ISO/IEC 30163

Edition 1.0 2021-03

INTERNATIONAL STANDARD

colour inside

Internet of Things (IoT) – System requirements of IoT and sensor network technology-based integrated platform for chattel asset monitoring

ISO/IEC 30163:2021-03(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC online collection - oc.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

ISO/IEC 30163

Edition 1.0 2021-03

INTERNATIONAL STANDARD

colour inside

Internet of Things (IoT) – System requirements of IoT and sensor network technology-based integrated platform for chattel asset monitoring

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 35.020; 35.240.40

ISBN 978-2-8322-9442-0

CONTENTS

INTERNET OF THINGS (IoT) – SYSTEM REQUIREMENTS OF IOT AND SENSOR NETWORK TECHNOLOGY-BASED INTEGRATED PLATFORM FOR CHATTEL ASSET MONITORING

FOREWORD

1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO National bodies.

3) IEC and ISO documents have the form of recommendations for international use and are accepted by IEC and ISO National bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC and ISO documents is accurate, IEC and ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC and ISO National bodies undertake to apply IEC and ISO documents transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC and ISO document and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC and ISO do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC and ISO marks of conformity. IEC and ISO are not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this document.

7) No liability shall attach to IEC and ISO or their directors, employees, servants or agents including individual experts and members of its technical committees and IEC and ISO National bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this ISO/IEC document or any other IEC and ISO documents.

8) Attention is drawn to the Normative references cited in this document. Use of the referenced publications is indispensable for the correct application of this document.

9) Attention is drawn to the possibility that some of the elements of this ISO/IEC document may be the subject of patent rights. IEC and ISO shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 30163 was prepared by subcommittee 41: Internet of Things and related technologies, of ISO/IEC Joint Technical Committee 1: Information technology.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
JTC1-SC41/189/FDIS	JTC1-SC41/204/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

In traditional chattel mortgage processes, the financial industry lacks standardized management for accessing chattel assets' information, assessing them and sharing the asset and mortgage information among stakeholders such as financial institutions. Furthermore, there is no standardized chattel asset monitoring and tracking (or no monitoring at all) which can quantify and validate chattel assets used as mortgage for loan applications. Even worse, some bad actors commit fraudulent activities by taking advantage of loopholes (i.e. no monitoring and lack of shared information), which damages both the financial and the chattel asset industries.

To resolve and avoid the unnecessary high risks borne by both financial and the chattel asset industries, sensor network (SN) and IoT technologies are highly applicable to real-time monitoring and tracking of stored and mobile chattel assets, although such kinds of technologies were not available in the past. However, no single SN or IoT technology will satisfy the entirety of chattel asset monitoring and tracking that can be accepted by stakeholders, especially the financial institution stakeholders. It will be an integrated system of multiple SN and IoT technologies, which will satisfy the requirements of the stakeholders.

By standardizing the system requirements of the integrated IoT/SN system, the real-time, on-demand, continual mobile asset monitoring and tracking can be achieved, for example, to verify the chattel assets' physical characteristics (weight, volume, location, etc.) during storage and in transit, to evaluate the chattel assets' true and actual market values, to validate the legitimacy of the chattel assets, etc.

This document promotes the development of the integrated IoT/SN platform for chattel asset mortgage management, which enables on-demand, real-time, continual chattel asset monitoring and tracking with verification, quantification, evaluation, and validation. This standardized integrated platform prevents fraudulent activities, protecting the chattel assets owned by the mobile asset industry and reducing unnecessary high risks borne by the financial institution. Furthermore, this document fills the gap between financial systems and the integrated platform utilizing the SN and IoT technologies.

INTERNET OF THINGS (IoT) – SYSTEM REQUIREMENTS OF IOT AND SENSOR NETWORK TECHNOLOGY-BASED INTEGRATED PLATFORM FOR CHATTEL ASSET MONITORING

1 Scope

This document specifies the system requirements of an Internet of Things (IoT) and Sensor Network (SN) technology-based platform for chattel asset monitoring supporting financial services, including:

– system infrastructure that describes functional components;

– system and functional requirements during the entire chattel asset management process, including chattel assets in transition, in/out of warehouse, storage, mortgage, etc.;

– performance requirements and performance specifications of each functional component;

– interface definition of the integrated platform system.

This document is applicable to the design and development of IoT/SN system for chattel asset monitoring supporting financial services.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

No terms and definitions are listed in this document.

