DCSA IoT data standard for remote Reefer container monitoring on board a vessel

December 17, 2020
Version 1.0

In short

This standard defines a minimum set of required data elements to be shared with the vessel crew to enable remote monitoring of smart Reefer containers on board a vessel, as well as a definition of the related IoT infrastructure objects.

Table of contents

Tables

Figures

Preface

DCSA envisions a digitally interconnected container shipping industry. DCSA's mission is to drive technology standards and frameworks that will enable carriers to bring innovative solutions to market. Our mission is to be the de facto standards body for the industry, setting the technological foundation for interoperable IT solutions. Together with our member carriers, DCSA creates vendor-neutral, technology-agnostic standards for IT and non-competitive business practices. By working towards the widespread adoption of these standards, our aim is to move the industry forward in terms of customer experience, efficiency, collaboration, innovation, and respect for the environment.

Smart containers that leverage IoT connectivity standards will usher in a new era of efficiency, transparency, and innovation in global trade. Interoperable smart container solutions will provide customers and carrier operational teams worldwide with relevant information on container (contents) status and whereabouts both at sea and on land.

The objective of the DCSA IoT Program (P2) is to secure investments in smart container tracking devices by ensuring connectivity and data exchange interoperability for the defined use cases across different versions of devices and vendors.

The IoT program deliverables aim to:

- Ensure long term availability and consistency of data to drive visibility and improve the customer experience.
- Enable all carriers to maximise operational and commercial benefits from this new technology.
- Ensure basic device security and access to data by defining minimum standards.

This publication is focused on data sharing to strengthen the container shipping industry's ability to send and receive data across industry participants. Furthermore, it aims to enable remote monitoring of Reefer containers on board a vessel. Ideally, this language will be inspired by existing standards and aligned with the industry process definitions put forth in the DCSA Glossary of Terms 2.0.

The standards published by DCSA are technology agnostic. DCSA does not point to the use of specific vendors' technologies or systems but relies on open-source shared requirements for the industry that can be used by all parties, regardless of the choice of technology.

Please refer to the DCSA website, https://dcsa.org/about/ for more information.

Legal disclaimer

This document

This document is a publication of the DCSA IoT Program. It focuses on the data to be exchanged to enable the Use Case: remote Reefer container monitoring on board a vessel. The aim of this standard is to ensure that relevant data captured from smart Reefer containers is shared with relevant parties (e.g., vessel crew) in a standardised fashion to enable remote monitoring on board a vessel.

Defining the minimum required set of Reefer container data elements is an important building block for interoperability and collaboration between stakeholders, which will provide better service to end users in a more efficient manner.

This document is supported and complemented by a range of supplementary DCSA publications. The supporting publications are:

DCSA Glossary of Terms 2.0

- The glossary is used to support the reader with definitions and explanations of the business terms used in DCSA documents. It ensures that all readers interpret the terms in the same way.

DCSA IoT Release 1: Standard for Gateway Connectivity Interfaces

- The first publication of the DCSA IoT Program, developed to ensure interoperability at the gateway radio interface level between IoT solutions deployed by the various supply chain participants in the shipping industry. In this document referred to as "IoT Release 1" or "Release 1".

Basic Terminology

In this document:

- The use of MUST is equivalent to REQUIRED and SHALL, indicating that it is an absolute requirement.
- MUST NOT is equivalent to SHALL NOT and indicates that it is an absolute prohibition of the specifications.
- SHOULD is equivalent to RECOMMENDED, meaning that there are valid reasons to ignore a particular requirement, but the implications need to be weighed.
- REQUIRED is equivalent to MANDATORY, meaning in this context that the given data element is an absolute requirement.

Terms, acronyms, and abbreviations

This list is not ordered alphabetically.

Term	Definition
Thermal container	Generic term for an Insulated container that may or may not be mechanically refrigerated. Insulated freight container having insulating walls, doors, floor and roof designed to delay the rate of heat transmission between the inside and the outside of the container (3.1 ISO 1496-2:2018)
Container refrigerating system	System that enables refrigeration of a container within the required temperature range, also known as Reefer Engine, Reefer Machinery or Integral Refrigeration Unit. Mechanically refrigerated container with a vapor compression refrigeration cycle using refrigerant as a working fluid (3.5 ISO 20854:2019).
Reefer container	A refrigerated container, or Reefer, is a sea container used in intermodal freight transport that is refrigerated for the transportation of temperature-sensitive cargo. The Reefer has an integral refrigeration unit (Reefer engine) which is powered by an external source (Reefer Power Supply). This can be a Reefer plug at the terminal or on board a vessel, or a genset when transported by truck or rail. A Reefer container has a data logger to record the temperature and the various physical parameters. The Reefer container is used to transport perishable cargo in a controlled atmosphere. The Reefer has a variety of sensors and a Reefer controller unit. Reefer containers are mainly used to maintain the temperature of the cargo. In addition to the temperature, dehumidification and ventilation settings should be controlled and measured. Some cargo, such as flower bulbs, require controlled humidity. In such cases, refrigeration units can regulate humidity. Thermal container served by a unit using a means of cooling such as liquefied gases, with or without evaporation control (ERU) (3.2 ISO 1496-2:2018).
Reefer controller unit	The Reefer controller unit is composed of a keypad that gives access to all necessary control settings to operate the Reefer container as well as the screen for viewing the different sensor measurements. The Reefer controller unit is used to set the desired physical parameters that meet the needs of the cargo being loaded and to display the sensor measurements, the different alarms (if any), and other technical data.

