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 It also gives information on projects, replaced and withdrawn publications.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

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.

b) Compatibility of network frame generation and interpretation. For data to be correctly transmitted over a network it is required to ensure usage of the common network frame format for correct operation of data transmit/receive procedures, network frame generation and interpretation for all the devices on the network. Compatibility levels:

   1) Fully compatible. Network nodes support common technologies responsible for network frame generation and interpretation (Example: IEEE 802.3 – IEEE 802.3).

   2) Compatible. Nodes support different technologies responsible for network frame generation and interpretation, but frame formats coincide with each other (Example: IEEE 802.3 – IEEE 802.11).

   3) Incompatible. Network nodes support different technologies responsible for network frame generation and interpretation (Example: IEEE 802.3 – IEEE 802.15.4).

c) Compatibility of the data transmission control procedure over the established communications channel. A common single data transmission control procedure should be implemented in all network nodes in order to ensure correct data transmission. Compatibility levels:

   1) Fully compatible. Network nodes support the same management procedures of data transmission over the established channel (Example: IEEE 802.3/IP LLC – IEEE 802.3/IP LLC).

   2) Incompatible. Network nodes support different management procedures of data transmission over the established channel (Example: IEEE 802.3/IP LLC – 6LoWPAN).

5.1.4 Compatibility requirements for network aspect

In order to ensure IIoT entities' compatibility for the aspect of global networking the following provisions apply.

a) Routing compatibility. For the accurate delivery of the data to the IIoT entity it is required to ensure joint operation of all IIoT entities (as network nodes) in terms of node identification, look-up for data transmission route over the network and further set-up of a connection between interoperating entities. Routers and similar devices are the main objects that unite the separate network into a global space providing the interconnection capabilities. Thus, the compatibility of network technologies for this is ensured. Compatibility levels:

   1) Fully compatible. Routers implementing their function provide the environment in which the optimal route is computed for every pair of interoperating nodes without any additional efforts (Example: all interacting nodes implement IPv4).

   2) Compatible. Routers implementing their function provide the environment in which the optimal route is computed for every pair of interoperating nodes by using the additional equipment or software.

   3) Partially compatible. Routers implementing their function provide the environment in which the route is computed for every pair of interoperating nodes but cut off the number of available addresses and additional protocol functionality such as encryption, quality of service guarantees, etc. (Example: IPv4–IPv6).

   4) Incompatible. Routers implementing their function provide the environment in which the route cannot be computed for every pair of interoperating nodes (Example: IPv4–LoRaWAN).

b) Network protocol compatibility. As the network layer provides the capability of unifying the separated networks into the single networking environment, it should be defined what the compatibility is in regard to the network protocols. Compatibility levels:

   1) Full compatible. The protocols implemented by IIoT entities are mutually complementary in terms of functions performed in the network layer (example IP–ICMP). Network protocols support joint operation both in the network, and on a detached from network device.

   2) Compatible. The protocols implemented by IIoT entities may co-exist in a network and support joint operation with other network protocols by introducing the additional software and equipment. Network protocols support joint operation both in the network, and on a detached from network device.

3) Incompatible. The protocols implemented by IIoT entities do not support joint operation.

c) Identifier compatibility. To ensure correct data exchanges it is necessary to provide support of same identification/addressing scheme at the network layer of the protocol stack. Compatibility levels:

1) Fully compatible. IIoT entities support the same addressing scheme and the format of identifiers.

2) Compatible. IIoT entities support different addressing schemes but the identifiers can be easily mapped on a one-to-one basis.

3) Partially compatible. One or more of the IIoT entities support the addressing scheme that provides a larger range of address space and not for all used identifiers from that space does a corresponding identifier from another space exist or can such an identifier be found.

4) Incompatible. IIoT entities use different identification systems.