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

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

4 Abbreviated terms

ACD access and communication domain

ASD application and service domain

OMD operation and management domain

PED physical entity domain

RA reference architecture

SCD sensing and controlling domain

UD user domain

5 Motivation

The chattel mortgage process usually consists of five steps, as shown in Figure 1.

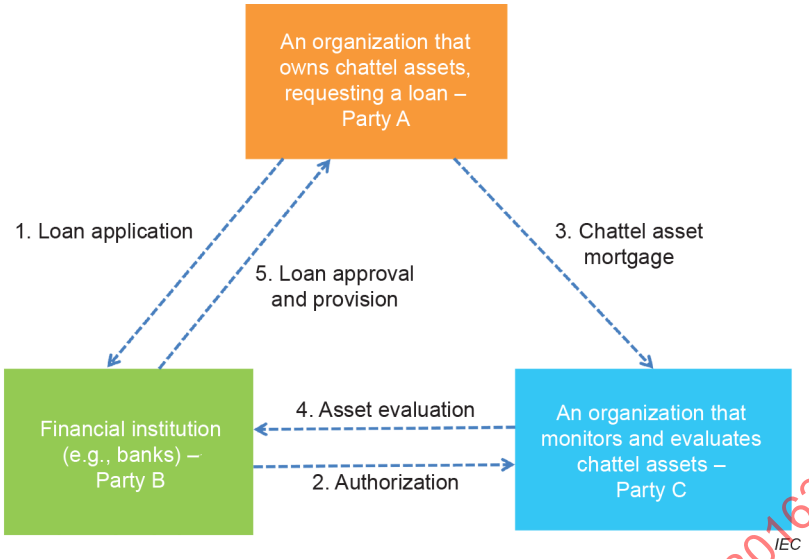

Figure 1 – Involved parties and their relationships in chattel mortgage financial services

1) Party A submits loan applications to Party B.
2) Party B authorizes Party C to deliver the chattel mortgage service, which is an organization responsible for monitoring and evaluating the chattel assets, usually owned by a third-party.
3) Party A mortgages its chattel asset to Party C.
4) Party C issues chattel asset evaluation for Party B, which acts as an important evidence in judging the loan repayment capacity of Party A.
5) After reviewing the loan application from Party A, the loan application evaluation by Party B, and the asset validation and evaluation report from Party C, Party B makes its final decision whether or not to approve the loan application from Party A.

Traditionally the responsibilities of Party C have been taken by humans, which makes the mobile assets vulnerable to fraudulent activities. For example, Company A applies for loans from Bank A using chattel mortgage, where mobile assets are stored in Warehouse A. However, Company B can illegally use mobile assets stored in Warehouse A that belong to Company A to apply for loans from Bank B. This case can occur because Bank B has no information for mobile assets stored in Warehouse A. The information asymmetry between banks causes lack of effective management on monitoring collateral assets. Another example could be that Company A illegally delivers those mobile assets stored in Warehouse A to Warehouse B for repeated applications for loans from Bank B. This can also occur because there is no standardized management for in- and out-of-warehouse check of collateral assets. To avoid the unnecessary loss of both financial and the chattel asset industries, this document provides the standardization of the IoT/SN platform, which integrates multiple SN and IoT technologies to realize the real-time, on-demand, continual chattel asset monitoring and tracking.

6 System infrastructure description of the integrated IoT/SN system

Figure 2 illustrates the system infrastructure of the IoT/SN integrated system for chattel asset and mortgage management. This system consists of six domains, which are in accordance with the IoT Reference Architecture (IoT RA) specified in ISO/IEC 30141.