Term	Definition
Container IoT Device	An IoT device installed on the container. It has the purpose of establishing communication between the container, internet, gateways, other IoT devices and/or sensors placed within the perimeter or inside the container. Its main function is to act as an interface between multiple sensors/other IoT devices on the container and the network or IoT gateway. This should not be confused with IoT devices placed on specific container cargo/packages/loads. (DCSA Glossary of Terms 2.0). With the addition of a Container IoT Device, a regular container becomes a *Smart Container*. In this document, a Reefer without IoT device is referred to as a *non-smart Container.*
IoT Gateway	Physical devices that act as a connectivity intermediary between multiple IoT container solution devices, IoT internet platforms and /or local systems of the IoT Network Supporting Infrastructure. Which is an IoT Gateway or group of IoT Gateways that are deployed in a specific area to enable connectivity capabilities and coverage for IoT endpoints such as IoT container devices, IoT internet platforms and/or local systems (DCSA Glossary of Terms 2.0).
DCSA compliant IoT infrastructure	IoT infrastructure that is compliant with the DCSA standards.
Reefer Power Supply	Condition where a connection to the three-phase power supply is present (3.24 ISO 20854:2019).
Reefer Fresh Air Vent	Adjustable orifice to allow a supply of outside air into a mechanical refrigeration container.
Reefer Alarm System	System constituting all electrical and electronic parts of the refrigerating system that monitor the correct function of the protective device(s) and/or give a warning in case of malfunctioning or refrigerant leakage (3.1 ISO 20854:2019).
Reefer Controlled Atmosphere	Modified atmosphere system installed in a thermal container served by a refrigeration unit, capable of generating and/or maintaining gas concentration levels different to those of the air outside the container (3.6 ISO 1496-2:2018).
Vessel Crew	The vessel crew represent the vessel operator on board the ship. Vessel crew are responsible for ensuring that the internal temperatures of refrigerated

Term	Definition
	containers (or Reefers) are correctly maintained during the sea passage and while in port. In addition, they must be able to tell the exact number of all types of containers—full and empty—loaded on the vessel at any time. In case of an alarm (coming from the Reefer alarm system), they must take corrective action. Today, the crew must walk throughout the entire vessel to check manually whether each Reefer is working correctly (UNECE: ECE/Trade/446).
Cargo Probe	Is a type of probe that was originally requested by the United States Department of Agriculture (USDA). It is a probe that is inserted into the merchandise and used by the authorities to determine if the merchandise is at the right temperature.

Table 1: Terms, acronyms & abbreviations

References

The documents listed below constitute the normative and non-normative references for the DCSA data exchange standards for remote Reefer container monitoring on board a vessel.

Normative references

The following referenced documents are taken into consideration and necessary for this publication.

- DCSA Glossary of Terms 2.0
- DCSA IoT Release 1: Standard for Gateway Connectivity Interfaces

Non normative references

The following referenced documents are non-normative external non-binding documents that might be useful.

- ISO 20854:2019 Thermal containers — Safety standard for refrigerating systems using flammable refrigerants — Requirements for design and operation
  This document describes the design of the mechanical refrigeration unit (MRU) and operation of container refrigerating systems in all anticipated operational modes and locations.
- ISO 1496-2:2018 Series 1 freight containers — Specification and testing — Part 2: Thermal containers
  This document gives the basic specifications and testing requirements for ISO series 1 thermal containers for international exchange and for conveyance of goods by road, rail, and sea, including interchange between these forms of transport.
- ISO 10368:2006 Freight thermal containers — Remote condition monitoring
  This document establishes the information and interfaces required to permit complying central monitoring and control systems employed by one carrier or terminal to interface and communicate with complying remote communication devices of differing manufacture and configuration used by other carriers and terminals.
- SMDG code lists
  SMDG has agreed to publish and maintain the following codes lists for the benefit of all interested parties available at http://www.smdg.org/smdg-code-lists/
- [ECE/Trade/446] UNECE (2019) The UNECE Trade Facilitation White Paper on Real-time Smart Container data for supply chain excellence.
  available at https://www.unece.org/index.php?id=53347
  This paper provides a detailed look into the various benefits of using Smart Containers as well as the various potential use cases for this technology.