5.1.5 Compatibility requirements for transport aspect

To ensure IIoT entities' compatibility with regard to the transport support, the following provisions apply.

a) Multiplexing/demultiplexing compatibility. To ensure correct data delivery to applications and services implemented by the IIoT entities, the address at the transport layer should contain the additional information sufficient for multiplexing/demultiplexing messages transferred between the IIoT entities. Compatibility levels:

1) Fully compatible. IIoT entities support the same multiplexing/demultiplexing scheme and the format of channel identifiers at the transport layer.

2) Compatible. IIoT entities support different multiplexing/demultiplexing schemes but the identifiers can be easily mapped on a one-to-one basis.

3) Partially compatible. One of the IIoT entities supports the multiplexing/demultiplexing scheme that provides a larger range of identifiers and not for all identifiers from that space does a corresponding identifier from another space exist or can such an identifier be found.

4) Incompatible. IIoT entities use different multiplexing/demultiplexing systems that cannot be mapped on each other.

b) Transport options compatibility. To ensure correct and timely data delivery between network and the IIoT entities it is required to ensure the compatibility of transport layer options supported by these entities, such as connection support, error detection and correction, delivery guarantees, etc. Compatibility levels:

1) Fully compatible. Transport layer protocols for interoperating IIoT entities are the same (Example: TCP – TCP).

2) Compatible. Transport layer options provided by the appropriate protocols allow combining (probably by converting) these protocols without losing the support of any parameters and modes of data transmission at this layer.

3) Partially compatible. Transport layer options provided by the appropriate protocols allow combining (probably by converting) these protocols but cannot guarantee the support of all parameters and modes of data transmission at this layer.

4) Incompatible. Transport protocols for interoperating IIoT entities are different and do not support interoperability feature (Example: SCTP – UDP).

5.1.6 Compatibility requirements for session aspect

To ensure IIoT entities' compatibility in with regard to the session support and management, the following requirements apply.

a) Session delivery and support compatibility. To implement a data exchange capability between IIoT entities and data delivery to a service provided by these entities within an identified session, it is required to ensure compatibility of the addressing nodes, services and sessions. Compatibility levels:

   1) Fully compatible. Network, transport and session protocols used by the IIoT entities are the same and their implementation does not restrict the key features required for the complete, timely and accurate data exchange within every session between these entities according to the established requirements of the session.

   2) Compatible. Network, transport and session protocols used by the IIoT entities are not the same but they may be converted in such a way that supports the complete and accurate data exchange between these entities according to the established requirements of the session.

   3) Partially compatible. Network, transport and session protocols used by the IIoT entities are the same or very similar but their implementation restricts the features required for supporting some options of data exchange between these entities within a session (for example, the possibility of requesting the particular service while the data still may be transferred between the IIoT entities, or the accuracy of data transfer to the service within an identified session while the service itself may be addressed).

   4) Incompatible. Network, transport and session protocols used by the IIoT entities or their implementation restrict the key features required for the data exchange between these IIoT entities.

b) Session control protocol compatibility. To ensure control of a session between two interoperating IIoT entities it is required to provide session protocols compatibility. Compatibility levels:

   1) Fully compatible. Session protocols used by IIoT entities for interoperating nodes are the same.

   2) Compatible. Session protocols used by IIoT entities are very similar but the set of their overlapped features is constrained (for example, timing or QoS options may very).

   3) Incompatible. Session protocols for interoperating IIoT entities are different and do not support interoperability feature of the required type (Example: SCP – H.245).

5.1.7 Compatibility requirements for data presentation aspect

To ensure IIoT entities' compatibility for the data presentation aspect the following requirements apply.

a) Compatibility of data encoding/decoding and compression protocols. To correctly convert data received from application layer protocols and applications into data format suitable for transmission over a network it is required to have in place compatibility of data encoding/decoding and compression protocols with other data encoding/decoding and compression protocols implemented by the IIoT entities. Compatibility levels:

   1) Fully compatible. Data encoding/decoding and compression protocols between interoperating IIoT entities are completely identical.

   2) Compatible. Data encoding/decoding and compression protocols between interoperating IIoT entities are not identical, but are capable of being mutually translated by negotiating the parameters or using converting mechanisms.