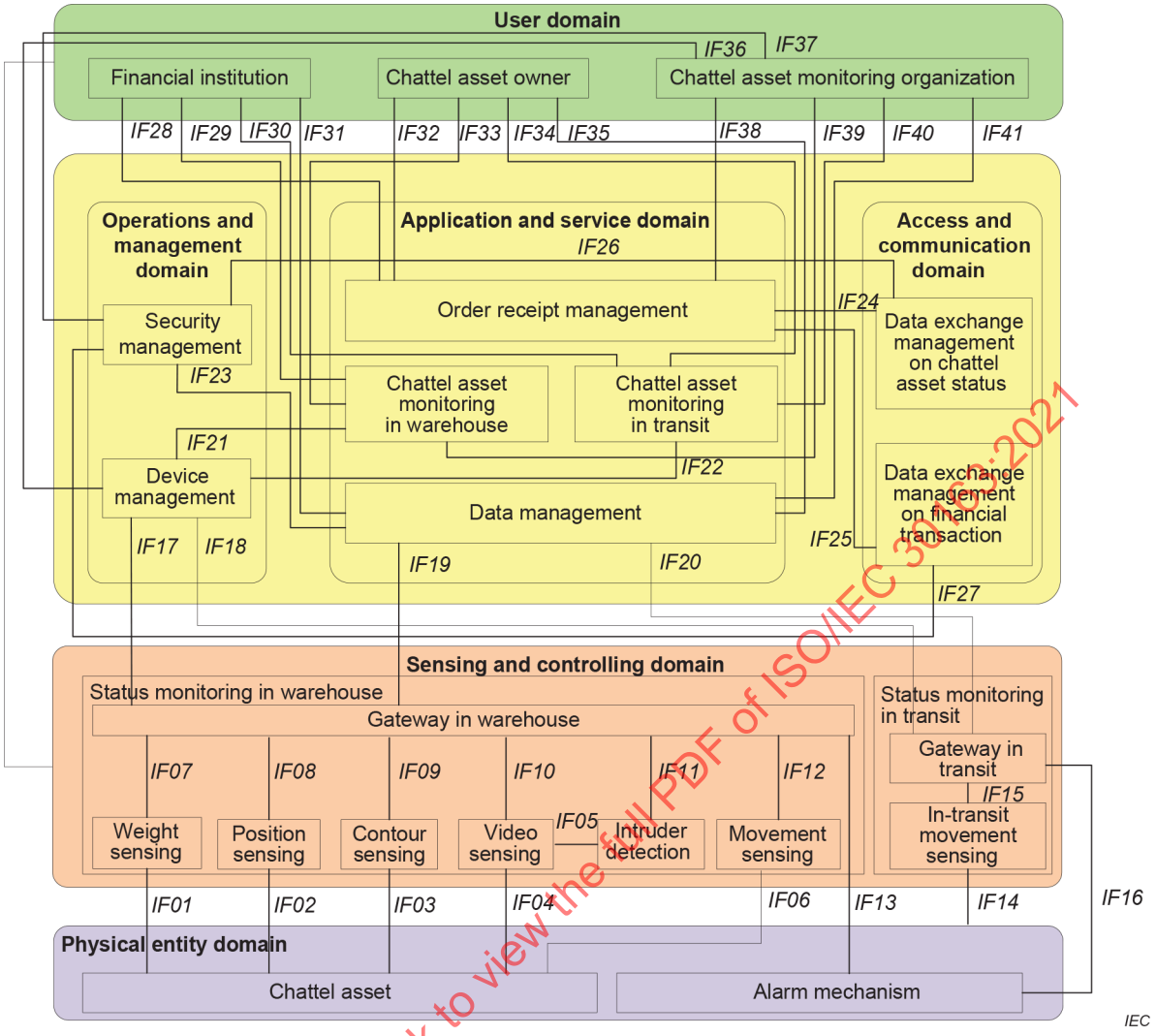

Figure 2 – System infrastructure of the IoT/SN integrated system

Each domain that maps to the IoT RA as shown in Figure 2 is described below.

1) Physical entity domain (PED) consists of chattel assets being monitored and tracked, where the examples of chattel assets can be steel coil, minerals, textile raw materials, etc.
2) Sensing and controlling domain (SCD) realizes sensing and controlling of the chattel assets. It contains functional entities for weight sensing, position sensing, contour sensing, video sensing, movement sensing, etc.
3) Application and service domain (ASD) provides asset monitoring and tracking services for the users in the user domain (UD), which is categorized into two levels: basic service and business service. Basic service provides support for business services, for example, data management. Business service offers specific services for the users, including stock monitoring in warehouse, in- and out-of-warehouse management, alarming management, etc.
4) Operation and management domain (OMD) provides system operational maintenance.
5) Access and communication domain (ACD) offers data and information access with external entities, for example, financial institutions' systems and platforms.

