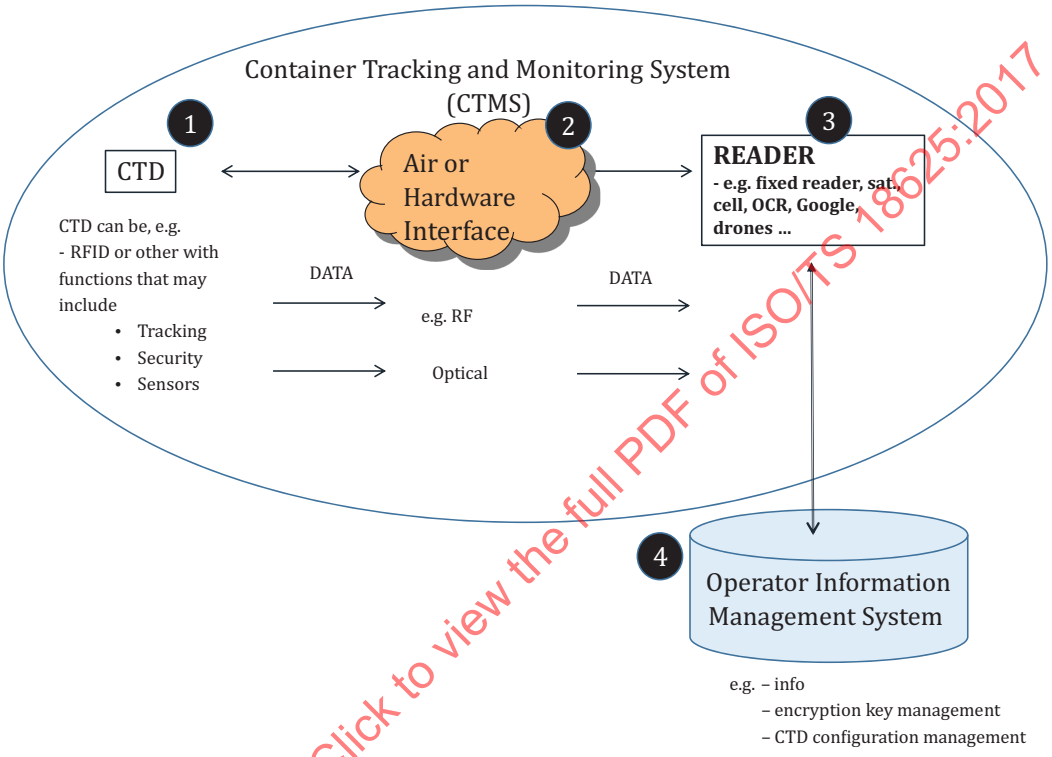

Figure 1 — System level architecture components for CTMS

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.

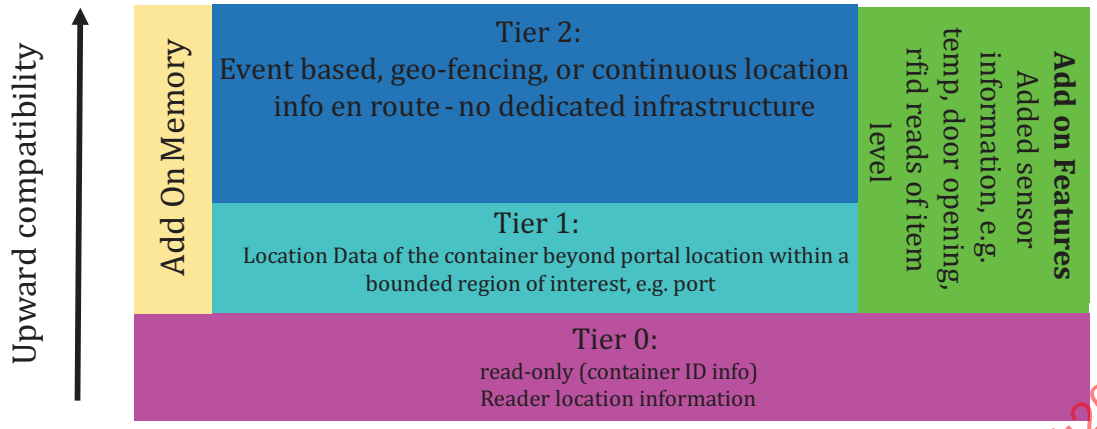

Figure 2 — Tiered approaches to CTMS

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.

