18 September 2020

IoT Container Standards

IoT Standard for Gateway Connectivity Interfaces

Version 1.0

Table of contents

List of figures

List of tables

Preface

The vision of DCSA (Digital Container Shipping Association) is to shape the digital future of container shipping by being the industry's collective voice. Together with our members, DCSA works towards alignment and standardisation of IT and non-competitive business practices. Our aim is to move the industry forward by setting frameworks for effective and universally adoptable standards and exploring possibilities for innovation. We are vendor neutral and technology agnostic to enable widespread adoption of DCSA standards.

The objective of the DCSA IoT Standard for Gateway Connectivity Interfaces is to enable industry-wide interoperability between IoT devices and the supporting network infrastructure. This standard relies solely on the shared requirements of the industry.

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

This document

This standard is the first publication of the DCSA's Internet of Things (IoT) program and is developed to ensure interoperability on the gateway radio interface level between IoT solutions deployed by the various supply chain participants in the shipping industry.

This publication is supported by a range of earlier publications by DCSA. The supporting publications are:

- **DCSA Industry Blueprint 1.0**
  Provides insights on as-is carrier processes. The DCSA Industry Blueprint comprises of processes related to the movement of a container/equipment from one location to another. These are processes that are linked to a shipment/booking, that are considered critical for industry digitisation and standardisation efforts and that are not considered commercially sensitive or of competitive nature.
- **DCSA Glossary of Terms 1.2**
  Promotes alignment between terms across all DCSA stakeholders in the container shipping industry. The second version of the glossary was published on the DCSA website in the summer of 2019, in the context of the Industry Blueprint.

Document ID

Table 1: Program ID

Name	**Description**
Program name	IoT Container Standards
Program number	2
Program director	Marcel van de Pol
Steering committee	André Simha (MSC), Steven Tsao (Yang Ming), Steen Larsen (Maersk)

Referenced documents

- DCSA Industry Blueprint 1.0 (can be found on the DCSA.org website)
- DCSA Glossary of Terms 1.2 (can be found on the DCSA.org website)
- Container Owners Association (COA) - Guide to Container Tracking and Telematics Technology: An Overview of Technology Issues and Choices for Container Operators and Leasing Companies (2019): https://www.containerownersassociation.org/wp-content/uploads/2018/03/COA-Guide-to-Container-Tracking-and-Telematics-Technology.pdf
- Cisco Press - IoT and Security Standards and Best Practices (2019): https://www.ciscopress.com/articles/article.asp?p=2923211&seqNum=6
- The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) – Smart Container Business Requirements Specifications (2019): https://www.unece.org/fileadmin/DAM/cefact/brs/BRS-SmartContainer_v1.0.pdf
- LoRa Alliance – LoRaWAN Regional Parameters RP002-1.0.0 (2019): https://lora-alliance.org/resource-hub/lorawanr-regional-parameters-rp002-100
- GSMA - Mobile IoT in the 5G future: NB-IoT and LTE-M in the context of 5G (2018): https://www.gsma.com/iot/wp-content/uploads/2018/05/GSMA-5G-Mobile-IoT.pdf
- ISO – ISO 10891: Freight containers — Radio frequency identification (RFID) — Licence plate tag (last reviewed in 2018): https://www.iso.org/standard/46282.html

1 Introduction

1.1 Objective

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 carriers' operational teams worldwide with relevant information on container (contents) status and whereabouts both at sea and on land.

In the most basic scenario for the container shipping industry, IoT refers to the concept of connecting sensors and other electronic devices mounted on the containers to the internet and / or local systems. This is done in order to send and receive data to and from these devices for different supply chain purposes and applications. Until now the lack of interoperability between different IoT solutions has made it virtually impossible to provide this information throughout the container journey[1]. The DCSA Gateway Connectivity Interfaces standard has been developed as the first step towards solving this lack of interoperability.

This standard will focus on the supporting network infrastructure in the form of IoT gateways that are deployed to enable connectivity for IoT container devices. In this context, gateways act as a connectivity intermediary between multiple IoT container devices, IoT cloud platforms and / or local systems. With this standard, all industry stakeholders such as carriers, vessel owners, ports, terminals, container yards or other infrastructure owners, will be one step closer to:

a) Designing the uniform network infrastructure that will support all IoT container solutions developed by different carriers and / or IoT providers;

b) Reduce the risk of investment on IoT devices without restricting individual strategies and/or priorities;

c) Create a volume in demand that industry stakeholders, market suppliers and service providers can leverage.

1.2 Overview

<u>DCSA IoT program scope</u>

This document constitutes Release 1 of the DCSA IoT standards program. Following this first release, Release 2 is planned for Q4 2020 and will extend on the communication protocol layers as well as data structures and data handling requirements. Release 3 is planned for Q2 2021 and will focus on the minimum requirements for IoT devices' physical and software security that support the industry use cases. Additional releases will be planned as the roadmap evolves.

The overview of the release plan for the DCSA IoT standards program is presented in Figure 1.

[1] "Guide to Container Tracking and Telematics Technology: An Overview of Technology Issues and Choices for Container Operators and Leasing Companies", Containers Owners Association (COA), 2019

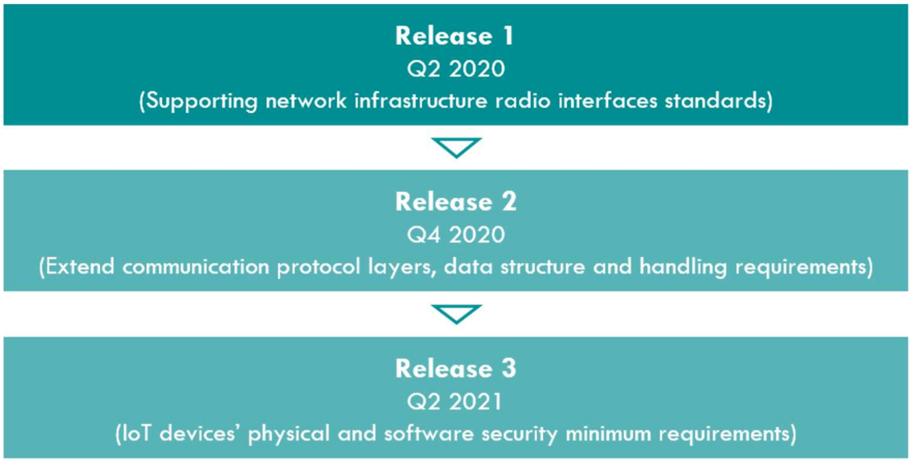

Release 1
Q2 2020
(Supporting network infrastructure radio interfaces standards)
Release 2
Q4 2020
(Extend communication protocol layers, data structure and handling requirements)
Release 3
Q2 2021
(IoT devices' physical and software security minimum requirements)