6) User domain (UD) includes the users for the system: financial institutions, chattel asset owners, chattel asset monitoring organization, etc. Chattel asset owner is the organization that owns chattel assets and requests a loan, which is Party A in Figure 1. Financial institutions usually mean banks, which are Party B in Figure 1 to provide loans for the chattel asset owner. Chattel asset monitoring organization is responsible for asset monitoring, which maps to Party C in Figure 1.

In this document, the general system functional and performance requirements for the IoT/SN integrated platform, which includes the entities in UD, OMD, ASD, ACD, and SCD, are specified. Additionally, the high-level, general interface descriptions between the entities are also described. Any requirements or interface descriptions related to financial transactions and processing are out of scope of this document.

7 System requirements of the IoT/SN technology-based integrated platform

7.1 General system functional requirements for the integrated platform

7.1.1 General

The general system functional requirements for the integrated platform are provided in 7.1 for the relevant domains shown in Figure 2, i.e. UD, OMD, ASD, ACD, and SCD. The software of the integrated platform should be upgradable by subsystem software modules.

7.1.2 Functional requirements for the entities in UD

7.1.2.1 Financial institution

Upon request, the financial institution shall receive order-related business data and the real-time video data of the chattel asset. In addition, when some unexpected events occur to the chattel asset, the financial institution shall receive an alarm with the event recording data.

7.1.2.2 Chattel asset owner

Upon request, the chattel asset owner shall receive order-related business data and the real-time video data of the chattel asset. In addition, when some unexpected events occur to the chattel asset, the chattel asset owner shall receive an alarm with the event recording data.

7.1.2.3 Chattel asset monitoring organization

Upon request, the chattel asset monitoring organization shall receive order-related business data and the real-time video data of the chattel asset. In addition, when some unexpected events occur to the chattel asset and the devices, or some unexpected security events occur, the chattel asset monitoring organization shall receive an alarm with the event recording data.

7.1.3 Functional requirements for the entities in OMD

7.1.3.1 Device management

The device management shall perform device configuration and maintain the operation status of the devices via local or remote management, including log recording, fault diagnosis, firmware management, power management, etc.

During normal operations, the device management shall receive operation and maintenance status from the gateway in warehouse and the gateway in transit.

When an unexpected event occurs at a device or devices and such an event is detected at the device management, the device management shall generate and send an alarm message with the relevant event recording data to the chattel asset monitoring organization as a dynamic interactive service.

7.1.3.2 Security management

The security management shall ensure network security and user privacy:

– illegal external access and terminal access shall be prohibited; and
– the user's information shall have authenticity, integrity and confidentiality, which are protected against any unauthorized access.

During normal operations, the security management shall receive sensing data of the chattel asset from the ASD, and exchange data of chattel status as well as that of financial transaction from external systems for the sake of secure data transmission.

When an unexpected event occurs, the security management shall send an alarm with relevant event recording data to chattel asset monitoring organization in the UD.

7.1.4 Functional requirements for the entities in ASD

7.1.4.1 Order receipt management

The order receipt management shall perform management with respect to the order of chattel mortgage business, for example, order creation, order information enquiry, order information update, order lock/release, etc. It shall receive the order operation instructions from the chattel asset monitoring organization, such as adding, deleting, modifying the orders. It shall send the chattel asset business data, including chattel asset status data (e.g. chattel asset type, specification, quantity, stock position) and chattel asset transaction data (e.g. pledgee, pledger, order number, order amount), to the ACD and the UD.

7.1.4.2 Chattel asset monitoring in warehouse

The chattel asset monitoring in warehouse shall receive in-warehouse monitoring tasks from the chattel asset monitoring organization in the UD and send back the execution data of the tasks.

– While the chattel assets are in the warehouse, it shall provide real-time monitoring of the chattel asset status, for example, it provides real-time stock position status enquiry and update.
– In addition, the chattel asset monitoring in warehouse shall provide in- and out-of-warehouse management through remote operations. For example, when chattel assets are delivered into warehouses, it shall perform information entry of chattel assets, the preliminary examination of chattel assets, the assignment of in-warehouse delivery, etc. When chattel assets are delivered out of warehouses, it shall perform the verification of chattel asset information, the assignment of out-of-warehouse delivery, etc.

When some unexpected events occur to the devices, the chattel asset monitoring in warehouse shall receive the alarm with relevant event recording data from the OMD. In addition, it shall send an alarm with event recording data to the UD when unexpected events are detected for the chattel asset, for example, unauthorized removal of the chattel asset.