5.7 System levels of performance

Flexibility is a defining characteristic of the CTMS. Not all containers, cargoes, and routes require the same degree of tracking and monitoring (if applicable). The CTMS is configurable to apply a level of tracking and monitoring capability in accordance with the user requirements while transferring all resulting information to an OIMS.

The CTMS architecture accommodates variability in both tracking (technology used, precision of measurement, device connectivity, time between fixes, etc.) and, if applicable, monitoring (sensor count, individual sensor characteristics, measurement precision, sensor connectivity, etc.) Theoretically, this variability can result in a large number of capability combinations; however, a study of operational scenarios leads to a reasonable subset of combinations to serve as system design points. These levels of performance are defined in 5.3 as tiers within the whole CTMS architecture.

The tiered approach can be applied to various characteristics of CTMS applications. The three primary areas are communications (types and capabilities), breadth of other (non-communication) capabilities, and depth of those capabilities. These are discussed in 5.8 to 5.10.

5.8 Communications

5.8.1 General

Various types of communication are needed within the CTMS concept to move information between sensors and CTDs, CTDs and Readers, and Readers and OIMS (and potentially back to the CTD). Three specific communication media are broadly discussed here: RFID, cellular and satellite communications (sitcom). These are clearly very different media, having very different capabilities and costs. This is not all-inclusive and does not address optical or hardwired means of communication.

5.8.1.1 RFID

RFID (including, but not limited to, active, passive, NFC, and BLE) is already broadly used in transportation, mostly for road tolling, traffic management, access control and inventory management. It uses an RF tag (transponder) applied to the tracked item and it communicates over relatively short ranges that vary with transponder capability and a (generally) fixed local infrastructure. Its relatively short communication range means that it is used primarily in controlled environments (like ports and terminals) where containers are assured to be near the appropriate infrastructure. Its strongest benefit is the relatively moderate costs involved. Many RFID devices do not require a power source (i.e. batteries) at all so there is no costly maintenance activities required.

5.8.1.2 Cellular

Cellular communications are well-known and ubiquitous. The obvious advantage of this media choice is that the infrastructure (cell towers) is already in place, covers the majority of populated areas and can move information effectively. Balancing this have some disadvantages: the installed devices require batteries or another power source which, in addition to costs, also raises maintenance issues, airtime also has a cost which may vary according to the periodicity and amount of information transmitted, and there are still numerous dead zones in the cellular coverage (e.g. between population centres, below decks and in some warehouses).

5.8.1.3 Satcom

Satellite communications is truly an anytime-anywhere medium, which is its biggest advantage. The infrastructure (satellites) is in place. But the installed devices are power-hungry, which result in costs and maintenance issues, and airtime has a high cost (limiting the amount of data that is practical/affordable to send). Line-of-sight limitations also apply.

5.9 Breadth of capability

Breadth of capability refers to whether or not a CTD has a specific capability. For example, does it have on-board user memory? Or does it have the capability to interact with add-on sensors, etc.? Numerous other capabilities are possible, including the ability to include remote programming and/or activating of the CTD, geo-fencing, and control over reporting functions and frequency.

5.10 Depth of capability

Depth of capability refers to the performance of an available capability. Just as there is a significant difference between devices without or with a certain capability, there can be a significant difference between devices with low vs high levels of that capability. For example, if a device is defined to have on-board memory, does it have a few bytes of memory, kilobytes of memory or gigabytes of memory? Or if a device is defined to have the capability to accept sensor inputs, can it accept one input, five inputs, ten inputs or even infinite inputs via a mesh scheme?

6 CTMS system requirements

6.1 Operational scenarios

6.1.1 General

The CTMS is designed to support operational scenarios involving the transportation of freight containers. However, to develop the system and specify its operating capabilities and levels of performance, the user of the CTMS needs to identify the system requirements.

A user with a relatively simple freight container supply chain (for example, one container once a week from the same shipper to the same consignee using the same transport service providers) can easily identify the nodes in the container journey where data collection from the CTD shall occur. There can be occasions when, in addition to whichever location information is needed, monitoring data from any container add-on sensors may be required.

A user with complex freight container supply chains with different types of cargoes and using many different transport service providers in various transportation modes may not as easily be able to identify typical container journeys with their attendant tracking and, if applicable, monitoring requirements. In these latter cases, it is recommended that the user, in order to identify the requirements of the CTMS and the required level of performance, does the following:

a) identifies a generic container journey;

b) breaks this journey into its constituent segments;

c) for each segment, identifies those events where the user sees a need for

   — location information, and determines at which level such information is needed, and

   — monitoring information and, if such information is needed, determines at which level and with which content it is needed.