   3) Incompatible. Data encoding/decoding and compression protocols between interoperating IIoT entities are different and do not support the mutual translation capability.

b) Encryption/decryption protocols compatibility. In order to set up a secure connection and ensure correct data transmission over such connection, encryption/decryption protocols compatibility is required. Compatibility levels:

   1) Fully compatible. Encryption/decryption protocols used by the IIoT entities are the same, their implementation does not restrict their joint use, and the same algorithms, parameters and key requirements are prescribed for use.

   2) Compatible. Encryption/decryption protocols used by the IIoT entities are the same but their implementation or requirements on algorithms, parameters or encryption keys constrains in a way their joint use but leaves available some options that meet the minimal requirements of all parties (so that they should negotiate on available options).

   3) Partially compatible. Encryption/decryption protocols used by the IIoT entities are the same but their implementation or requirements on algorithms, parameters or encryption keys constrains in some way their joint use without leaving an option that meets the minimal requirements of one or more parties (so that they should negotiate on changing the least risks values or reject the communication).

   4) Incompatible. Encryption/decryption protocols for interoperating IIoT entities are different and do not support the interoperability feature.

5.1.8 Compatibility requirements for application aspect

To ensure IIoT entities' compatibility for the application aspect, the following requirements apply.

a) Application layer protocols' and applications' compatibility. For application layer protocols to operate correctly it is required to ensure compatibility of such protocols with applications that make use of them. Compatibility levels:

   1) Fully compatible. Applications implement part of their functionality specifically for a selected application protocol.

   2) Compatible. Application level protocols used by the IIoT entities are similar by their functionality and/or specification but only a constrained set of the functions provided by these protocols is available for all these entities, even if the protocol converter or gateway is used.

   3) Partially compatible. Applications do not make use of the selected application protocol to implement part of their functionality, but provide converting mechanisms for conversion of the selected protocol to some other protocol or data format.

   4) Incompatible. Applications neither make use of the selected application protocol to implement part of their functionality, nor provide any special mechanisms for its conversion due to the dramatic differences in their functional purpose or specification.

b) Compatibility of an application protocol with network suite. To implement data conversion from an application protocol format into data transmission format it is required to ensure compatibility of the application protocol with network services (network suite). Compatibility levels:

   1) Fully compatible. Such an application protocol is fully compatible with network services of lower OSI layers.

   2) Compatible. Level requirements not specified.

   3) Partially compatible. A given protocol is not compatible with network services of lower OSI layers, but possesses special mechanisms for conversion of such a protocol into another application protocol which is compatible with the network suite.

   4) Incompatible. The given protocol has no compatibility with network services of lower OSI layers.

c) Application protocol compatibility. To achieve correct data exchanges between applications running by interoperating IIoT entities, it is required to ensure application protocol compatibility between such protocols. Compatibility levels:

   1) Fully compatible. Application protocols used for the IIoT entities' interaction are completely identical and support the comprehensive joint work of the applications run by these IIoT entities.

2) Compatible. Application protocols between IIoT entities are not identical, but have in place special mutual conversion mechanisms for interpretation of messages received from each other and support the comprehensive joint work of the applications run by the IIoT entities.

3) Partially compatible. Application protocols between IIoT entities are not identical, but the applications run by the IIoT entities are capable of performing some joint work but not comprehensive.

4) Incompatible. Applications run by the IIoT entities can't work jointly because of the drastic differences of the supported protocols.

5.1.9 Compatibility requirements for measuring and automation aspect

To ensure IIoT entities' compatibility with regard to measuring and the proper and coherent support of automation, the following requirements apply.

a) Compatibility of interoperation protocol with measuring devices. For correct interaction with sensors/actuators, it is required to match the compatibility requirements of physical interfaces of the controlling device (CD) with those supported by measuring devices (MD). Compatibility levels:

1) Fully compatible. A controlling device has a physical interface compatible with measuring devices and supports a protocol of interoperation with MDs.

2) Compatible. Level requirements not specified.

