ISO/IEC 30162

Edition 1.0 2022-02

INTERNATIONAL STANDARD

colour inside

Internet of Things (IoT) – Compatibility requirements and model for devices within industrial IoT systems

ISO/IEC 30162:2022-02(en)

IEC Secretariat
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 It also gives information on projects, replaced and withdrawn publications.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 Products & Services Portal - products.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 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

ISO/IEC 30162

Edition 1.0 2022-02

INTERNATIONAL STANDARD

colour inside

Internet of Things (IoT) – Compatibility requirements and model for devices within industrial IoT systems

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040; 35.020; 35.240.50

ISBN 978-2-8322-1073-2

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNET OF THINGS (IoT) – COMPATIBILITY REQUIREMENTS AND MODEL FOR DEVICES WITHIN INDUSTRIAL IoT SYSTEMS

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.

ISO/IEC 30162 has been prepared by subcommittee 41: Internet of Things and Digital Twin, of ISO/IEC joint technical committee 1: Information technology. It is an International Standard.

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

FDIS	Report on voting
JTC1-SC41/251/FDIS	JTC1-SC41/265/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1, available at www.iec.ch/members_experts/refdocs and www.iso.org/directives.

IMPORTANT – The "colour inside" logo on the cover page of this document 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

Dynamic growth and embracing of digital technologies in all spheres of human life has created the conducive basis for transitioning toward the digital economy, while adoption of Industrial Internet of Things (IIoT) is one of the major technology directions of the digital economy growth. As it is essential to implement IIoT technologies in enterprises worldwide, the issue of practical aspects in the realization of the IIoT concepts has gained vital importance. In particular, one of the existing problems is unavailability of transparent mechanisms in terms of how and in what way to establish connections of industrial equipment to cloud platforms designed for data collection and analysis.

As soon as numerical programmable tools became widely available, the development of technologies and protocols enabling management and control of the industrial equipment control software utility within an enterprise network became necessary. At that time, management of such control utility over Internet was out of question. In parallel, a number of concerns arose due to the design and development of proprietary technologies and protocols; in most cases, they are incompatible with each other. Since such technologies and protocols were the intellectual property (IP) of the relevant enterprise, no legal framework describing structure and operation principles of such technologies and protocols existed. As the IIoT concept started to appear, activities aimed at standardizing and documenting the previously developed technologies and protocols began. As a result of the analysis of existing protocol elements, a document having a general list or register of protocols was developed. Notwithstanding, the compiled document contained just descriptions of the existing set of technologies and protocols, without the information about their ability to interact with each other, or about the methods of connecting to cloud-based platforms. Each manufacturer built the systems based on those protocols that the manufacturer considered to be the most suitable for solving specific tasks. Numerous manufacturers' equipment use specific protocols that were specially developed by the manufacturers for the management and data delivery tasks for different industrial solutions. For instance, the protocols described in IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, Modbus, DNP3, etc. are widely used today.

In the initial stages, developers and large enterprises insisted on using their own proprietary protocols, arguing that their protocols were designed and developed for executing specific functions. For instance, IEC 61850 (describing some protocols) is widely applied for power substations while Modbus is used for transmitting raw data from pressure sensors. Controller area network (CAN) technology is mostly adopted in the automotive industry and robotics (see ISO 11898 series). As a variety of protocol versions started to emerge, different version and metadata format incompatibility became apparent. A majority of production hardware supports Modbus-RTU and Modbus-ASCII, while a more advanced version of Modbus-TCP protocol no longer requires such complications as RTU and ASCII. The major problems are data conversion from one protocol to another and protocol identification using certain attributes (semantic) for seamless interoperability of the IIoT devices and platforms. The interoperability issues can be resolved by defining particular compatibility requirements for the IIoT devices, applications, systems, components, and other IIoT entities.

This document specifies compatibility requirements for various entities of the IIoT systems that can be used as guidance for connecting, configuring and testing of industrial hardware.