Figure 1: Overview of planned releases for DCSA's IoT standards program

Release 1 scope

In this standard, DCSA follows an IoT-centric protocol stack model in line with common practices[2]. This model is a simplification of the Open Systems Interconnection (OSI) reference model defined by the International Standards Organisation (ISO). The model followed by DCSA is composed of four layers as opposed to the seven layer OSI model. The simplified model, presented in Figure 2, is considered a better fit for IoT solution purposes.

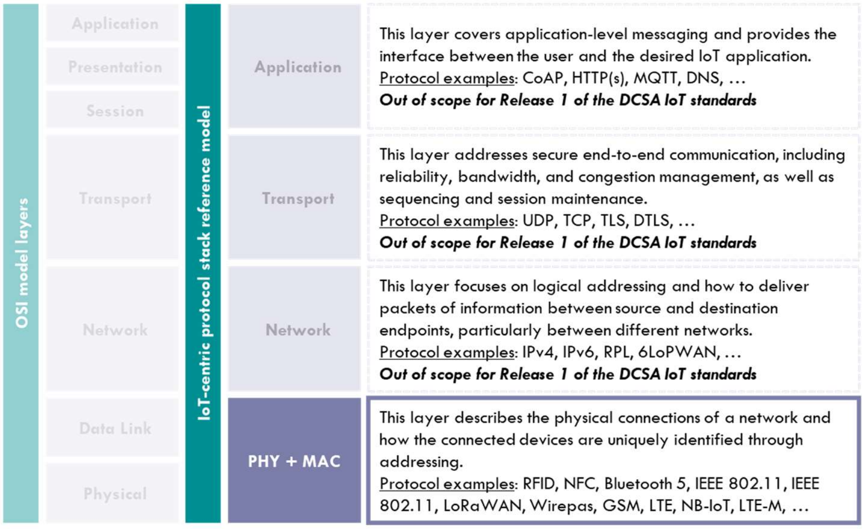
The protocol stack model forms the basis for identification and assessment of existing IoT connectivity technologies. The scope of Release 1 covers part of the Physical and Media Access Control (PHY+MAC) layer, specifically focusing on the basic physical connection characteristics related to the radio interfaces. The remaining layers of the reference model are out of scope of this publication.

DCSA recognises that a number of other organisations are working on standards within the IoT space for the container shipping industry. In particular, the Smart Container working group of the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT)[3]. This working group is currently working on a data model standard for smart container solutions. DCSA has looked closely at this and other initiatives.

To this date DCSA has not identified any other working groups in this space with a focus on radio interfaces and specifically the PHY and MAC layers of the presented protocol stack model. Based on this, DCSA does not see any overlap between the work presented in this document, existing standards and standards currently under development.

[2] R. Irons-Mclean, A. Sabella, M. Yannuzzi, "IoT and Security Standards and Best Practices", Cisco press, 2019

[3] "Smart Containers Business Requirements Specifications", The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), 2019



This layer covers application-level messaging and provides the interface between the user and the desired IoT application.
Protocol examples: CoAP, HTTP(s), MQTT, DNS, …
Out of scope for Release 1 of the DCSA IoT standards

This layer addresses secure end-to-end communication, including reliability, bandwidth, and congestion management, as well as sequencing and session maintenance.
Protocol examples: UDP, TCP, TLS, DTLS, …
Out of scope for Release 1 of the DCSA IoT standards

This layer focuses on logical addressing and how to deliver packets of information between source and destination endpoints, particularly between different networks.
Protocol examples: IPv4, IPv6, RPL, 6LoPWAN, …
Out of scope for Release 1 of the DCSA IoT standards

This layer describes the physical connections of a network and how the connected devices are uniquely identified through addressing.
Protocol examples: RFID, NFC, Bluetooth 5, IEEE 802.11, IEEE 802.11, LoRaWAN, Wirepas, GSM, LTE, NB-IoT, LTE-M, …

Figure 2: IoT-centric protocol stack used as reference model for the DCSA IoT standards

Release 1 publication structure

The structure of this document is as follows:

- **Section 1:** Description of the current standard publication, objectives, scope and key references;
- **Section 2:** Introduction of the development model and main components that constitute the standard
- **Section 3:** Presentation of the IoT Gateway Connectivity Interfaces standard, detailing the radio interfaces that shall be present on gateways devices comprising the IoT supporting network infrastructure;
- **Section 4:** Definition of the standard adoption guidelines that aim to provide guidance on the implementation of these standards;
- **Section 5:** Conclusion.

1.3 Conformance

All parties in the container shipping industry are encouraged to implement and follow the IoT radio interfaces standards specified in this document.

1.4 Normative references

The documents listed below constitute the normative references for publication 1.0 of the DCSA IoT standard for Gateway Connectivity Interfaces:

- DCSA Industry Blueprint 1.0;
- DCSA Glossary of Terms1.2.

2 Standard development model

This standard recommends a set of radio interfaces that shall be the basis of various IoT gateway device specifications. The basis of this publication is a range of inputs and components that have been collected and assessed by DCSA.

An overview of the main elements of the standard development model and scope is presented in Figure 3.