3) Partially compatible. A controlling device either has no physical interface required for interoperation with an MD, or does not support an interoperation protocol with such a device. In this case operation with such an MD is possible using special converting units to be connected to the CD.

4) Incompatible. A controlling device has no physical interface for operation, either with the MD or with a special converting unit.

5.1.10 Compatibility requirements for semantic aspect

To ensure IIoT entities' semantic compatibility, the following requirements apply.

a) Session understanding and scope compatibility. To ensure correct semantic interaction of the IIoT entities it is required to ensure that their approach to the identification and understanding of the session scope is the same or similar. Compatibility levels:

1) Fully compatible. IIoT entities define the session notion in a completely identical way, including session parameters and their interpretation.

2) Compatible. IIoT entities define the session notion in a slightly varying way, but the general approach to description of what the session is and the general approach to which session parameters should be supported generally coincide.

3) Incompatible. IIoT entities define the session in a completely different way so aligning session notions for these entities is not possible even if some of the parameters are the same.

b) Compatibility of message format interpretation approach. For correct interpretation of data between devices, users, systems and services it is required to ensure mutual interpretation of message formats from given IIoT entities. Compatibility levels:

1) Fully compatible. Formats of messages for the data exchange between interoperating IIoT entities and the approach to the interpretation of these messages and their parameters are completely identical.

2) Compatible. Formats of messages for the data exchange between interoperating IIoT entities and the approach to the interpretation of these messages and their parameters are similar and may be mutually supported, probably by the use of converting mechanisms, without losing any parameters.

3) Partially compatible. Formats of messages for the data exchange between interoperating IIoT entities and the approach to the interpretation of these messages and their parameters may be mutually supported, probably by the use of converting mechanisms, with loss of support of some optional parameters.

4) Formats of messages and the approach to the interpretation of these messages and their parameters supported by the IIoT entities are not capable of being converted to each other.

c) Compatibility of the approach to data interpretation. For correct perception and presentation of information received from measuring devices, it is required to ensure correct interpretation of such information by entities of the existing IIoT system. Compatibility levels:

1) Fully compatible. The way in which the data is perceived, interpreted and presented by different IIoT entities is the same.

2) Compatible. The way in which the data is perceived and interpreted by different IIoT entities is the same, or the data may be easily converted to get the required interpretation. The presentation of this information may vary.

3) Incompatible. The ways in which the data is perceived and interpreted by different IIoT entities differ drastically. These kinds of interpretation cannot be converted to each other.

5.2 Connectivity non-functional compatibility requirements

5.2.1 Compatibility requirements for version compatibility

To ensure IIoT entities' compatibility at the level of solution versions' compatibility, the following recommendations apply.

a) Backward compatibility. A new version of a solution should have features to ensure correct interoperation with an earlier version of the same solution. Compatibility levels:

1) Fully compatible. A given solution has some or other methods to ensure compatibility with an earlier version of the solution.

2) Incompatible. A given solution has no features to ensure compatibility with an earlier version of the solution.

b) Forward compatibility. An earlier version of the solution should have features ensuring correct interoperation with a later version of the same solution. Compatibility levels:

1) Fully compatible. A given solution has some or other methods to ensure forward compatibility with a later version of the solution.

2) Incompatible. A given solution has no methods to ensure compatibility with a later version of the solution.

5.2.2 Compatibility requirements for QoS management

To ensure IIoT entities' compatibility for the quality of service (QoS) aspect, the following conditions should be met.

a) Compatibility of QoS management methods. Compatibility levels:

1) Fully compatible. The QoS management methods are the same for the IIoT entities.

2) Compatible. The QoS management methods are similar and may be slightly changed for their joint use, without losing any of the parameters that comprise the subject of management.

3) Partially compatible. The QoS management methods are similar and may be slightly changed for their joint use, with the loss of some of the parameters that comprise the subject of management.

4) Incompatible. The selected application protocol is not compatible with the QoS management methods operating in the solution and has no QoS management system of its own.