1 Introduction

This section details the objective of the release and the general information that applies to the whole release document.

1.1 Objective

The objective of this release is to describe the "remote Reefer container monitoring on board a vessel" use case and to define the required minimum set of data elements to be shared with the vessel crew. Three data categories are defined to be able to classify the IoT data elements as public, semi-private and private data.

Remote monitoring is feasible when using IoT container devices that are able to collect data from the Reefer controller units, process it and send these data elements to local servers and applications on board a vessel via the gateways on board a vessel.

1.2 Smart Containers potential benefits

The UNECE Trade Facilitation White Paper on Real-time Smart Container data for supply chain excellence (ECE/Trade/446) provides an overview of the various benefits of using Smart Containers for the different logistics chain stakeholders including for Reefer container monitoring by the vessel crew. This white paper highlights that Smart Containers may play a role in enhancing the operations on board vessels by enabling the crew to remotely monitor the temperature of the Reefers and to ensure that the engines of the Reefers are running correctly. Early alerts will enable the vessel crew to take mitigating actions to attempt to save the cargo instead of discovering damaged cargo after the fact (e.g. upon delivery to the BCO). In addition, thanks to Smart Container solutions, the vessel crew will be able to compare remotely, in a timely manner, and at any time during the voyage, the total number of full and empty containers aboard the vessel to substantiate the numbers originally loaded according to the stowage plan.

1.3 Use Case value proposition

Defining the minimum set of required data to be shared with the vessel crew to enable remote Reefer monitoring on board a vessel is an important building block for interoperability and collaboration between stakeholders. Automation of the Reefer monitoring process is key to minimising human error and increasing operational efficiency while providing better service to end users. In addition, the vessel crew will be able to focus on exceptional cases, which will minimise the amount of manual labour they must perform.

1.4 Building on IoT Release 1

The DCSA IoT Release 1 "Standard for Gateway Connectivity Interfaces" defined a range of physical connectivity interfaces to be used as communication channels in support of IoT devices across different domains. Building on this, the document at hand defines the data standard for remote Reefer container monitoring on board a vessel. By utilising the standardised gateway interfaces, a range of data-centric use cases are enabled, hereunder the operationalisation of remote monitoring of Reefers. The flow of data from point of inception into onboard servers and applications allows the vessel crew to perform remote Reefer container monitoring.

Note. The physical radio interfaces specified in Release 1 will serve as an enabler to wirelessly communicate Reefer data on board a vessel. Whereas other legacy communication infrastructure such as Power Cable Transmission (PCT, see ISO:10368) might continue to function as an additional means to collect Reefer data.

1.5 Structure of this document

The structure of this document is as follows:

- Section 1: Introduction and objective of this standard
- Section 2: Description of the current (non-IoT) process
- Section 3: Description of the Use Case, process description and user stories
- Section 4: Description of the prerequisites and detailing of the data elements
- Section 5: Standard adoption guidelines
- Section 6: Conclusion

1.6 Conformance

All shipping lines are encouraged to implement and follow the remote Reefer container monitoring on board a vessel-related data requirement outlined and specified in this document.

2 Generic process for current (non IoT based) Reefer monitoring on board a vessel

This section introduces the Reefer container monitoring on board a vessel use case by detailing the process as it is currently performed.

2.1 Overall process description

Among their multiple duties, vessel crew have the responsibility to monitor whether the Reefers are working correctly on board a vessel during the vessel journey. Whenever the Reefer is not working properly, the vessel crew must do their best to take corrective action as per mutual agreements between the Reefer operator and the vessel operator.

Currently, the vessel crew must regularly walk down to each Reefer to check its parameters and make sure it is functioning properly to ensure the cargo transit is carried out with minimum product quality loss. This is a time-consuming, manual, and repetitive task which requires physical effort and has an increased risk for human error. For some special Reefer containers with high value cargo or health-related products (e.g., vaccines or blood plasma), efficient monitoring of temperature stability is crucial. These containers come with stringent instructions requesting frequent monitoring and reporting.

Reefer containers are embedded with an array of sensors that are connected to the Reefer controller unit. Vessel crew must check whether the controller unit of the Reefer container loaded on the vessel is properly connected to the power supply and working properly (e.g., no alarms have been raised and all displayed measurements are within the desired parameters). Whenever a Reefer raises alarms, the vessel crew must take corrective action where possible. Otherwise, the vessel crew must report the malfunctioning as soon as possible to concerned parties as identified in the voyage information. Either the Reefer container is repaired on board or it is discharged at the next port.