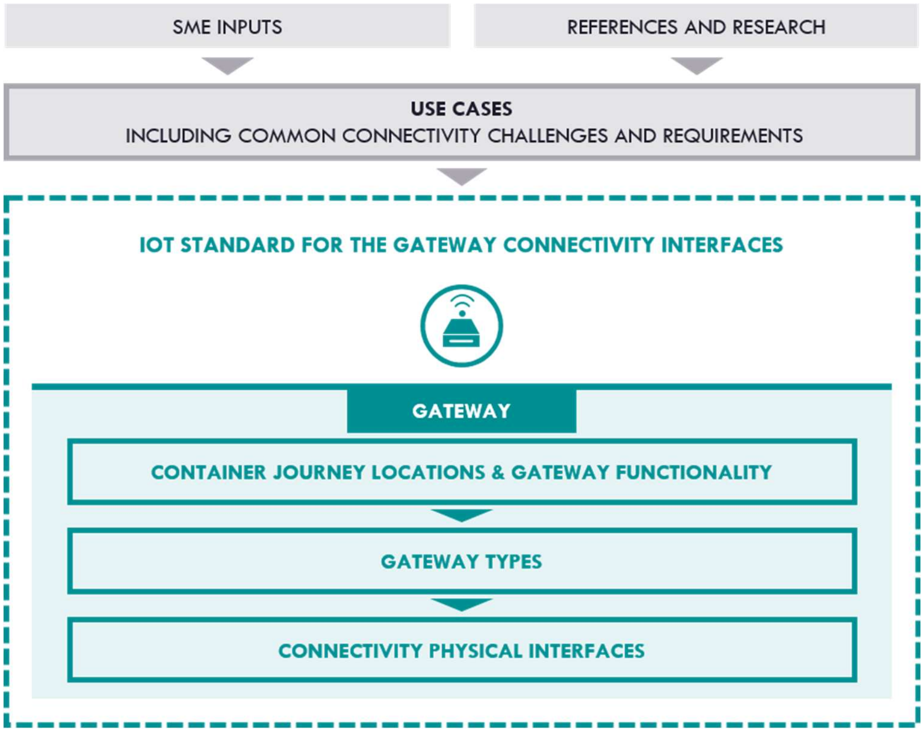

SME INPUTS
REFERENCES AND RESEARCH
USE CASES
INCLUDING COMMON CONNECTIVITY CHALLENGES AND REQUIREMENTS
IOT STANDARD FOR THE GATEWAY CONNECTIVITY INTERFACES
GATEWAY
CONTAINER JOURNEY LOCATIONS & GATEWAY FUNCTIONALITY
GATEWAY TYPES
CONNECTIVITY PHYSICAL INTERFACES

Figure 3: Development model for DCSA Gateway Connectivity Interfaces standards

2.1 Main inputs for the standard

The standard at hand is a product of the following main inputs:

- **Subject matter expert (SME) inputs:** each stage of the standard development process is validated with industry SMEs provided by DCSA member companies to ensure industry and technical relevance of the standard;
- **References and research**: the radio interfaces selection process is conducted by the DCSA core team. This is based on internal researches, studies of key IoT container solution requirements and a technical assessment of all relevant IoT connectivity protocols.

2.2 Use cases

A short-list of IoT container use cases labelled as critical for the industry have been identified and prioritised by DCSA. The shared connectivity challenges across these use cases are defined and translated into requirements. They represent the minimum set of capabilities the IoT gateway radio interfaces shall support.

Based on the commonalities in requirements, deployment locations and functionalities, 3 use case Groups have been defined and are listed below in non-prioritised order:

1. Reefer container sensor & other data monitoring, tracking and remote control;
2. Dry container sensor data monitoring and tracking;
3. Automatic electronic container registration.

The broad scope of the use case Groups does not allow for all the requirements to be quantified. They are therefore given as qualitative descriptions and/or ranges. Future releases of the DCSA IoT standard will further detail the use case Groups' requirements.

The requirements are summarised in Table 2 and detailed in the following descriptions:

1. **Reefer container sensor & other data monitoring, tracking and remote control:** activity monitoring, tracking and remote control of relevant parameters on the reefer container sensors & control unit. This Group covers all the aspects related to maintaining the freshness, quality and lifespan of perishable products. In addition, it enables operational teams to better track, manage maintenance and promptly respond to alarm indicators from reefer containers.

   Minimum requirements for the radio interfaces of the specified use case Group:

   a) Coverage: cover and operate on main locations of the container journey (land & sea);

   b) Performance in radio constrained environments: handle communication barriers, such as physical obstacles limiting the radio wave propagation, and interference caused by other devices;

   c) Density of devices: handle high density environments in terms of connected devices, with enough capacity to allow thousands of simultaneous connections;

   d) Type of communication: enable two-way communications to send and receive data;

   e) Frequency of data exchanged: handle data reporting on scheduled or event/ alarm basis up to a few data exchanges per hour;

   f) Typical data payload: handle sufficient data payload to support all reporting activities including container geolocation, temperature, door opening, humidity, gas and control unit commands;

   g) Power: provide low power consumption modes of operation for when the reefer is off the power grid;

   h) Security: provide encryption mechanisms to protect non-public data.

2. **Dry container sensor data monitoring and tracking:** location tracking and sensors parameters monitoring on dry containers. This use case Group enables improved estimated arrival times for dry containers, monitoring of alarms caused by critical events and evaluation of the risks on the different shipping container journey locations.

   Minimum requirements for the radio interfaces of the specified use case Group:

   a) Coverage: cover and operate on main locations of the container journey (land & sea);

   b) Performance in radio constrained environments: handle communication barriers, such as physical obstacles limiting the radio wave propagation, and interference caused by other devices;

   c) Density of devices: handle very high density environments in terms of connected devices with enough capacity to allow tens of thousands of simultaneous connections;

   d) Type of communication: enable two-way communications that allows to send and receive data;

   e) Frequency of data exchanged: handle data reporting on scheduled or event/ alarm basis up to a few data exchanges per hour;

   f) Typical data payload: handle sufficient data payload to support all reporting activities including container geolocation, temperature, door opening, humidity and gas;

   g) Power: highly reliable low power consumption modes of operation to maximise devices' lifespan and minimise battery replacement;

   h) Security: provide encryption mechanisms to protect non-public data.