INTERNET OF THINGS (IoT) – COMPATIBILITY REQUIREMENTS AND MODEL FOR DEVICES WITHIN INDUSTRIAL IoT SYSTEMS

1 Scope

This document specifies network models for IIoT connectivity and general compatibility requirements for devices and networks within IIoT systems in terms of:

a) data transmission protocols interaction;

b) distributed data interoperability and management;

c) connectivity framework;

d) connectivity transport;

e) connectivity network;

f) best practices and guidance to use in IIoT area.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

3.1
co-existence
degree to which a product can perform its required functions efficiently while sharing a common environment and resources with other products, without detrimental impact on any other product

[SOURCE: ISO/IEC 25010:2011, 4.2.3.1]

3.2
compatibility
degree to which a product, system or component can exchange information with other products, systems or components, and/or perform its required functions, while sharing the same hardware or software environment

[SOURCE: ISO/IEC 25010:2011, 4.2.3]

3.3
edge gateway
heterogeneous IoT gateway that takes part in functionality of mobile edge host, especially its data processing functions

3.4
IIoT compatibility
degree to which an industrial system, information resource or other IIoT entity can exchange information with any other IIoT entities, and/or perform its required functions, while sharing the same hardware or software environment and network

Note 1 to entry: Compatibility includes interoperability and co-existence in accordance with Annex A of ISO/IEC 25010:2011.

[SOURCE: ISO/IEC 25010:2011, 4.2.3, modified – "a product, system or component" has been replaced with "an industrial system, information resource or other IIoT entity"; "products, systems or components" has been replaced with "IIoT entities"; and "and network" has been added after "environment".]

3.5
IIoT service platform
part of an IIoT platform responsible for the interactions with the IIoT end-nodes and for providing services to the user

3.6
Industrial Internet of Things
IIoT
Internet of Things based enabling approach for industrial transformation, by taking advantage of existing and emerging information and communication technologies

[SOURCE: Rec. ITU-T Y.4003]

3.7
industrial Internet connectivity framework
framework for the software development used to develop applications that are responsible for the mutual compatibility of various IIoT application protocols and payload formats for the semantic aspect of the compatibility model

3.8
Industrial Internet of Things gateway
IIoT gateway
entity of an IIoT system which provides interconnection between one or more devices within IIoT systems and external networks for interoperability even in the case of incompatibility or partial compatibility between devices, between devices and networks, and between networks

Note 1 to entry: An IIoT gateway is also known as a heterogeneous IIoT gateway.

Note 2 to entry: An IIoT gateway combines the capabilities of edge gateway and SIIG (semantic Industrial Internet of Things gateway) to solve the problems in order to ensure the compatibility of various communication technologies and protocols between themselves and the Internet and other communication networks for satisfying the industrial sector requirements.

3.9
interoperability
degree to which two or more systems, products or components can exchange information and use the information that has been exchanged

[SOURCE: ISO/IEC 25010:2011, 4.2.3.2]

3.10
semantic Industrial Internet of Things gateway
SIIG
IIoT gateway that ensures the compatibility of IIoT systems in terms of the semantic aspect

Note 1 to entry: The main task of the semantic Industrial Internet of Things gateway is to ensure the mutual compatibility of various application protocols and IIoT payload formats.

3.11
controller area network
CAN
high-integrity bus system for networking intelligent devices within a system

Note 1 to entry: Commonly used in embedded networks for vehicles or medical equipment.

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.872]

4 Description of IIoT compatibility aspects and levels

4.1 IIoT compatibility aspects

4.1.1 General

The compatibility requirements aspect is a separate part of the requirements combined at different technological levels.

Compatibility aspects for the IIoT entities are represented by both functional and non-functional aspects. As defined in ISO/IEC 30141, the physical entities of IoT and IIoT devices are sensors and actuators. The information given in 4.1.2 and 4.1.3 can be found in checklist format in Annex A.

4.1.2 Connectivity functional compatibility description by aspects for the IIoT entities

To determine connectivity functional compatibility requirements for the IIoT entities, the appropriate aspects are as follows.

a) Physical aspect.

Ensuring the IIoT entities' compatibility with regard to data transmission media should address the issues of using the same media for exchanging signals between physical interfaces of data transceivers, of the format for transmitting the signals over the physical channel (analogue, digital) as well as of ensuring the electromagnetic compatibility [ISO/IEC 7498-1, IEC 61000-1-2:2016].

b) Media Access Control (MAC) aspect.

Ensuring the IIoT entities' compatibility at MAC layer should agree on the implementation of controlling the access to data transmission media; addressing possible issues, including the detection and resolution of the network frame collisions; assigning addresses to the nodes in the local area network (LAN) [IEEE 802.1AC-2012, IETF RFC 2637, IETF RFC 2341, IETF RFC 2661].

c) Logical Link Control (LLC) aspect.