2.2 Step by Step process description

Once the Reefer container is loaded on the vessel, vessel crew must execute the following steps as part of the proper boarding and handling of the Reefer containers (see also Figure 1):

Step 1: Inspect the Reefer container and plug it in manually, whenever this is required.

Step 2: Check whether the Reefer engine is running (ON/OFF?).

Step 3: Check and compare the current Reefer settings entered via the Reefer Controller Unit with the requested settings (e.g., cargo temperature set point) as defined in the Cargo documentation (e.g., Cargo Manifest).

Step 4: Check for the presence of active alarms.

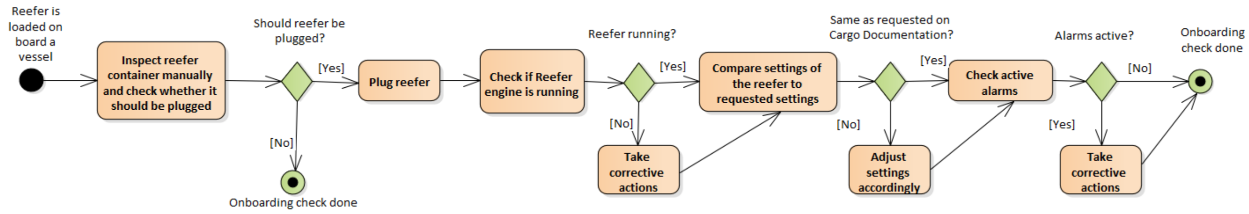

Figure 1: Initial Reefer container monitoring activity diagram

Periodically, the vessel crew must check the following and act accordingly (see also Figure 2).

Step 1: Check whether the Reefer engine is running (ON/OFF?).

Step 2: Check whether the Reefer container measurements are in range of requested settings.

Step 3: Check the existence of active alarms? If yes - check further and act accordingly.

a. Controller model/type
b. Operating mode
c. Cargo to assess the sensitivity and urgency

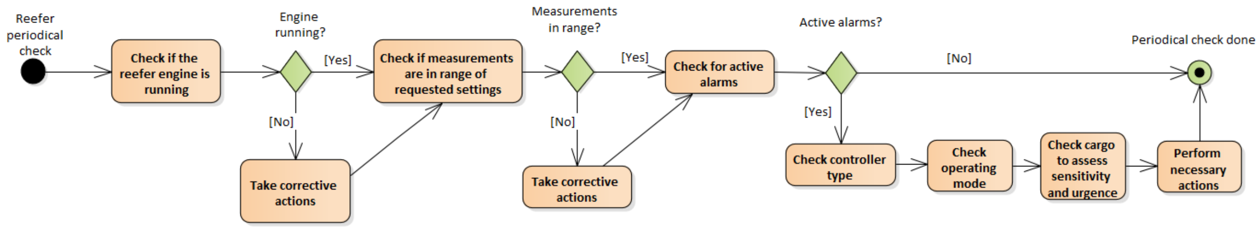

Figure 2: Periodical Reefer container monitoring activity diagram

3 IoT-based process for Reefer monitoring on board a vessel

This section describes the IoT-based process for Reefer monitoring on board a vessel. Three user stories are detailed as illustrative examples.

3.1 Overall process description

Reefer containers equipped with IoT container devices can communicate locally with servers and applications on board a vessel. The container IoT device interfaces with the Reefer controller unit to collect relevant data and forward it to the local servers and applications on board a vessel. Vessel crew can access and monitor the Reefer container measurements and alarms remotely. Hence, the vessel crew will be able to monitor the Reefer containers in an automated way, which will limit visual inspections to specific Reefer containers that raise alarms and/or report malfunctions. Early alerts will enable the vessel crew to be more effective and take mitigating actions in a timely fashion to attempt to save the cargo.

3.2 Step by step process description

For a foreseeable time, vessel crew will need to distinguish between non-smart containers that require manual inspection and smart containers that can be remotely monitored. This information needs to be exchanged between vessel operator and container operator in advance as a prerequisite. This is outside the scope of this publication but could be done by exchanging SMDG codes in advance.

The vessel crew must follow the generic non-IoT-based Reefer container monitoring process on board a vessel described above to manually monitor the non-smart Reefer containers. Once any Reefer container is loaded, vessel crew must inspect it and plug it in manually, whenever required.

The smart container IoT device will be forwarding regular monitoring data and independent alarm events based on data provided by the Reefer controller unit according to schedules and priorities to be defined in future specification to onboard monitoring system.

The IoT device sends the agreed-upon Reefer container measurements and active alarms as detailed in the table below to the local servers and applications on board a vessel (see Table 2).