3. **Automatic electronic container registration:** automatic registration of reefer and dry containers' ID and generic specifications in key on-land locations such as entry or exit gates of container depots, railway stations, terminals etc. It relies on electronic tags that are attached to the containers, configured with the containers' ID and generic specifications data. This use case Group aims to enable a systematic approach for automatic container identification and supply chain applications. It is an alternative approach to the existing methods such as Optical Character Recognition (OCR) and manual interactions. These existing methods are error prone, time consuming and have limited capabilities on registering containers moving at speed.

   Minimum requirements for the radio interfaces of the specified use case Group:

   a) Coverage: cover and operate on key on land locations and at speed scenarios (e.g. moving trucks or trains);

   b) Radio propagation & interference performance: not expected to face considerable communication constraints;

c) Density of devices: Operate in low density environments, handling the short-range connectivity of tens' of IoT devices simultaneously;

d) Type of communication: enable two-way type of communications that allows to send and receive data;

e) Frequency of data exchanged: No specific frequency is required, data is reported on event-based mode;

f) Typical data payload: handle sufficient data payload to support the reporting of container ID + generic container specifications;

g) Power: highly reliable very low power consumption modes of operation to maximise devices' lifespan and minimise battery replacement;

h) Security: limited need for data encryption (expected to involve only publicly available data).

Table 2: Minimum requirements for the radio interfaces for each use case Group

	Reefer container sensor & other data monitoring, tracking and remote control	**Dry container sensor data monitoring and tracking**	**Automatic electronic container registration**
Coverage	Cover and operate on main locations of the container journey (land & sea)		Cover and operate on key on land locations and at speed scenarios (e.g. moving trucks or trains)
Performance in radio constrained environments	Handle communication barriers, such as physical obstacles limiting the radio wave propagation, and interference caused by other devices		Not expected to face considerable communication constraints
Density of devices	Handle high density environments in terms of connected devices, with enough capacity to allow thousands of simultaneous connections	Handle very high density environments in terms of connected devices with enough capacity to allow tens of thousands of simultaneous connections	Operate in low density environments, handling the short-range connectivity of tens' of IoT devices simultaneously
Type of communication	Enable two-way communications that allows to send and receive data		
Frequency of data exchange	Handle data reporting on scheduled or event/ alarm basis up to a few data exchanges per hour		No specific frequency is required, data is reported on event-based mode
Typical data payload	Handle sufficient data payload to support all reporting activities including container geolocation, temperature, door opening, humidity, gas and control unit commands	Handle sufficient data payload to support all reporting activities including container geolocation, temperature, door opening, humidity and, gas	Handle sufficient data payload to support the reporting of container ID + generic container specifications
Power	Provide low power consumption modes of operation for when the reefer is off the power grid;	Highly reliable low power consumption modes of operation to maximise devices' lifespan and minimise battery replacement	Highly reliable very low power consumption modes of operation to maximise devices' lifespan and minimise battery replacement
Security	Provide encryption mechanisms to protect non-public data		Limited need for data encryption (expected to involve only publicly available data)

2.3 Main standard components

DCSA gateway connectivity interfaces standards cover three main differentiating aspects:

- **Container journey locations and gateway functionality:** The journey of an IoT container includes different locations such as vessel, ports, terminals and container depots. Each of these locations have specific characteristics which result in different requirements for radio interfaces to enable the continuity of wireless communications. This standard takes these differences into consideration and presents a logical differentiation of gateways based on expected deployment locations and required IoT functionalities;
- **Gateway types:** The gateway types represent the different supporting network infrastructure that can be deployed along the container journey, by different stakeholders;
- **Physical connectivity interfaces:** DCSA categorises the gateway's physical connectivity interfaces into two sub-categories as illustrated in Figure 4. Only the internal interfaces are in scope for Release 1 of the DCSA IoT standards:
    - **Internal radio interfaces:** used to establish wireless communication between the gateway and the IoT container device solutions;
    - **External interfaces:** used to establish wireless or wired communication between the gateway and the cloud/internet or other local infrastructure (also known as backhaul connection).

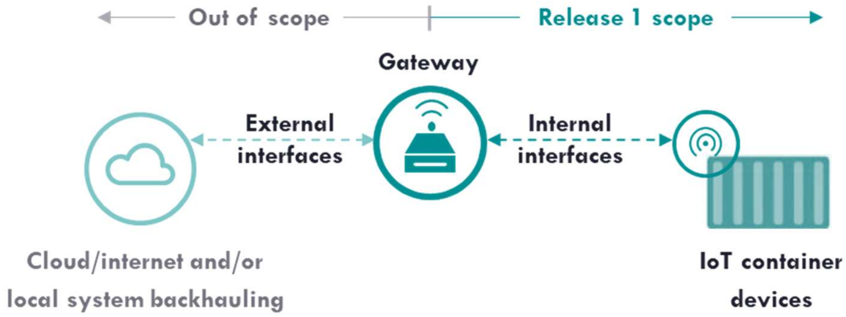


Figure 4: Overview of the internal and external IoT Gateway interfaces

Note: Release 1 does not standardise the external interfaces. This allows each gateway owner to define the best approach based on local requirements and available local infrastructure. In order to drive interoperability across the industry, Section 4 presents a minimum set of adoption guidelines for the external interfaces.

3 Gateway connectivity interface standards

Based on the defined use case Groups, target locations and required functionalities, four types of gateways are identified for this standard. The gateway types form the edge of the supporting network infrastructures that can be deployed along key locations of the container journey. For each gateway type, the standard identifies the internal radio interfaces that shall be supported.

Use case Groups 1 and 2 are very similar in terms of functionalities and requirements. They can be supported by the same types of gateways that will mainly vary between sea and land installation locations. Use case Group 3, Automatic electronic container registration, is quite different to the first two use case Groups and requires different types of gateways that will vary in terms of their main functionality.

An overview of the different types of gateways and a summary of their internal radio interfaces standards is presented in Figure 5.