This recommended approach is referred to as the “Event Library” and is described in more detail in 6.1.2.

6.1.2 “Event Library”: Journey segments and associated events

The generic freight container journey can be broken into the following segments:

a) journey initiation;

b) drayage;

c) marine terminal handling;

d) rail terminal handling;

e) storage/transfer yard;

NOTE The events for this segment is similar for either the marine terminal events (e.g. barge and domestic shipping) or the rail terminal events (transfer from rail to truck and *vice versa*). Therefore, Annex A does not describe the events for this segment.

f) marine transit;

g). rail transit;

h) long-haul road transit;

i) Journey termination.

6.1.3 For each journey segment, the user may develop a list of events that are associated with the use of a CTMS. For example, for the "journey initiation", the segment of the list of events might be as follows:

Event Library #1: Journey initiation

— Device is associated to specific container.

— Device is configured for specific journey.

— Device is associated to a bill of lading.

— Other user data which might include cargo information.

— Container and device are associated to conveyance.

— Container and device are associated to a generator set (genset) when installed.

— Report reefer/tank parameter status.

— Report mounting of CTD.

— Activate the CTD.

— Report location of container.

— Report packed vs empty.

— Report doors closed.

— Report doors sealed.

— Report container sensor status.

— Report first movement.

Annex A includes the list of possible events for each of the segments of the generic freight container journey.

6.2 Specific system requirements

6.2.1 General

The decision to select a particular CTD shall consider basic system requirements to include physical, environmental, performance, and operational parameters.

6.2.2 Physical/structural requirements

Physical requirements include the physical constraints and features for the equipment and storage of raw /processed data, physical security needs, power requirements, number of units, weight of units, colour of units, and finish requirements. The CTD shall not interfere with or reduce the useful cargo volume of the container. The CTD shall be installed in a fashion that does not degrade the original structural or environmental integrity of the container as defined by ISO standards for various shipping container types.

6.2.3 Environmental requirements

Examples of environmental requirements include, but are not limited to, temperature, shock, humidity, and vibration, pressure extremes, dust, salt spray, water immersion, RFI/EMI susceptibility, etc. All elements of the CTMS shall survive in their intended environment. Environments on the exterior of the container are as defined in ISO 18185-3. Some elements may be designed to mount exclusively on the interior of a host container and, in those cases, a reasonable relaxation is possible of environmental requirements related to direct exposure to the marine environment. Any environmental testing shall be conducted based on physical location and usage in and of the container. If the container is part of the device, e.g. mounted inside, then the conditions of ISO 18185-3 shall be applied to the CTD and the container as a system.

6.2.4 Operational and performance requirements

Operational requirements include security issues and approvals, the procedure and number of people required to input data and manage/maintain the database and distribution, the procedure for users to access the data, reliability, maintainability, etc. The performance requirements would include how quickly data can be moved through the process from start to finish, how much data can be handled, accuracy of the data stored, the type of data stored and retrievable, data products that will be available to the user, etc.

6.3 Readability

6.3.1 General

The CTMS' reading capability differ according to the tier of the CTD (see 5.2 and 5.3 for the tier concept).

For CTDs at Tier 0, the system should be capable of reading the CTD in all of the operational scenarios identified in ISO/TS 10891. These scenarios are essentially limited to portal locations with only a minimum of at least 5 m read distance. A Tier 0 device could not be read in many of the events in Annex A. Localization may not be supported in all the scenarios. In situations where localization is not possible, the CTMS shall have a system level capability to establish the relationship between a CTD and the container onto or in which it is affixed.

For CTDs at Tier 1, the system should be capable of reading the CTD in all of the operational scenarios identified in ISO 18185-2. These scenarios involve portal locations as well as certain bounded areas, e.g. parts of a port or rail terminal but not the entire terminal, with variable read distances at variable speeds. A Tier 1 device might not be read in several of the events in Annex A. Localization might not be supported in all the scenarios. In situations where localization is not possible, the CTMS shall have a system level capability to establish the relationship between a CTD and the container onto or in which it is affixed.

For CTDs at Tier 2, the system should be capable of reading the CTD in all of the operational scenarios discussed in Annex A. A Tier 2 device should be read in all of the events in Annex A. Localization shall be supported in all the scenarios.

6.3.2 Container monitoring

CTDs at Tiers 1 and 2 may, in addition to an inherent location finding capability, include the ability to monitor one or more container attributes. Whether the CTD shall include monitoring capabilities and, in the affirmative, what such monitoring capabilities shall be, will be defined by the user of the CTMS.