7.1.4.3 Chattel asset monitoring in transit

The chattel asset monitoring in transit shall receive in-transit monitoring tasks from the chattel asset monitoring organization in the UD and send back the execution data of the tasks. It shall provide real-time monitoring of the chattel asset status (e.g. vibration, tilting).

When some unexpected events occur to the devices, the chattel asset monitoring in transit shall receive the alarm with relevant event recording data from the OMD. In addition, it shall send an alarm with event recording data to the UD when unexpected events are detected for the chattel asset, for example, severe vibration of the chattel asset.

7.1.4.4 Data management

The data management shall store and process the data of the integrated platform. It shall receive sensing data of the chattel asset from the gateways in the SCD and send the real-time video data of chattel asset to the UD upon request. In addition, it can send the sensing data to the OMD for the sake of secure transmission.

The data management shall have backup and shall not be lost when unexpected disaster occurs, for example, system power off. The data shall be recovered after the system is resumed.

7.1.5 Functional requirements for the entities in the ACD

7.1.5.1 Data exchange management on chattel asset status

The data exchange management on chattel asset status shall realize data exchange on chattel asset status for the ASD and OMD with external systems. It shall receive the chattel asset status data from the ASD. In addition, it shall send the exchange data of chattel asset status received from external systems to the OMD.

7.1.5.2 Data exchange management on financial transaction

The data exchange management on financial transaction shall realize data exchange on financial transaction for the ASD and OMD with external systems. It shall receive the chattel asset transaction data from the ASD. In addition, it shall send the exchange data of chattel asset financial transaction from external systems to the OMD.

7.1.6 Functional requirements for the entities in the SCD

7.1.6.1 Weight sensing

The integrated platform shall acquire the weight data of the chattel asset in the warehouse using the weight sensing subsystem.

The weight sensing subsystem will trigger early warning when the gross weight declared in the order receipt exceeds ±5 % of the actual gross weight of the chattel asset.

7.1.6.2 Position sensing

The integrated platform shall acquire the position data of the chattel asset using the position sensing subsystem.

The position sensing subsystem shall trigger alarms in the following cases:

– the actual stock position of the chattel asset differs from that as declared in the order receipt; and
– the chattel asset is placed in an unauthorized area in the warehouse.

7.1.6.3 Contour sensing

The integrated platform shall acquire the three-dimensional contour and the volume of the chattel assets using the contour sensing subsystem.

The contour sensing subsystem shall trigger early warning when it cannot finish scanning of the contour within a certain period of time or the chattel asset is obstructed from the scanning field of view.

The contour sensing subsystem shall trigger alarms when the actual volume of the chattel asset differs from the declared volume in the order receipt.

7.1.6.4 Video sensing

The integrated platform shall acquire the video streaming data in the monitoring area of a warehouse.

The video sensing subsystem will trigger early warning when the chattel asset in the monitoring area is removed without any authorization. The warehouse administrators need to check the early warning and trigger alarms manually after confirmation.

7.1.6.5 Intruder detection

The integrated platform shall analyse and determine the intrusion behaviour via video analytics. The video analytics can be performed locally by using a computer vision technology for the monitoring area of a warehouse.

– For the case of human intrusion during warehouse off-hours, the alarm systems in all entries (e.g. windows, doors, gates, elevators, passage, etc.) shall be activated. When the alarm systems detect any movements, alarm(s) shall be sent to the operators on duty.
– A gate for car license-plate recognition shall be used at the entrance of the chattel asset monitoring area. After the system is armed, if a car breaks through the gate, the emergency response system – such as auto-controlled tyre spikes, automatic road blockers, or automatic retractable bollards – shall be triggered to prevent its entry.

7.1.6.6 Movement sensing

When the monitored chattel asset is in the warehouse or in transit, the platform shall identify the chattel asset, acquire and analyse the status of the chattel asset – vibration, tilting, etc. – by movement sensing. In addition, it sends alarms to the integrated platform via the gateway when the following events occur:

– the movement sensing subsystem detects that the chattel asset is moved without receiving any command or does not match the order receipt specification;
– the movement sensing unit is maliciously destroyed or lost, leading to the platform not being able to receive the status pinging signal response from it; and
– the battery power of the movement sensing subsystem is lower than the pre-set power level.

