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 It also gives information on projects, replaced and withdrawn publications.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.

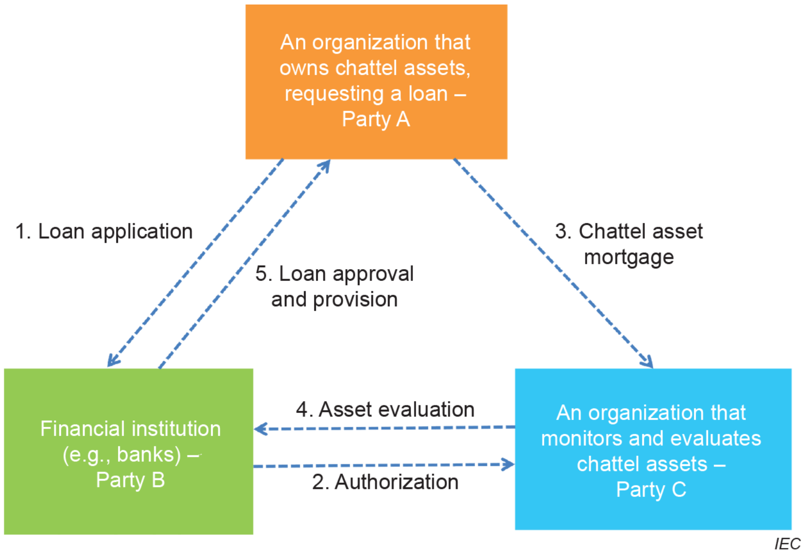

Figure 1 – Involved parties and their relationships in chattel mortgage financial services

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.

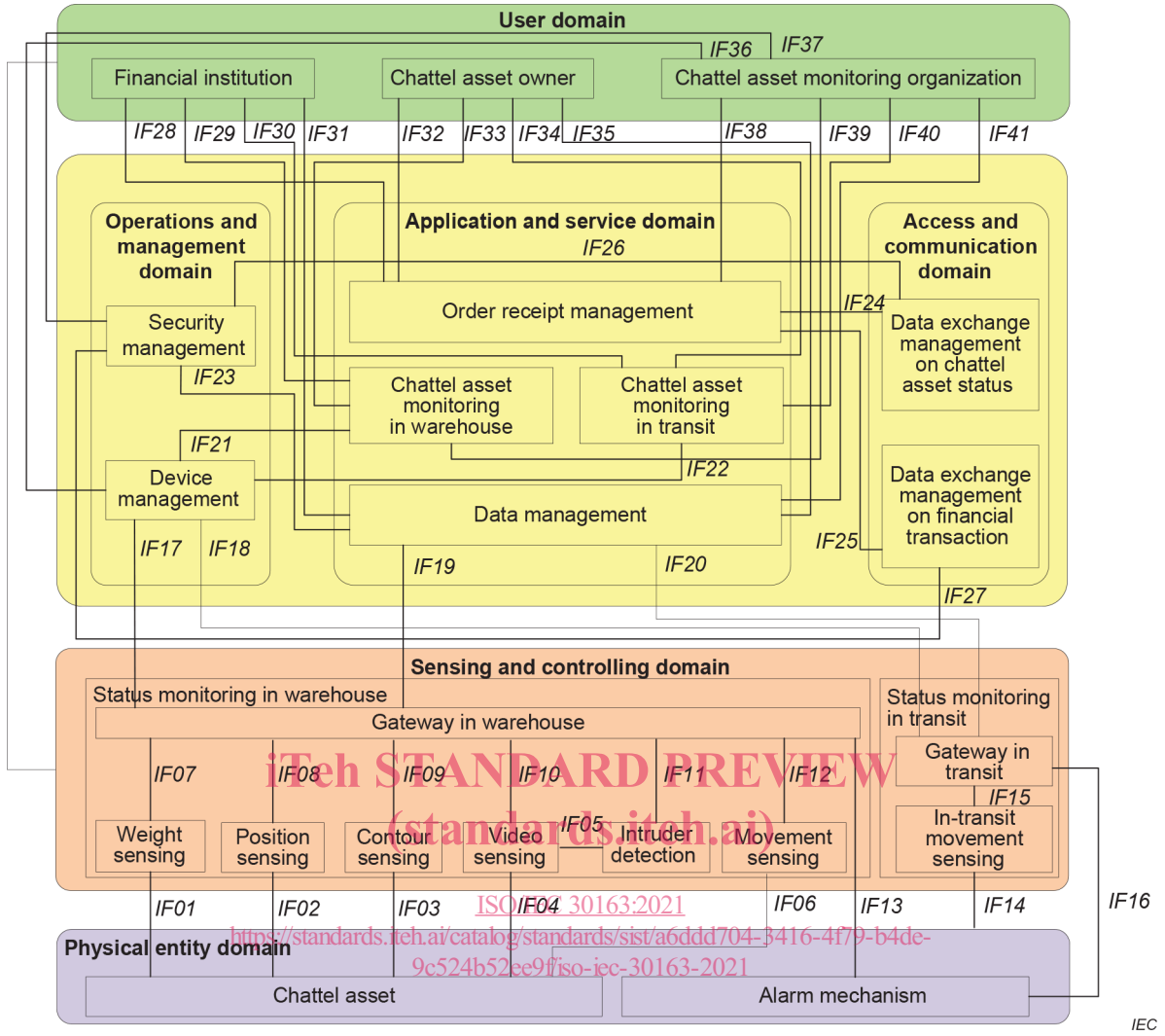

Figure 2 – System infrastructure of the IoT/SN integrated system

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.