One of the container sensors to be monitored could be detection of breaches of the container integrity, either detection of container door openings and/or detection of breaches of the container walls. In either scenario, the user defined threshold requirement for detection of breaches would need to be established, e.g. more than x cm movement of the container door from its closed position or holes in the container wall wider than xx cm^2.

For any container attribute monitoring, the CTD would need to trigger an event status. For example, such event status messages may be triggered if any of the following events occur:

— door opening event;

— pre-set internal temperature limit exceeded;

— self-test failures;

— low battery.

The latter event implies that the CTD would have the ability to monitor battery life. The battery life requirement could be expressed in hours or days, e.g. 1 680 hours (or 70 days) which is the minimum under operational loads and environments, or it could be further qualified with a pre-defined number of interrogations per day for a container trip lasting, for example, 70 days.

Other relevant requirements would include data storage for alerts and queries, memory storage media and size, and operational availability.

6.4 Accuracy and reliability of the CTMS

ISO/TS 10891 and ISO 18185-2 contain requirements for accuracy (99,99 %) and reliability (99,998 %); however, more analysis needs to be conducted to establish the specific requirements for the CTMS architecture (see Figure 1).

Requirements that need to be determined could include the following:

— a user-defined/configurable false alarm rate where a false alarm is defined as an alarm generated when conditions did not warrant an alarm (false positive); or when no alarm was generated when conditions did warrant an alarm (false negative);

— a probability of detection, defined as the accurate detection of sensor functions;

— a GNSS accuracy, defined as the accuracy within a range that provides location of the container.

6.5 Data

Table 1 shows a notional set of data elements. Other data elements might apply at a higher tiers and sensor functionality may be used at the discretion of the CTD user. The items in pink will be part of all tiers.

Table 1 — CTD Container ID data and values

Data	Value		Unit representation	Notes
	Minimum	Maximum		
Tag manufacturer ID	—	—	Alphanumeric	From ISO/IEC 15963 or ISO/IEC 7816-6
Tag type	00	99	Numeric	ISO/TS 10891
Tag location code	A	Z	Alphabetic	From ISO/TS 10891
Owner code	AAA	ZZZ	Alphabetic	ISO 6346
Equipment category identifier	U, J, or Z	—	6 Alphabetic	ISO 6346
Serial number	000000	999999	Numeric	ISO 6346
Check digit	0	9	Numeric	ISO 6346
Size and type code	00/AA	99/ZZ	Alphanumeric (4 characters)	ISO 6346
Max gross mass (kilograms)	00000	99999	Numeric	ISO 6346
Tare mass (kilograms)	00000	99999	Numeric	ISO 6346
Data routing	—	—	—	Used as an identifier for routing data from a CTD to an OIMS
GNSS location	—	—	Numeric (NMEA Standard GPRMC message)	—
Sensor error bits	—	—	—	Only available if sensors are used.
Time Stamp — UTC	—	—	—	—
Extendibility flag	0	1	Numeric	—

7 Container Tracking Device (CTD)

7.1 General device information (variety/range of devices)

The central element of the CTMS is a Container Tracking Device (CTD). The CTMS will, at any Tier (level), have an inherent location-finding capability, but the characteristics of this capability will increase significantly for CTDs at Tiers 1 and 2. CTDs at these latter two tiers may also include the ability to monitor one or more container attributes.

Whether the CTD shall include monitoring capabilities and, in the affirmative, what such monitoring capabilities shall be, will be defined by the user of the CTMS. Because of the tier approach used in this document, the CTD may take numerous forms and come in many varieties, spanning from RFID tags to sensors to built-in features of the container structure.

7.2 Device installation/mounting

The CTD can, if it is not built into the container, be mounted on or in the container as long as the physical requirements in 6.2 are met. The CTD shall be able to be installed with common tools within a reasonable amount of time to not disrupt the flow of the supply chain.

7.3 General device functions for security

As described in 5.6, security is both a basic requirement and a function of the CTMS solution. The security function is based on providing status about a container's physical security (if the container is so equipped). Examples of physical security include door openings, breach detection, geo-fencing,

etc. as defined by the CTD owner/operator. Container types, security-related monitoring/reporting mechanisms and user requirements related to security vary widely, but a few generalities are obvious. Monitoring (and reporting) of container security nearly always require a higher-level communication device. Security monitoring generally requires the ability to accept/process sensor inputs. A power source is likely needed. The level to which security is important defines a tier of capability and flow down to define many operational needs of any security monitoring solution.