7.1.6.7 Gateway in warehouse

The gateway in warehouse shall acquire the status information of the chattel asset in the warehouse using the subsystems of weight sensing, position sensing, contour sensing, etc., and shall send it to the platform.

7.1.6.8 Gateway in transit

The platform shall acquire the status information of the chattel asset in transit: whether the chattel assets are moved from the vehicle or not, whether there are dangerous actions leading to the risk of the chattel assets being damaged or not, etc. In addition, the platform acquires the location of the vehicle via the gateway in transit. The gateway in transit sends alarms to the integrated platform when it is maliciously removed, or its battery power is too low.

7.2 General system performance requirements for the integrated platform

7.2.1 General

The general system performance requirements are provided in 7.2 for the relevant domains shown in Figure 2, i.e. UD, OMD, ASD, ACD, and SCD.

In 7.2.2, the performance requirements for the entities in the UD are specified by the response times related to an enquiry service, a static interactive service, and a dynamic interactive service. The performance requirements for the entities in the OMD, ASD, and ACD are identified by the types of messages between entities without specifying the time requirements, for example, the time durations for message generation, message transmission, etc. However, the sum of all entities involved in the enquiry service, the static interactive service, and the dynamic interactive service shall meet each response time performance requirements.

In 7.2.3, the performance requirements for the entities in SCD are specified.

7.2.2 Performance requirements for the entities in the UD, OMD, ASD, and ACD

7.2.2.1 Performance requirements of the response times for the entities in the UD

– Enquiry service response time: The response time shall be less than three seconds for enquiry service, which provides the users with relevant information about the chattel asset on enquiry, for example, financial institutions check chattel asset location via the platform.

– Static interactive service response time: The response time shall be less than one second for static interactive service, through which users submit input information to the integrated platform without requesting feedback from the platform, for example, users fill in a registration form of the platform.

– Dynamic interactive service response time: The response time shall be less than four seconds for dynamic interactive service, through which users submit input information to the integrated platform that needs feedback from the platform, for example, chattel asset monitoring organization uploads supporting files, pictures to the platform to verify the status of the chattel asset.

7.2.2.2 Performance requirements of the response times for the entities in the OMD

7.2.2.2.1 Device management

The functional requirements of the device management are specified in 7.1.3.1.

The time to process the event occurrence data from the gateways, to generate the alarm message with the relevant event data, and to transmit the alarm message shall be sufficiently small such that when it is summed up with all other times involved in providing the dynamic interactive service, the overall response time is within the four-second performance requirement.

7.2.2.2.2 Security management

The functional requirements of the security management are specified in 7.1.3.2.

The time to receive the sensing data from the ASD, to generate and deliver the alarm message with the relevant event data shall be sufficiently small such that when it is summed up with all other times involved in providing the dynamic interactive service, the overall response time is within the four-second performance requirement.

7.2.2.3 Performance requirements for the entities in the ASD

7.2.2.3.1 Order receipt management

The functional requirements of the order receipt management are specified in 7.1.4.1.

The time to receive the order operation instructions from the chattel asset monitoring organization or to transmit the chattel asset business data upon request shall be sufficiently small such that when it is summed up with all other times involved in providing the dynamic interactive service and enquiry service, the overall response times are within the four-second and three-second performance requirements, respectively.

7.2.2.3.2 Chattel asset monitoring in warehouse

The functional requirements of the chattel asset monitoring in warehouse are specified in 7.1.4.2.

The time to receive in-warehouse monitoring tasks from the chattel asset monitoring organization, to transmit execution data of the tasks, to generate and deliver the alarm message with the relevant event data shall be sufficiently small such that when it is summed up with all other times involved in providing the dynamic interactive service, the overall response time is within the four-second performance requirement.

7.2.2.3.3 Chattel asset monitoring in transit

The functional requirements of the chattel asset monitoring in transit are specified in 7.1.4.3.

The time to receive in-transit monitoring tasks from the chattel asset monitoring organization, to transmit execution data of the tasks, to generate and deliver the alarm message with the relevant event data shall be sufficiently small such that when it is summed up with all other times involved in providing the dynamic interactive service, the overall response time is within the four-second performance requirement.

7.2.2.3.4 Data management

The functional requirements of the data management are specified in 7.1.4.4.

The time to receive and process the sensing data from the SCD, to transmit the sensing data to the OMD, or to transmit the real-time video data upon request shall be sufficiently small such that when it is summed up with all other times involved in providing the dynamic interactive service and enquiry service, the overall response times are within the four-second and three-second performance requirements, respectively.