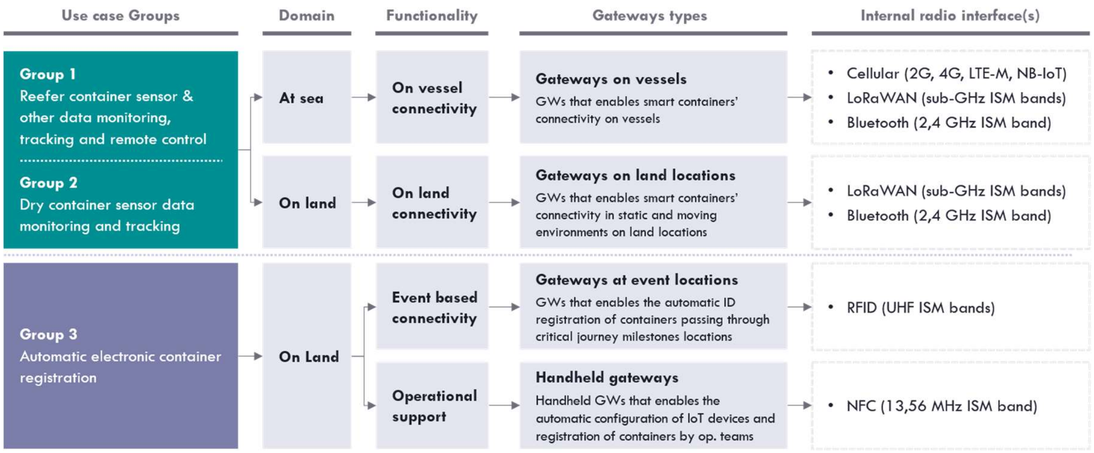

Use case Groups
Domain
Functionality
Gateways types
Internal radio interface(s)
Group 1
Reefer container sensor & other data monitoring, tracking and remote control
Group 2
Dry container sensor data monitoring and tracking
At sea
On land
On vessel connectivity
On land connectivity
Gateways on vessels
GWs that enables smart containers' connectivity on vessels
Gateways on land locations
GWs that enables smart containers' connectivity in static and moving environments on land locations
• Cellular (2G, 4G, LTE-M, NB-IoT)
• LoRaWAN (sub-GHz ISM bands)
• Bluetooth (2,4 GHz ISM band)
• LoRaWAN (sub-GHz ISM bands)
• Bluetooth (2,4 GHz ISM band)
Group 3
Automatic electronic container registration
On Land
Event based connectivity
Operational support
Gateways at event locations
GWs that enables the automatic ID registration of containers passing through critical journey milestones locations
Handheld gateways
Handheld GWs that enables the automatic configuration of IoT devices and registration of containers by op. teams
• RFID (UHF ISM bands)
• NFC (13,56 MHz ISM band)

Figure 5: Overview of gateway types and associated internal radio interfaces standards

To enable container IoT solutions for use case Groups 1 and 2 it is required to have connectivity on critical journey locations. These can be grouped in on land and at sea location domains. These domains are significantly different in terms of frequency regulations and available connectivity infrastructure. For this reason, two gateway types supporting use case Groups 1 and 2 are defined:

- "Gateways on vessels": Gateways that can be installed on the vessels enabling the deployment of private cellular networks at sea;
- "Gateways on land locations": Gateways that can be installed on land locations and will complement the existing public cellular communication infrastructure.

Container IoT solutions for use case Group 3 require connectivity to be enabled at specific on land journey locations. The gateway types for this use case Group can be differentiated based on their key functionalities:

- "Gateways at event locations": Gateways that enables the automatic ID registration of containers passing through critical on land milestone locations;
- "Handheld Gateways": Handheld gateways that enable the automatic configuration of IoT devices and registration of containers by operational teams.

The following sections describe each gateway type and the rationale behind them in detail.

3.1 Radio standards for "Gateways on vessels"

This section presents the standard for the **"Gateways on vessels".** The standard recommends the radio interfaces that shall be enabled by one or more statically mounted gateways deployed on vessels to enable dedicated IoT supporting network infrastructure at sea. Private IoT networks on vessels are the only viable option for providing connectivity for IoT solutions at sea, where no public network coverage capable of fulfilling the use case Groups requirements is available.

Table 3: Summary of standards for the "Gateways on vessels"

Gateway type:	**Use case Group(s):**	**Domain:**
Gateways on vessels	1 & 2	At sea

Definition
Gateways that can be installed on the vessels enabling the deployment of private cellular networks at sea.

Standards for gateway internal radio interfaces
Cellular (2G, 4G, LTE-M, NB-IoT)
LoRaWAN (sub-GHz ISM* bands)
Bluetooth (2,4 GHz ISM* band)

* *Industrial, Scientific & Medical*

During vessel operations, the location of the vessel may alternate between national and international waters. Across these locations, different regulations of the radio wave frequency spectrum are enforced. To adhere to these regulations, the gateways installed on a container vessel shall be able to adapt to local regulations throughout the vessel journey. This is particularly important while operating on national waters and can be implemented by allowing the gateways to:

- Selectively activate and deactivate the cellular radio interfaces dependent on licensed spectrum;

- Switch between the ISM frequency bands according to its regional parameters[4].

On board a container vessel the environment can be heavily constrained in terms of radio waves propagation and interference. This is due to the large amount of metal containers and the metal structure of the vessel itself. To overcome these constraints and ensure effective connectivity capabilities, three complementary radio interfaces are recommended. They are cellular, LoRaWAN and Bluetooth. Together these are the internal radio interfaces standards of the "Gateways on vessels" that collectively shall be available and usable across the vessel. The three radio interfaces can be made operable from a single multiprotocol gateway or from multiple gateways that enable one or more of the standardised radio interfaces. Depending on the size of the vessel and the solution design, multiple gateways can be required to ensure good coverage for all the containers regardless of their locations.

3.1.1 Standards for gateway internal radio interfaces

Cellular (2G, 4G, LTE-M, NB-IoT)

Cellular physical radio interfaces are amongst the most widely adopted and tested wireless interfaces worldwide. Some of the cellular radio interfaces are already adopted by parties in the container shipping industry for reefer container IoT solutions.