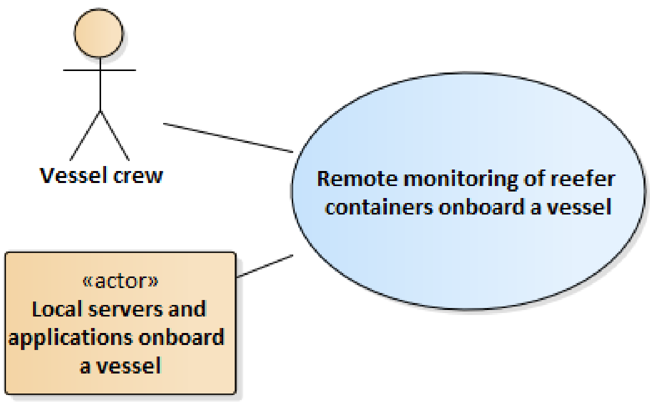

Figure 3: Use case diagram

Use case details

Short description	Defines the minimum Reefer container data elements and alarms to be shared with the vessel crew to enable remote monitoring of Reefers on board a vessel
Actors	Reefer container, container IoT device, Reefer controller unit, vessel crew, local server, local applications, and vessel gateway
Sender	Container IoT device
Receiver	Vessel crew
Triggers	- Active Alarms - if any - Any relevant event such as Reefer engine status change (ON/OFF) - Periodic reporting of the agreed-upon Reefer controller unit measurements
Preconditions	- The vessel is equipped with a DCSA-compliant IoT infrastructure ensuring the communication capability - Reefer container is either equipped permanently with an IoT container device or could be equipped temporarily with an IoT container device on board a vessel - Whenever possible, the vessel crew could plug the temporary IoT container device into the Reefer controller unit - Whether the Reefer container is equipped with a permanent or temporary container IoT device, this container IoT device must be compatible with the DCSA IoT infrastructure installed on board a vessel - The Reefer container operator must have an operational agreement with the vessel operator
Postconditions	Reefer container data is shared with the vessel crew on board a vessel
Data flows	From the Reefer controller unit to the container IoT device to the gateway, to the local server/applications on board a vessel
Data elements and attributes	Agreed-upon Reefer container controller unit data elements and alerts as defined in detail in Table 6 and Table 7

Exceptions	- The vessel is not equipped with a DCSA-compliant infrastructure - The Reefer container is not equipped with a DCSA-compliant container IoT device - The Reefer container operator did not subscribe to remote Reefer monitoring on board a vessel - The vessel operator does not support local monitoring

Table 2: Use case details

3.3 User Story examples

The requirements of the local servers and applications are out of the scope of this publication. However, to illustrate the potential usage of this use case, this section defines the common components required to enable this use case and describes a few user stories as usage examples.

The focus of this release is on data elements only; hence, the common components are shared as an illustrative simplified reference, providing a common vocabulary and data flows. Figure 4 lists all the common components needed to enable remote monitoring of Reefer containers on board a vessel including:

- The Reefer controller unit which generates raw Reefer container data elements as usual without any further modification of its behaviour.
- The container IoT device which is the key component responsible for interfacing, receiving, processing and transmitting the data in the appropriate format and according to connectivity specifications to the local servers and applications.
- The gateways on board the vessel which receive the data collected from the onboard-compatible container IoT devices and forward it to the local server(s) - as it is – only.
- The local servers and applications which are needed for storing, distributing, processing, and displaying the data to the actors (i.e., vessel crew) that are entitled to access this service.
- The vessel crew which operates the vessel transporting the Reefer containers (see also earlier mentioned definition).

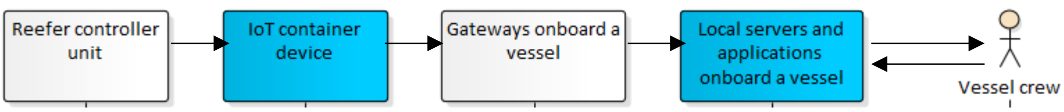

Figure 4: Illustrative common components and data flow

The user stories in Table 3 below illustrate potential ways of performing remote Reefer container monitoring on board a vessel. The user stories described here are examples and do not constitute a comprehensive list.

User Stories

ID	As a [person / role]	I [want to]	[So that]
1	As a Vessel Crew	I want to get notifications of all the alerts coming from all the Reefer containers on board of vessel	so that I can take mitigating actions faster to potentially save the cargo, instead of discovering later that a violation of the required setting range had occurred
2	As a Vessel Crew	I want to automatically access relevant Reefer container sensor measurements coming from all smart Reefer containers on my vessel Note. The data will be polled from the local servers and not directly from container IoT device.	so that I can perform smart Reefer container measurement monitoring in a more efficient way
3	As a Container Operator	I want to make the sensor measurements and alerting thresholds from my smart Reefer container available to vessel crew	so that the vessel crew is able to automatically monitor my smart Reefer container, without bothering about individual interface standards

Table 3: User Stories

3.3.1 User story 1

Figure 5 below Illustrates the sequence diagram of User Story 1, which describes the interactions between the different system components. The alarms are generated by the Reefer controller unit and collected by the container IoT device, which is capable of using the gateways on board a vessel as a means to pass the alarms to the Local services and applications. The alarms are processed and pushed to the vessel crew, who will automatically see them remotely.