7.2.2.4 Performance requirements for the entities in the ACD

7.2.2.4.1 Data exchange management on chattel asset status

The functional requirements of the data exchange management on chattel asset status are specified in 7.1.5.1.

The time to process the chattel asset status data from the ASD and to transmit the exchange data of chattel asset status received from external systems shall be sufficiently small such that when it is summed up with all other times involved in providing the dynamic interactive service, the overall response time is within the four-second performance requirement.

7.2.2.4.2 Data exchange management on financial transaction

The functional requirements of the data exchange management on financial transaction are specified in 7.1.5.2.

The time to process the chattel asset transaction data from the ASD and to transmit the exchange data of chattel asset financial transaction from external systems shall be sufficiently small such that when it is summed up with all other times involved in providing the dynamic interactive service, the overall response time is within the four-second performance requirement.

7.2.3 Performance requirements for the entities in the SCD while in warehouse

7.2.3.1 Weight[1] sensing subsystem

The performance requirements of the weight sensing are shown in Table 1.

Table 1 – Performance requirements of weight sensing

Parameters	Performance requirements
Weighing accuracy	The weighing accuracy, A, is defined as: $A = (W_m - W_a) / W_a \times 100\,\%$, where W_m is the measured weight value of the chattel asset; and W_a is the actual weight. The weighing accuracy, A, shall be less than or equal to 5 %.

7.2.3.2 Position sensing subsystem

The performance requirements of the position sensing are shown in Table 2.

Table 2 – Performance requirements of position sensing

Parameters	Performance requirements
Position accuracy in warehouse	Shall be no greater than 10 centimetres
Positioning response time	Shall be no greater than one second, depending on network status. (If the network becomes unavailable, there will be no data transmitted.)

7.2.3.3 Contour sensing subsystem

The performance requirements of the contour sensing are shown in Table 3. In order to improve the measurement accuracy, jitters shall be avoided if laser radar scanning is used.

Table 3 – Performance requirements of contour sensing

Parameters	Performance requirements
Volume inconsistency threshold	Shall be no greater than ±10 %
Time limit of contour sensing	Shall be no greater than 600 seconds

7.2.3.4 Video sensing subsystem

The performance requirements of the video sensing are shown in Table 4.

[1] In this document, the mass of an object is referred to as its weight although in fact these two are not the same.

Table 4 – Performance requirements of video sensing

Parameters	Performance requirements
Camera resolution	Support at least 720P HD with focal plane array (FPA) of 1280 × 720.
Response time of chattel asset movement detection	Shall be less than 15 seconds

7.2.3.5 Intruder detection subsystem

The performance requirements of the unauthorized access or intruder detection are shown in Table 5.

Table 5 – Performance requirements of unauthorized access or intruder detection

Parameters	Performance requirements
Response time of intrusion detection	Shall be less than three seconds

7.2.3.6 Gateway in warehouse

The performance requirements of the gateway in warehouse are shown in Table 6.

Table 6 – Performance requirements of gateway in warehouse

Parameters	Performance requirements
Working temperature	−20 °C to 60 °C

7.2.4 Performance requirements for the entities in the SCD while in transit

7.2.4.1 In-transit movement sensing

The performance requirements of the movement sensing are shown in Table 7.

Table 7 – Performance requirements of in-transit movement sensing

Parameters	Performance requirements
Working temperature	−10 °C to 50 °C
Endurance	Shall be no less than three months
Permissible use time after low power consumption	Shall be no less than 72 hours
Alarm response time	Shall be no greater than 10 seconds
Battery life	Shall be no less than two years

7.2.4.2 Gateway in transit

The performance requirements of the gateway in transit are shown in Table 8.

Table 8 – Performance requirements of gateway in transit

Parameters	Performance requirements
Working temperature	−20 °C to 60 °C
Position accuracy in-transit	Shall be within 20 metres. (This requirement is dependent on a number of conditions, e.g. weather, geography, affecting the availability of the GPS satellites, and also on network connectivity. It is possible that the data will not be obtained in certain situations.)
Acceleration sensing	Shall detect the start of vehicle movement with response time less than one second. Shall detect the vehicle's return to the static state with the response time less than 30 seconds. Can effectively filter out the relevant interference, such as opening and closing car doors, surrounding vibration and other external interference sources.
Alarm response time	Shall be no greater than 15 seconds

8 System interface descriptions between the entities

The system interfaces are shown in Figure 2, which describes the logical relations or connections between domains. Table 9 describes the interfaces between Entity 1 and Entity 2. The interface in Table 9 is unidirectional from Entity 1 to Entity 2 unless indicated otherwise in the interface description.