Ensuring the IIoT entities' compatibility with regard to data transmission over the provisioned logical link should: (1) help with combining networks of different topologies; (2) support network frame generation and efficient error correction when errors occur during data transmission at MAC level; and (3) facilitate proper data transmission control over the established communications channel [IEEE 802.2-1994].

d) Network aspect.

Ensuring the IIoT entities' compatibility at the network layer should be required for the support of unified addressing scheme and routing of messages. It also helps with quality control, managing and reconfiguring the network logical topology [ISO/IEC 7498-1, IETF RFC 791].

e) Transport aspect.

Ensuring the IIoT entities' compatibility should consider the multiplexing/de-multiplexing compatibility and support of matching options, e.g. for the data transmission over the established connection, control of this transmission, and others [ISO/IEC 7498-1, Rec. ITU-T X.224, Rec. ITU-T X.225, Rec. ITU-T X.234, IETF RFC 1122].

f) Session aspect.

Ensuring the IIoT entities' compatibility should consider the mechanism for communications session set-up and completion over global networks and maintaining and synchronizing sessions [ISO/IEC 7498-1, Rec. ITU-T X.224, Rec. ITU-T X.225, Rec. ITU-T X.234, IETF RFC 1122].

g) Data presentation aspect.

Ensuring the compatibility at the data presentation layer should address possible issues related to different data formats by using special-purpose protocols, covering data coding/decoding according to these protocols and data compression prior to its transmission over a network [ISO/IEC 7498-1, W3C Extensible Markup Language (XML) 1.0 (Fifth Edition), IETF RFC 4506, IETF RFC 7303].

h) Application aspect.

Ensuring the compatibility at the application layer should address possible issues of accessing the network services, exchanging application-specific service messages, error detection and correction [ISO/IEC 7498-1].

i) Measuring and automation aspect.

Ensuring the compatibility of measuring and automation of the IIoT devices (sensors, actuators), and application and services should guarantee the compatibility of the physical interfaces of IIoT sensors/actuators to address issues of interoperating heterogeneous sensors, actuators, and IIoT applications and services [Rec. ITU-T H.810, Rec. ITU-T H.811].

j) Semantic aspect.

Ensuring the semantic compatibility should address the issues of correct interpretation of the information which IIoT devices exchange among each other [Rec. ITU-T Y.4111/Y.2076].

4.1.3 Connectivity non-functional compatibility description by aspects for the IIoT entities

To determine connectivity non-functional compatibility requirements for the IIoT entities, the appropriate aspects are as follows.

a) Version aspect.

Ensuring the version compatibility should aim at providing the capability of interoperation of any earlier or later version of the same software (backward and forward compatibility, respectively) [ISO/IEC/IEEE 9945].

b) Quality of service (QoS) management aspect.

Ensuring the compatibility of QoS management methods should address possible issues of timely processing of data, processing data of various types, optimization factors such as selection of data delivery route, etc. [Rec. ITU-T G.1010, IETF RFC 4594].

c) Security and privacy aspect.

Ensuring the compatibility of methods supporting security of IIoT entities should address the gaps in design and implementation of protection mechanisms and ensures the trustworthiness aspects of these solutions such as data confidentiality and integrity, availability and reliability of service provision, privacy, safety, and resilience of systems and overall IIoT infrastructure [ISO/IEC 27000 to ISO/IEC 27009, Rec. ITU-T X.1362, Rec. ITU-T Y.4806].

d) Compliance aspect.

Ensuring the compatibility with international, national, and industry standards, guidelines, laws and regulations should facilitate the creation of the global informational environment which is used in conformity with a law and boost the transfer of technologies in a way that is considered appropriate for the particular state, administrative unit, community, or industrial sector.

e) Safety aspect.

Ensuring that IIoT function will not intervene, jeopardize implemented safety functions, or affect applied safety measures [IEC 60950-1:2005, IEC 60950-1:2005/AMD1:2009, IEC 60950-1:2005/AMD2:2013, IEC 62368-1:2014, IEC TR 63069: 2019, IEC 61508].

4.2 IIoT compatibility levels

The following compatibility levels for the different aspects of the IIoT entities should be defined.

a) Fully compatible.

In the industrial systems, information resources or other IIoT entities shall be capable of exchanging information and performing their required functions in a shared environment without any need to modify their input and/or output interfaces, protocols, software and hardware means or to introduce converting devices (adapters, gateways, etc.).

b) Compatible.