Operating cellular infrastructure on land typically requires a license due to local regulations on the utilisation of cellular frequency bands. On international waters there is no cellular infrastructure readily available and the national spectrum regulations do not apply. Thus, there is no licensing required to operate a cellular radio network. This is an opportunity for the deployment of private cellular networks for IoT connectivity onboard container vessels. Today, cellular physical radio interfaces are already being applied in IoT solutions for on land-based communication. Utilizing them onboard the vessel can lead to significant synergies.

Traditional radio interfaces such as 2G (GSM/GPRS/EDGE), 3G (UMTS/HSPA+) and 4G (LTE) are the most commonly adopted. At the time of this publication, several key considerations have been taken into account when selecting the most appropriate cellular radio interface for this standard:

- Cellular protocols are constantly under development and choosing a radio interface associated with a legacy protocol should be avoided. With the advent of 5G, several countries are already planning to phase out 2G and 3G networks. The 2G and 3G protocols are still the most widely implemented cellular protocols but they are rapidly losing ground to 4G and in the long term to 5G;
- Between 2G and 3G, the former is currently the most widespread, efficient and cost effective cellular protocol for IoT use cases with low power and performance requirements;

[4] "LoRaWAN Regional Parameters RP002-1.0.0", LoRa Alliance, 2019

- 3G is not included as part of the "Gateway on vessel" internal radio interfaces since: (i) it does not offer specific characteristics that can be applied to IoT applications that are not already covered by 2G and 4G and (ii) it is being phased out;
- With 5G in its initial stages of adoption, 4G protocols are still the most capable cellular technologies available worldwide. They have been developed to provide a wide range of options for its applications, from high demanding to resource efficient performance levels;
- 3GPP (the main organisation developing cellular standards) has recently released new low power wide area network (LPWAN) and narrowband protocols as part of its LTE suite. These protocols are optimised for IoT applications and will continue to be developed as part of the 5G specifications, meaning that their long-term status is confirmed[5]. These protocols are LTE-M and NB-IoT;
- LTE-M is a version of LTE specially designed for IoT networks. The protocol enables long range bi-directional communication under low power requirements. It ensures full interoperability and backwards compatibility with previous and subsequent 3GPP releases. Thereby, traditional LTE devices will be able to operate with the LTE-M protocol;
- NB-IoT is a protocol especially suited for propagation in constrained environments with a considerable density of IoT devices. It is not fully backwards compatible with devices that utilise existing 3GPP protocols. However, it is designed to achieve excellent co-existence performance with legacy 2G and 4G implementations;
- The availability of LTE-M and NB-IoT worldwide is still limited. However, adoption is expected to ramp up in the coming years;

Based on these considerations, DCSA recommends 2G, 4G, LTE-M and NB-IoT as the cellular radio specifications that shall be supported by the "Gateways on vessels". This decision will help to guarantee:

- Fulfilment of connectivity requirements for use case Groups 1 and 2;
- Increased flexibility for cellular connectivity solutions on IoT container devices;
- Backward compatibility between existing and future cellular capabilities.

However, cellular physical radio interfaces present several operational gaps in the "Gateways on vessels" context. The gaps are that cellular radio interfaces:

(i) Can only be operated without a license on international waters;

(ii) Have limited capabilities to deal with propagation and interference constraints and;

(iii) Have restricted capacity to handle a high density of connections.

[5] "Mobile IoT in the 5G future: NB-IoT and LTE-M in the context of 5G", gsma.com, 2018

To tackle these issues, two additional physical radio interfaces based on LoRaWAN and Bluetooth specifications are required as part of the "Gateway on Vessels" standard communication capabilities.

LoRaWAN (sub-GHz ISM bands)

LoRaWAN is a Low-Power Wide Area Network (LPWAN) IoT radio interface that offers long range and low power consumption capabilities on the unlicensed sub-GHz bands. It is widely available and adopted globally on a range of different IoT applications.

LoRaWAN operates in license-free sub-GHz Industrial, Scientific & Medical (ISM) bands and it is possible to deploy its radio interface on land and at sea without a frequency license. The sub-GHz ISM bands are managed regionally and vary between the global regions. To guarantee worldwide operation while on national waters, the gateways with LoRaWAN physical radio interfaces shall be able to switch between the ISM band frequencies throughout the vessel journey. The sub-GHz frequencies are very well suited for IoT applications in constraint environments due to the penetration properties of this frequency range.

The capabilities of this additional radio interface will increase the vessels' supporting network infrastructure reliability. It also increases the flexibility of the supporting network infrastructure with a widely available physical radio interface that helps to fulfil the connectivity requirements of use case Groups 1 and 2 at sea.

Similar to the cellular radio interfaces, LoRaWAN has restricted capacity to handle a high density of connections. This limitation can be tackled by the deployment of more gateways to increase the network capacity or by utilising the high capacity properties of an additional physical radio interface, based on 2,4 GHz ISM band (Bluetooth).

Bluetooth (2,4 GHz ISM band)

Bluetooth is one of the most widely adopted radio interfaces for IoT wireless personal area networks. Its physical radio interface specifications allow for low power operational modes (Bluetooth Low Energy) and operates on the global 2,4 GHz ISM license free band. It has no license restrictions for deployments at sea or on land.

The direct communication range of the Bluetooth radio is limited when compared with cellular and LoRaWAN. This can be compensated by adopting mesh topology capabilities that rely on Bluetooth physical radio specifications. These mesh capabilities can be configured at the upper layers of the protocol stack.

Bluetooth physical radio interface specifications add the possibility of mesh topology and high network capacity to the vessel's supporting network infrastructure. This provides an important complementarity with the other proposed radio interfaces and additional means for addressing the connectivity requirements of use case Groups 1 and 2.

3.2 Radio standards for “Gateways on land locations”

This section presents the standard for the **“Gateways on land locations”** gateway type. The standard defines the gateways that can be deployed on land locations as a complement to existing public cellular communication infrastructure. The main purpose is to ensure and increase connectivity coverage and connectivity capabilities along the container on land journey.