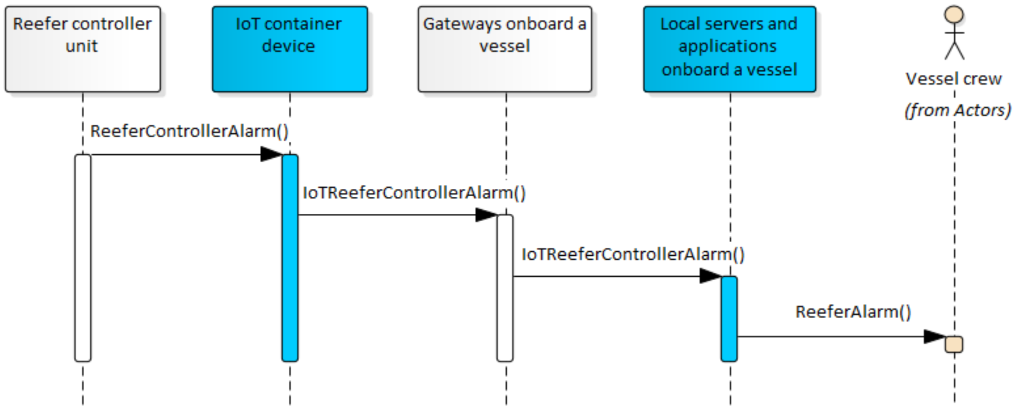

Figure 5: Illustrative sequence diagram of User Story 1

3.3.2 User Story 2

Figure 6 below Illustrates the sequence diagram of User Story 2 which describes the interactions between the different system components enabling the vessel crew to search and access the measurements generated by a given Reefer container. The Reefer container raw data set is generated by the Reefer controller unit, collected, and sent by the IoT container device over the gateways on board a vessel. By using the onboard applications interface, the vessel operator will have access to the most recent as well as historic Reefer container data received and stored by the local sever from all connected Reefer containers on board. The Reefer container data is pulled from the local servers and applications without the need for two-way communication between Reefer and gateways on board a vessel.

Note. For this user story, the local applications will use the information stored in the local servers; information will not be obtained by pinging the IoT container devices directly.

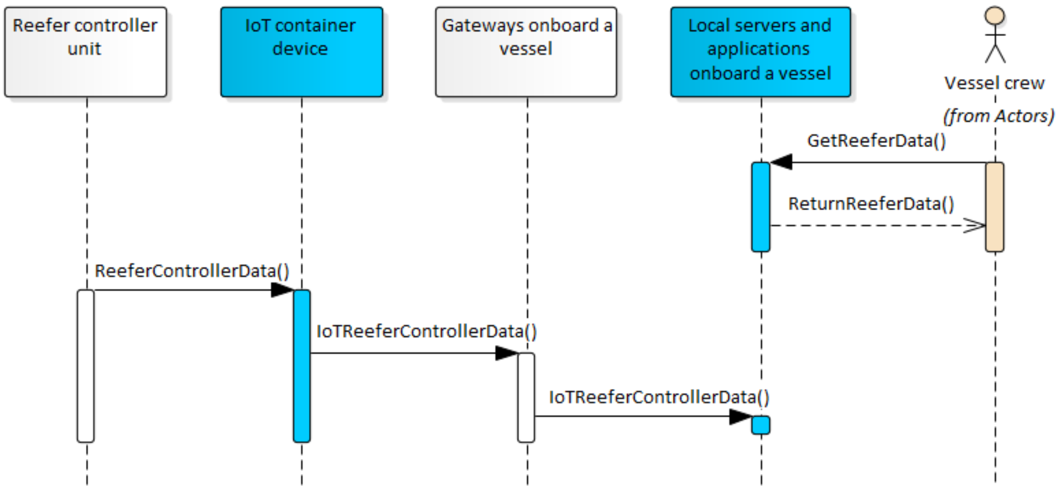

Figure 6: Illustrative sequence diagram of User Story 2

4 Prerequisites and data elements

In this chapter, we list the prerequisites of the IoT-based Reefer monitoring on board a vessel and the minimum list of required data sets to be shared with the vessel crew to enable the implementation of the remote Reefer containers monitoring on board a vessel use case.

4.1 Prerequisites

To enable IoT-based Reefer container monitoring on board a vessel there are multiple prerequisites. Two of those prerequisites are (1) the need to differentiate between smart versus non-smart ones, and (2) the need to categorise the data elements based on their associated access rights. These two prerequisites are detailed below.