5.2.3 Compatibility requirements for security and privacy aspects

As the IIoT entities may vary in their purpose and security objectives, the following main goals will be considered for compatibility requirements for security and privacy.

a) Compatibility on security policy is the capability to support in two IIoT entities the security rules and constraints which would be combined or integrated in a consistent way and do not interfere with the functional purpose, privacy policy, safety and other trustworthiness aspects and non-functional requirements for both systems.

b) Compatibility on privacy policy is the capability to support in two IIoT entities the rules and constraints on storing and handling personal data which would be combined or integrated in a consistent way and do not interfere with the functional purpose, security policy, safety and other trustworthiness aspects and non-functional requirements for both systems.

The compatibility of the level of security policy and privacy constraints is provided at the level of functional specification.

While the level of security policy and privacy are logically separated and may even pursue opposing goals, the methods of their implementation are often similar. These methods and technical capabilities, supporting security and privacy, are connected to some extent with IIoT entities' architectural design and communication protocols. If security policy and privacy policy are aligned, technically they are implemented by the same or similar means.

Because of this, further compatibility on the security level and compatibility on privacy level are considered as a whole (referring to it as compatibility at the security level).

To ensure IIoT entities' compatibility on the security level, the following conditions should be met.

a) Compatibility of security policy. Compatibility levels:

   1) Fully compatible. Security mechanisms of the same type enforce the consistent security policies which constrain neither each other nor the functions of IIoT entities to which these policies apply.

   2) Compatible. The IIoT entities are compatible in regard to implementation of security policies. Security mechanisms enforcing security policies may be configured in such a way that they constrain neither each other nor the functions of IIoT entities to which these policies apply.

   3) Partially compatible. The IIoT entities set up the consistent security policies. Security mechanisms of IIoT entities may either constrain each other or not be allowed to be used together due to functional, environmental or other limitations. At the same time, security policies allow for their joint enforcement by newly introduced controls for these solutions.

   4) Incompatible due to security policies.

The following are general considerations in regard to compatibility of security policy.

Consistency and compatibility of security policies. In case two IIoT entities support different security policies, their consistent (and, thus, compatible) security policy shall represent the intersection of the rules and constraints comprising these policies. If the compatible set of rules allows nothing, the initial security policies are incompatible. If the compatible security policy is inconsistent with other functional or non-functional requirements of one of the IIoT entities, the IIoT entities are incompatible due to their security policies.

Compatibility of IIoT entities implementation on security policy. Implementation and configuration of the IIoT system should be consistent with its security policy. If the implementation and configuration of at least one of two IIoT entities are inconsistent with their compatible security policy, the IIoT entities are incompatible due to their security policies.

Negotiation on compatible security policy. Checking for compatibility of security policies and negotiation of the compatible security policy may be conducted by one of the following approaches.

1) The first, decentralized approach requires exchanging the parameters among IIoT entities using the specific protocol for negotiation of security regime.
2) The second, centralized approach is based on using the central device or gateway receiving the parameters from other solutions and setting the security regime according to the option that fits all contexts.

Enforcement of compatible security policy. The enforcement of compatible security policy over the whole functionality of the IIoT entities requiring compatibility usually is not effective. The reasonable approach is identifying and applying the complementary constraints to the control and informational flows that come to one IIoT system from another.

For the decentralized approach, every IIoT system is responsible for the enforcement of the compatible security policy while exchanging the information and/or participating in control relationships with other solutions. This approach is capable of enforcing the compatible security policy only at the receiver of the communication; thus, it potentially gives fewer guarantees for security.

For the centralized approach, the central device or gateway is responsible for the separation of informational and control flows and enforcement of compatible security policy on these flows. This approach is capable of enforcing the compatible security policy transparently and independently of any side of communication; thus, it potentially gives more strict guarantees for security.