Additionally, there is data security which can be achieved by the use of encryption and techniques such as authentication prior to and during data transfer. Initial work in security of RFID data is covered in ISO/IEC 29167 (all parts), which describe options for encryption and authentication.

8 Infrastructure elements

8.1 General

The on-board CTMS element(s), i.e. CTDs (including any sensor elements present), shall be able to provide information to an OIMS via infrastructure-based communications. Many CTD-to-infrastructure communication choices are possible, but any specific journey or journey segments will likely favour one choice over another based on cost and operational requirements. Some devices may be capable of communicating via multiple modes, with programmed logic controlling the order in which modes are accessed.

For the three communication choices described in 5.8, the infrastructure elements are quite different. RFID requires a (generally) user-installed infrastructure, consisting of RFID readers at choke points or portals where containers (with CTDs) will pass closely. Current RFID readers (or at least their antennas) need to be located no more than a few tens of metres from CTDs for passive devices and no more than a few hundreds of metres from CTDs for active devices. For cellular communications, the fixed infrastructure (cell towers) is provided by the cellular carriers, but prior arrangements need to be made to get information from the cellular network to the OIMS. For satcom communications, the infrastructure are the satellites and ground stations, but again, the information shall be able to flow smoothly to the OIMS.

8.2 Data interface(s)

Regardless of the infrastructure used, data/information, as defined by the user, shall be routed to the OIMS. Data entering this system shall consist of compliant data elements conforming to a compliant element arrangement. Since information may (probably will) be coming from a variety of sources over a variety of media paths and contain a variety of data elements (according to the application needs and the media capabilities), it is very important to have a carefully controlled interface at the boundary of the OIMS. Data formats between the CTMS and the OIMS is beyond the scope of this document but will need to be addressed in an appropriate standard underpinning the OIMS.

The identification of the OIMS to receive the data feeds is critical if the CTMS is to achieve even minimal success. Identification of the communication address of the OIMS shall be available and transmitted in a standard format.

8.3 Other infrastructure elements (any other non-device distributed elements)

Other infrastructure elements may be incorporated as part of any specific CTMS implementation. There has been no attempt to create standards for other elements, although user input may eventually provide a reason to do so.

9 Safety and regulatory considerations

CTMS compliant with this document, including their CTDs and readers, shall meet safety requirements for power, duty cycle and electromagnetic radiation. In addition, such tags and their readers shall comply with the relevant safety requirements, including those that apply for radio frequencies.

With respect to sources of ignition [as stated in Regulation 19 Chapter II-2 of the International Maritime Organization (IMO)'s Safety of Life at Sea (SOLAS) Convention], electrical equipment and wiring shall not be fitted in enclosed cargo spaces or vehicle spaces unless it is essential for operational purposes in the opinion of the Administration. However, if electrical equipment is fitted in such spaces, it shall be of a certified safe type for use in the dangerous environments to which it may be exposed unless it is possible to completely isolate the electrical system (e.g. by removal of links in the system, other than fuses). Cable penetrations of the decks and bulkheads shall be sealed against the passage of gas or vapour. Through runs of cables and cables within the cargo spaces shall be protected against damage from impact. Any other equipment which may constitute a source of ignition of flammable vapour shall not be permitted.

With respect to electromagnetic compatibility, CTMS compliant with this document shall comply with IEC 60533.

Annex A
(informative)

Event library

A.1 The following is a detailed description of an event library. This description is not intended to be all inclusive but is representative of what potential CTMS users have identified to this point.

A.2 The list of possible events comprising the generic journey stated in 6.1 is repeated here for ease of reference.

The generic freight container journey can be broken into the following segments:

a) journey initiation;

b) drayage;

c) marine terminal;

d) rail terminal or storage/transfer yard

NOTE The events for this segment is similar for either the marine terminal events (e.g. barge and domestic shipping) or the rail terminal events (transfer from rail to truck and *vice versa*). Therefore, this annex combines events for this segment.

e) marine transit;

f) rail transit;

g) long-haul road transit;

h) journey termination.

A.3 Event library #1: Journey initiation

— Device is associated to specific container.

— Device is configured for specific journey.

— Device is associated to a bill of lading.

— Other user data which might include cargo information.

— Container and device are associated to conveyance.

— Container and device are associated to genset when installed.

— Report reefer/tank parameter status.

— Report mounting of CTD.

— Activate the CTD.

— Report location of container.

— Report packed vs empty.

— Report doors closed.