Table 4: Summary of standards for the “Gateways on land locations”

Gateway type:	**Use case Group(s):**	**Domain:**
Gateways on land locations	1 & 2	On land

Definition
Gateways that can be installed on land locations and will complement the existing public cellular communication infrastructure.

Standards for gateway internal radio interfaces
LoRaWAN (sub-GHz ISM bands)
Bluetooth (2,4 GHz ISM band)

Throughout the on land container journey, a range of different locations such as ports, terminals, container yards, depots, trucks and trains exist. Transportation close to shore and on rivers using means of transport such as barges are considered part of on land locations.

While on land, local regulations of the radio frequency spectrum considerably limit the options for unlicensed deployment of cellular networks. Therefore, cellular radio interfaces will not be considered as options for the “Gateways on land locations” gateway type.

Cellular coverage provided by public infrastructure might not always be available or provide sufficient capacity for critical on land locations. Additionally, enhanced connectivity capabilities might be necessary for these locations to efficiently handle the potential connectivity obstacles, IoT solution connectivity requirements and / or cellular network gaps. To do this, industry stakeholders can deploy gateways based on the “Gateways on land locations” standard enabling the two recommended internal radio interfaces. The two radio interfaces, based on LoRaWAN and Bluetooth, can be operable from a single multiprotocol gateway or from multiple gateways that enable each of the standardised radio interfaces. Depending on the on land deployment area and the solution design, multiple gateways can be required to ensure sufficient connectivity capabilities for a larger or high density area.

3.2.1 Standards for gateway internal radio interfaces

LoRaWAN (sub-GHz ISM bands)

LoRaWAN is a Low-Power Wide Area Network (LPWAN) IoT radio interface that offers long range and low power consumption capabilities on the unlicensed sub-GHz bands. It is widely available and adopted globally on a range of different IoT applications.

LoRaWAN operates in license-free sub-GHz ISM bands and it is possible to deploy its physical radio interface on land and at sea without a frequency license. In order to guarantee compliance with the local regulations, the “Gateways on land locations” shall be configured to operate on the right local ISM band frequency. The sub-GHz frequencies are very well suited for IoT applications in constraint environments due to the penetration properties of this frequency range.

These LoRaWAN characteristics help to fulfil the connectivity requirements of use case Groups 1 and 2 and complement cellular public network coverage on land.

LoRaWAN has restricted capacity to handle a high density of connections. This limitation can be tackled by the deployment of more gateways to increase the network capacity or by utilising the high capacity properties of an additional physical radio interface, based on 2,4 GHz ISM band (Bluetooth).

Bluetooth (2,4 GHz ISM band)

Bluetooth is one of the most widely adopted radio interfaces for IoT wireless personal area networks. Its physical radio interface specifications allow for low power operational modes (Bluetooth Low Energy) and operates on the global 2,4 GHz ISM license free band. It has no license restrictions for deployments at sea or on land.

The direct communication range of the Bluetooth radio is limited when compared with cellular and LoRaWAN. This can be compensated by adopting mesh topology capabilities that rely on Bluetooth physical radio specifications. These mesh capabilities can be configured at upper layers of the protocol stack.

Bluetooth physical radio interface specifications add the possibility of mesh topology and high network capacity to the IoT supporting network infrastructure on land. This provides an important complementarity with the other proposed radio interfaces and additional means for addressing the connectivity requirements of use case Groups 1 and 2.

3.3 Radio standards for “Gateways at event locations”

This section presents the standard for the **“Gateways at event locations”** gateway type. The standard defines the gateways that can be deployed on land at key milestone locations along the container journey. The main purpose of this static gateway is to enable automatic container registrations by electronically reading digital tags mounted on containers. The tags may contain the ID and generic specifications of the container. Examples of the generic specifications that might be configured on the electronic tag can be found on the existing ISO10891[6] standard. These specifications are public information and can be transferred both to local systems and/or directly to the cloud/ internet. The data can be made accessible to interested parties, thus enabling simple automation of supply chain applications and tracking functions.

Table 5: Summary of standards for the “Gateways at event locations”

Gateway type:	**Use case Group(s):**	**Domain:**
Gateways at event locations	3	On land

Definition
Gateways that enables the automatic ID registration of containers passing through critical on land milestone locations.

Standards for gateway internal radio interfaces
RFID (UHF* ISM bands)

**Ultra High Frequency*

The gateway can be statically deployed at key milestone locations such as:

- Entrances and exits gates on ports, terminals, container yards, inland depots and freight stations;
- Border crossings;
- Toll plazas and highway gates;
- Train terminals and railway sidings;
- Barge terminals;
- Container operational infrastructure (e.g. loading cranes);
- Any other static location that can benefit from automatic container registration.

The less demanding performance requirements related to use case Group 3 allows for a single connectivity internal radio interface to be standardised for this gateway type.

[6] “ISO 10891: Freight containers — Radio frequency identification (RFID) — License plate tag”, ISO, 2018 (last review)

3.3.1 Standards for gateway internal radio interfaces

RFID (UHF ISM bands)

Radio Frequency Identification (RFID) is a wireless connectivity radio interface typically used for identification and tracking of objects or people. It is already implemented in various standalone projects across the container shipping industry. Its added value comes from having the required capabilities for simple automation use cases that can greatly benefit the industry as a whole.

RFID utilises a wide range of license free frequency bands and it has no license restrictions for on land deployments. Most RFID systems with requirements similar to use case Group 3 operate on the UHF bands.

The UHF RFID radio interface allows low power operational modes, a reading range of a few meters and the flexibility to deploy either passive (no batteries) or active (battery dependent) tags. These tags usually have a lifespan of up to 20 years in passive tags and 2 to 5 years for active tags. The long lifespan of the RFID tags allows for a less frequent execution of the demanding process for container tag replacement. Container and cargo shipment specific UHF RFID tags technical specifications developed by the ISO 10891 standards can be used as reference in this context.

UHF RFID tags typically have restricted storage capacity and data encryption measures. However, these capabilities are still sufficient to store and handle the basic public container information expected to be transferred on the context of use case Group 3.