4.1.1 Differentiation of non-smart versus smart containers

The SMDG codes could be used to differentiate non-smart containers versus smart ones. These codes are published in the SMDG Attribute code list in Table 4 below. This information must be provided by the container operator before loading the containers as a prerequisite for the IoT-based Reefer containers monitoring on board a vessel use case.

Code	Name	Description
SMC	Smart Container	Container equipped with IoT Device
SMP	Container with passive Tag	Container equipped with a passive Tag (e.g. RFID) enable automatic registration

Table 4: SMDG code list for smart container identification

Note. There is no code for a non-smart container because that is the global default for all containers.

4.1.2 Definition of data categories

Reefer containers can generate more types of data than the data elements required for remote monitoring on board a vessel. Considering the security, privacy, and legal requirements, it is important to define the associated data access rights to offer the expected functionalities while respecting the competitive advantage of the different stakeholders.

Hence, allowing any parties to access data from a given IoT container device must be done according to well-defined data governance rules. Three different categories of data are introduced in this document. For each category, a short description, recommended encryption mechanisms and an example are presented in Table 5 below.

	Public data	Semi-private data	Private data
Description	Data that is accessible to all parties without restrictions	Data that is accessible only to partners upon agreement for individual shipments, or within a given geographical area or inter-party service agreement	Data that is reserved for container operator usage only
Encryption	One-way non-encrypted	One-way encrypted, shared with stakeholders on need-to-know basis, requires authenticated access	Two-way encrypted, payload only accessible to the data owner
Example	The container identification system data - ISO 6346	Smart Container data for local monitoring such as Setpoint, Retpoint, Power supply connection, etc.	GPS position labelled as final place of delivery

Table 5: Data Categories

4.2 Data elements

Table 6 and Table 7 list, define and categorise the Mandatory and Optional Reefer container data elements to enable the remote Reefer container monitoring on board a vessel use case.

Mandatory data is required as the minimum set of data to enable the vessel crew to perform basic remote Reefer container on board a vessel. Optional data classification regroups the data elements that are either (1) not always applicable for a given cargo being transported or (2) additional data elements that give more information remotely to the vessel crew making the IoT process more automated.

4.2.1 Mandatory data elements

Table 6 lists and defines the minimum set of Reefer container data that must be sent by the IoT devices to the local servers and applications on board a vessel.

Mandatory data elements

Name	Description	Data category
ID	An identifier of the Container (Container Number)	Public
Controller Model and Type	The Reefer controller unit specific Model and type as defined by its manufacturer	Semi-private
Measurement reading Date & Time (UTC)	UTC Date and time of this reading as recorded by the Reefer controller unit	Semi-private
Power On / Off	The status of the integrated refrigeration unit (Reefer Engine On/Off)	Semi-private
Active controller alarms	Presence of active alarm(s) on the Reefer controller unit (Yes/No)	Semi-private
Temperature Set point (°C)	Target value of the temperature for the Reefer based on the cargo requirement	Semi-private
Supply Temperature (°C)	Temperature measured by the supply probe (placed at the bottom, at the beginning of the aircycle), measuring the supply of fresh air going in	Semi-private
Return Temperature (°C)	Temperature measured by the return probe (placed at the top, at the end cycle), measuring the supply of fresh air going out	Semi-private
Supply Temperature 2 (°C)	Temperature measured by the back-up supply probe (placed at the bottom, at the beginning of the aircycle), measuring the supply of fresh air going in	Semi-private
Return Temperature 2 (°C)	Temperature measured by back-up return probe - (placed at the top of the end cycle), measuring the supply of fresh air going out	Semi-private

Table 6: Mandatory data

4.2.2 Optional data elements

The following Table 7 lists and defines the optional Reefer container data elements that could be sent in addition to the mandatory data elements (listed in Table 6 above) by the IoT devices to the local servers and applications on board a vessel.

Optional data elements

Name	Description	Data category
Active controller Alarm list	Enumeration of all the active alarms raised from a given Reefer controller unit	Semi-private
Operating Mode	Operation mode of the container (see Table 8 for the list)	Semi-private
Temperature Inrange	An indication of whether the average of the measured supply and return temperatures is within the desired range as defined in the settings (Yes/No)	Semi-private
Ambient Air Temperature (°C)	The air temperature outside the Reefer container	Semi-private
O_2 Setpoint (%)	The percentage of the controlled atmosphere O_2 target value	Semi-private
O_2 (%)	The percentage of the controlled atmosphere O_2 sensor measurement	Semi-private
CO_2 Setpoint (%)	The percentage of the controlled atmosphere CO_2 target value	Semi-private
CO_2 (%)	The percentage of the controlled atmosphere CO_2 sensor measurement	Semi-private
Humidity Setpoint (%)	The percentage of the controlled atmosphere humidity target value	Semi-private
Humidity (%)	The percentage of the controlled atmosphere humidity sensor measurement	Semi-private