Table 9 – Interface description

Interface	Entity 1	Entity 2	Interface description
IF01	Chattel asset	Weight sensing	Weight sensing acquires weight data of the chattel asset through this interface.
IF02	Chattel asset	Position sensing	Position sensing acquires location data of the chattel asset through this interface.
IF03	Chattel asset	Contour sensing	Contour sensing acquires contour data of the chattel asset through this interface.
IF04	Chattel asset	Video sensing	Video sensing acquires photo, audio and video data of the chattel asset through this interface.
IF05	Video sensing	Intruder detection	Video sensing sends video information of the chattel asset in the warehouse monitoring area to intruder detection through this interface. The information is further analysed by intruder detection for determining the intrusion behaviour.
IF06	Chattel asset	Movement sensing	Movement sensing acquires the status of the chattel asset (e.g. displacement, tilting) through this interface, to determine whether there exists potential risk of damage to the chattel asset, etc.
IF07	Weight sensing	Gateway in warehouse	Weight sensing sends weight data of the chattel asset to gateway in warehouse through this interface.
IF08	Position sensing	Gateway in warehouse	Position sensing sends position data of the chattel asset to gateway in warehouse through this interface.

Interface	Entity 1	Entity 2	Interface description
IF09	Contour sensing	Gateway in warehouse	Contour sensing sends contour data of the chattel asset to gateway in warehouse through this interface.
IF10	Video sensing	Gateway in warehouse	Video sensing sends photo, audio and video data of the chattel asset to gateway in warehouse through this interface.
IF11	Intruder detection	Gateway in warehouse	When intrusion is detected (e.g. some bad actors steal the chattel asset), intruder detection sends intrusion event recording data, such as intrusion time, screenshot, to gateway in warehouse through this interface.
IF12	Movement sensing	Gateway in warehouse	When some unexpected events occur to movement sensing (e.g. being removed maliciously, low battery), movement sensing sends alarm recording data, such as alarm occur time, alarm reason, to gateway in warehouse through this interface.
IF13	Gateway in warehouse	Alarm mechanism	When unusual conditions are detected (e.g. unauthorized removal of the chattel asset from the warehouse), or some unexpected events occur to movement sensing (e.g. being removed maliciously), gateway in warehouse sends alarm instructions to alarm mechanism (e.g. audio-visual alarm, tyre spikes) through this interface.
IF14	Chattel asset	In-transit movement sensing	Movement sensing acquires the status of the chattel asset (e.g. vibration, tilting) through this interface, to determine whether there exists potential risk of damage to the chattel asset, etc.
IF15	In-transit movement sensing	Gateway in transit	When some unexpected events occur to movement sensing (e.g. being removed maliciously, low battery), movement sensing sends alarm recording data to gateway in transit, such as alarm occur time, alarm reason.
IF16	Gateway in transit	Alarm mechanism	When unusual conditions are detected (e.g. severe vibration of the chattel asset), or some unexpected events occur to movement sensing (e.g. being removed maliciously), gateway in transit sends alarm instructions to alarm mechanism (e.g. audio-visual alarm) through this interface.
IF17	Gateway in warehouse	Device management	Gateway in warehouse sends its operation and maintenance status to device management through this interface, such as configuration parameters, failure description.
IF18	Gateway in transit	Device management	Gateway in transit sends its operation and maintenance status to device management through this interface, such as configuration parameters, failure description.
IF19	Gateway in warehouse	Data management	Gateway in warehouse sends sensing data of the chattel asset in warehouse (e.g. weight data, position data) to data management through this interface.
IF20	Gateway in transit	Data management	Gateway in transit sends sensing data of the chattel asset in transit (e.g. vibration, tilting) to data management through this interface.
IF21	Device management	Chattel asset monitoring in warehouse	When devices are in unusual conditions (e.g. device failure), device management sends alarm recording data, such as alarm occur time, alarm reason, to chattel asset monitoring in warehouse through this interface.