The UHF RFID radio specifications are thus capable to address connectivity requirements of use case Group 3 in a cost effective and optimised manner for the “Gateway at event location” context.

3.4 Radio standards for “Handheld gateways”

This section presents the standard for the **“Handheld Gateways”** gateway type. The standard defines the mobile handheld gateways that can be used by operational teams on use case Group 3 functions. The main purpose of this gateway type is to support operational teams on automatic container IoT devices configuration and registrations. This in turn will increase the automation of operational teams’ interactions with the IoT devices and help reduce manual configuration and registration errors. The data collected by the gateway can be transferred to local systems and/or directly to the cloud/ internet. The data can be made accessible to interested parties, thus enabling simple automation of supply chain and tracking functions.

Table 6: Summary of standards for the “Handheld gateways”

Gateway type:	**Use case Group(s):**	**Domain:**
Handheld gateways	3	On land

Definition

Handheld gateways that enables the automatic configuration of IoT devices and registration of containers by operational teams.

Standards for gateway internal radio interfaces
NFC (13,56 MHz ISM band)

The handheld gateways can be present at any container at land locations where operational teams need to be supported with this devices’ capabilities. The less demanding performance requirements allows for a single connectivity internal radio interface to be standardised for this gateway type.

3.4.1 Standards for gateway internal radio interfaces

NFC (13,56 MHz ISM band)

Near Field Communications (NFC) is a nearfield wireless radio interface operating in license free bands (13,56 MHz). It is widely adopted across multiples industries for very short-range peer-to-peer communication. It can easily be adopted by smartphones, tables, laptops and other mobile devices without having to acquire frequency licenses.

This radio interface does not require a synchronisation process between devices or manual configurations. Setting up the communication between the gateway and IoT devices via NFC is typically simpler than for other wireless technologies.

NFC tags are typically passive and require no batteries which helps to avoid a regular and demanding process of container tag replacement. The tags typically have limited storage capacity and restricted data encryption measures. However, these capabilities are still considered to be sufficient to store and handle the basic public container information.

The NFC radio specifications are thus capable of addressing connectivity requirements of use case Group 3 in a cost effective and optimised manner for the “Handheld gateway” context.

4 Standard Adoption Guidelines

The standards defined in section 3 aim to harmonise the radio interfaces of the IoT gateways that are deployed to enable connectivity for IoT container solutions. To the knowledge of DCSA, these standards do not exclude or replace any other standards defined or currently being developed within the container shipping industry.

In order to support and provide guidance on the implementation of these standards, DCSA recommends the guidelines for adoption presented in Table 7:

Table 7: Standard adoption guidelines

Subject area	Guidelines
1. Interoperability	Interoperability is achieved if: • Everyone that adopts the standard enables connectivity for different IoT solutions from multiple parties through the standardised gateways; • Connectivity for IoT devices is established by any of the radio interfaces in the respective gateway type standards; • Connection to the radio interfaces from multiple parties' IoT solutions is allowed depending on agreements made with the gateway(s) owner and / or operator.
2. IoT supporting network infrastructure	The IoT supporting network infrastructure deployed in the form of IoT gateways shall: • Support all standardised internal radio interfaces for the defined gateway types. The standardised physical radio interfaces can be operable from a single gateway or from multiple gateways that jointly enable all of the standardised radio interfaces; • Have at least one operational external connectivity interface that allows access to the internet/cloud or to local systems. The external interface shall have sufficient bandwidth capacity to enable the target IoT container solutions. This standard does not exclude the possibility for gateway owners to add additional radio interfaces on the IoT gateways outside of these recommendations.
3. Regulations & safety	All radio interfaces compliant with this standard shall not be harmful to container cargo and/or personnel and shall meet the safety and regulatory requirements of the appropriate government regulations. This includes, but is not restricted to: • Radio frequency regulations; • Electromagnetic radiation regulations.

	The use of the standardised radio interfaces shall be restricted in hazardous environments such as near or around explosives or flammable gasses unless these devices have been certified as safe for such use by the appropriate authorities.
4. Data structure & handling	IoT container data structure and handling shall be in line with relevant standard publications from DCSA. Available publications from the DCSA Data and Interface program: • Interface standard for track & trace 1.0; • Information model 1.0. Publications under development by the DCSA IoT Container Standards program: • IoT data structure and handling (Release 2 - planned).
5. Installation and maintenance	IoT devices installation and maintenance shall be in line with relevant standard publications from DCSA. Publications under development by the DCSA IoT Container Standards program: • IoT devices installation and maintenance (Release 2 - planned).
6. Security	Security shall be in line with relevant standard publications from DCSA. Available publications from the DCSA Cyber Security program: • DCSA Implementation Guide for Cyber Security on Vessels v1.0; • Asset management and risk assessment templates. Publications under development by the DCSA IoT Container Standards program: • IoT software security (Release 3 - planned).
7. Devices' physical specifications	IoT devices' physical specifications shall be in line with relevant standard publications from DCSA. Publications under development by the DCSA IoT Container Standards program: • IoT devices physical requirements (Release 3 - planned).

5 Conclusion

In this Release from the IoT standards program, DCSA standardises the physical internal radio interfaces for the gateways. The standards are developed together with Subject Matter Experts from all the DCSA member companies.

This publication serves as the foundational work to enable interoperability at the gateways' internal radio interfaces level for the defined use cases. It is also the basis for future IoT standard releases from DCSA. The current order of releases is as follows:

- Release 1 (refers to this publication): focuses on the internal radio interfaces standards of the supporting network infrastructure for IoT containers;
- Release 2 (planned for Q4 2020): will extend the communication protocol layers as well as data structures and data handling requirements;
- Release 3 (planned for Q2 2021): will focus on the minimum requirements for IoT devices' physical and software security that support the industry use cases.

Additional releases will be planned as the roadmap evolves.

DCSA appreciates your feedback. Please go to our website and check out the standards page. Using the online version, you can mark up the documents and provide us with your comments.

Legal disclaimer