Name	Description	Data category
Air Exchange Setpoint (m3/h)	Target value for the air exchange rate which is the rate at which outdoor air replaces indoor air within a Reefer container (e.g., vent positioning)	Semi-private
Air Exchange (m3/h)	The rate at which outdoor air replaces indoor air within a Reefer container sensor measured (in m3 per hour) using the adjustable Reefer Fresh Air vent	Semi-private
Cargo Probe 1 Correction Factor	A factor to be multiplied with the Cargo Probe 1 measurement to correct a systemic error in the in-transit cold treatment program	Semi-private
Cargo Probe 1 (°C)	Temperature measured by the probe inside the cargo (a.k.a. USDA 1 measurement)	Semi-private
Cargo Probe 2 Correction Factor	A factor to be multiplied with the Cargo Probe 2 measurement to correct a systemic error in the in-transit cold treatment program	Semi-private
Cargo Probe 2 (°C)	Temperature measured by the probe inside the cargo (a.k.a. USDA 2 measurement)	Semi-private
Cargo Probe 3 Correction Factor	A factor to be multiplied with the Cargo Probe 3 measurement to correct a systemic error in the in-transit cold treatment program	Semi-private
Cargo Probe 3 (°C)	Temperature measured by the probe inside the cargo (a.k.a. USDA 3 measurement)	Semi-private
Cargo Probe 4 (°C)	Temperature measured by the probe inside the cargo (a.k.a. USDA 4 measurement)	Semi-private

Table 7: Optional data

4.2.3 Operating Modes

This section presents the list of the generic operating modes that could be shared with the vessel crew as part of the optional data elements.

Operating Modes list

The following is the list of the generic operation modes. This list could be expanded in the future if required.

Operating Modes	Description
Reefer Controlled Atmosphere	Creation of an appropriate atmosphere (e.g., by modifying gas composition to rectify the O_2 and CO_2 levels) to slow down physiological deteriorations and prolong storage duration.
Defrost	Defrost of evaporator to avoid ice in the machinery. When water and heat pass the evaporator of the Reefer machinery, ice is formed. This effect needs to be kept to a minimum, as it has a negative impact on the cooling performance of the Reefer machinery
Economy	Reefer is in low power consumption mode
Full cool	Reefer is at maximum power to rapidly cool the temperature
Modulation	Reefer adjusts power output of the compressor enabling it to speed up or slow down according to the requirement of the loaded Reefer cargo
Pre-trip inspection (PTI)	The PTI is an extensive check of the machinery to ensure that the Reefer machinery is running properly at the correct settings
Idle	No active cooling or heating of any sort
Heating	The temperature in the air of the Reefer will heat at a faster rate than the temperature of the product
Cool Reduced	Makes the cooling process less intense when the temperature reaches a specified limit
Start Up	Sets the Reefer in operation mode
Shut down	Shuts down the Reefer machinery

Operating Modes	Description
Cooling	The temperature in the air of the Reefer will be cooled at a faster rate than the temperature of the product
Alarm	Active alarms are raised and displayed on the Reefer controller unit

Table 8: Operating mode list

4.3 Standard adoption guidelines

Reefer container operators are compliant with this standard as long as they share the minimum set of mandatory data elements generated by their Reefer containers (equipped with IoT containers devices) with the local servers and applications on board a vessel to enable vessel crew to perform the IoT-based remote Reefer container monitoring process.

Depending on the contracted Reefer container local monitoring, and the associated Service Level Agreements (SLAs) and Service-Level Objectives (SLOs), the local monitoring requirements may vary. This standard does not preclude the container operators and vessel operators from sharing a richer set of Reefer container data elements (than the minimum set of mandatory Reefer container data and optional data elements) as specified in their commercial agreements. In addition, this standard does not preclude having different levels of local support/maintenance on board a vessel.

5 Conclusion

This release defines the minimum set of required data elements to be shared with the vessel crew to enable remote monitoring of smart Reefer containers on board a vessel. Remote Reefer containers monitoring has the potential to improve the operational efficiency on board a vessel. The vessel crew will be empowered to focus their attention on Reefer containers that raise alarms and take corrective actions promptly, rather than repeatedly check all Reefer containers.

As future work, all IoT container device data including the Reefer data defined in this release shall be integrated in the DCSA data model, a cornerstone of the DCSA modelling work. DCSA Information Model 2.0 must be updated accordingly. The DCSA Information Model 2.0 organises and catalogues the information required for better collaboration between stakeholders, offering a common language and data semantics for entities, processes, and events. This release in itself is not sufficient for implementation of this use case. Subsequent releases will complement this release.