In the industrial systems, information resources or other IIoT entities shall be capable of exchanging information and performing their required functions in a shared environment by adapting their input and/or output interfaces, used protocols, software and hardware means to each other or to the environment, or introducing converting devices (adapters, gateways, etc.).

c) Partially compatible.

The industrial systems, information resources or other IIoT entities shall be capable of exchanging information to some extent and performing a constrained set of their required functions in a shared environment, probably with the help of additional tools unifying or converting their input and/or output interfaces, used protocols, procedures implemented by their software and hardware means. The partial compatibility may be reached by negotiating the acceptable constraints on functionality among the parties.

d) Incompatible.

The industrial systems, information resources or other IIoT entities are not capable of exchanging information and performing even a constrained set of their required functions in a shared environment due to the drastic differences in technology, functional or non-functional requirements.

5 Compatibility requirements

5.1 Connectivity functional compatibility aspects

5.1.1 Compatibility requirements for physical aspect

In order to ensure compatibility of IIoT entities with regard to the physical aspect the following provisions apply.

a) Data transmission media compatibility. Any network node should support data transmit/receive over the same transmission media or have in place devices ensuring interoperation of segments transmitting data over different media (wire-line: electrical line, copper wire, fibre-optic; wireless: radio-channels, laser, etc.). Compatibility levels in regard to data transmission media support:

   1) Fully compatible. Nodes use one and the same data transmission media.
   2) Incompatible. Special adapters should be employed for compatibility of nodes in the network.

b) Data transmit/receive system compatibility. Physical interfaces of nodes connected to the network should support data transmit/receive based on the selected format of information transmission in the network (analogue, digital). Compatibility levels:

   1) Fully compatible. Network nodes use identical data transmission formats (Example: PSTN device – PSTN device, radio transmitter – radio receiver).

   2) Compatible, if digital-to-analogue or analogue-to-digital converters are used.

c) Electromagnetic compatibility. If wireless data transmission media is used for data transmission in a given network, it is required to ensure network devices' electromagnetic compatibility according to the IEC 61000 series.

5.1.2 Compatibility requirements for MAC aspect

To ensure IIoT system compatibility with regard to the media access the following provisions apply.

a) Media access compatibility. To correctly access data transmission media (DTM), transmit/receive network interfaces of network nodes connected to the common media should have common DTM access synchronization system. Compatibility levels:

   1) Fully compatible. Nodes having access to data transmission media operate on the basis of the same DTM access control technology (Example: CSMA/CA – CSMA/CA).

   2) Incompatible. Nodes having access to data transmission media operate on the basis of various DTM access control technologies (Example: DTDMA – CSMA/CA).

b) Addressing framework compatibility. To ensure correct data exchanges in the MAC layer it is required to provide a common single addressing framework for all the nodes connected to the network. Compatibility levels:

   1) Fully compatible. Network nodes adhere to the common single link layer addressing framework (Example: MAC-48 – MAC-48).

   2) Compatible. Network nodes have different link layer addressing frameworks, but translation mechanisms are provided (Example: EUI-48 – EUI-64).

   3) Incompatible. Network nodes follow different incompatible link layer addressing frameworks (Example: IAB – EUI-64).

c) Compatibility of procedures to detect and mediate data transmission collisions. In order to provide for correct detection and mediation of data transmission collisions it is required to ensure correct interoperation of collision control systems on all networking devices by synchronizing the involved collision detection and mediation protocols (algorithms). Compatibility levels:

   1) Fully compatible. Collision detection and mediation protocols (algorithms) used for network nodes are identical (Example: Reed–Solomon codes – Reed–Solomon codes).

   2) Compatible. This level considers collision avoidance strategy by using additional software or hardware appliances.

   3) Incompatible. Collision detection and mediation protocols (algorithms) used for network nodes are incompatible. Example: Turbo Convolutional Codes – Reed–Solomon codes).

5.1.3 Compatibility requirements for LLC aspect

To ensure IIoT entities' compatibility with regard to data transmission over the provisioned logical link, the following provisions apply.

a) Compatibility of the network topologies, including switching procedures. Compatibility levels:

   1) Fully compatible. Networks at the LLC level support the same or consistent topologies.

   2) Compatible. Networks support different topologies which may be integrated probably by using protocol extensions (Example: IEEE 802.1q).

   3) Incompatible. Networks support substantially different topologies which cannot be integrated.