The gateway enforcing the compatible security policy should implement the following basic functions.

a) Separate the communication environment of IIoT entities into domains (or segments) according to the security policies valid in these domains.
    1) Verify the consistency and compatibility of security policies.
    2) Verify the compatibility of implementations on security policy.
    3) Negotiate on compatible security policy.
    4) Validate the control and informational flows between these domains according to the compatible security policy for the IIoT entities in these domains.
    5) Verify the compatible security policy completion for the messages or other communication units.
b) Compatibility of communications and connectivity security capabilities refers to the features supporting secure and trustworthy information exchange that fits the consolidated security objectives for the compatible IIoT entities. Compatibility levels:
    1) Fully compatible. Security mechanisms implementing protection capabilities for the communications may negotiate on the parameters of the information exchange that they would consider as secure and trustworthy.
    2) Compatible. Consistent (and compatible) in regard to security policies. IIoT entities have the same security concerns and objectives in regard to communications and connectivity. Support of secure and trustworthy information exchange according to these objectives and concerns requires newly implemented security mechanisms at least for one of the communicating parties.
    3) Incompatible. IIoT entities have security concerns and objectives in regard to information exchange that, being satisfied would constrain either each other or the main functions of at least one of the solutions.

c) Compatibility of service specific security capabilities refers to the features facilitating application-level security and trustworthiness for the services provided by IIoT entities and consumed by other compatible IIoT entities. Compatibility levels:

   1) Fully compatible. Security mechanisms implementing service-specific security capabilities may be combined into a security solution that acts as a whole enforcing the security policy that fits the needs of all IIoT services.

   2) Compatible. Consistent (and compatible) in regard to security policies. IIoT entities have the same security concerns and objectives in regard to service provision.

   3) Incompatible. IIoT entities have the security concerns and objectives in regard to service provision that, being satisfied would constrain either each other or application-level features implemented at least by one of the services.

d) Compatibility of secure integration capabilities refers to the mitigation of the risks connected to the integration process of compatible IIoT entities. Compatibility levels:

   1) Fully compatible. Secure integration capabilities implemented to support the integration process of IIoT entities (integrity and authenticity control for software and equipment, verification of supply chain and others) are consistent for these IIoT entities and do not constrain their expected functionality and the possibility of their joint use.

   2) Incompatible. Secure integration capabilities implemented to support the integration process of one of the IIoT entities considerably constrain the possibility of the joint use of these solutions.

e) Compatibility of authentication and authorization capabilities refers to the possibility of using the same schemes, factors, protocols and technical means for the provision of authorized access to the features of compatible IIoT entities. Compatibility of authentication security aspect may have safety-related issues for incorrectly blocking critical access. Compatibility levels:

   1) Fully compatible. Authentication and authorization mechanisms for the IIoT entities implement the same or very similar schemes, factors, protocols and features for the provision of authorized access to the functionality of these IIoT entities.

   2) Compatible. Consistent (and compatible) in regard to authentication and authorization policies. Authorized access to the features of IIoT entities requires the implementation of schemes, factors, protocols and features for authentication that allow their joint implementation by newly introduced mechanisms for at least one of the solutions.

   3) Incompatible. Authorized access to the features of one of the IIoT entities requires the implementation of schemes, factors, protocols and features for authentication that are inappropriate at least for one of these solutions, and vice versa.

f) Compatibility of security audit capabilities, the accountability of events and parameters and the possibility of integrating the log entries according to the comprehensive structure. Compatibility levels:

   1) Fully compatible. Security audit capabilities implemented by IIoT entities provide all the data required by their compatible audit policy and allow for the joint use of the recorded security related events.

   2) Incompatible. Security audit capabilities implemented by IIoT entities either do not provide all the data required by the compatible audit policy of these solutions or do not allow for the joint use of the recorded security related events.

g) Compatibility of cryptographic means refers to the compatibility of cryptographic protocols of the various purposes (for encrypting data, verifying the source authenticity, etc.), cryptographic algorithms and their parameters. Implementation of cryptographic algorithms and protocols should provide the negotiation on parameters and their configuration that meets the local laws and export restrictions of the states and areas where compatible solutions are planned to be used. Compatibility of cryptographic security aspect may have safety-related issues for incorrectly blocking critical access, critical time delays, etc. Compatibility levels:

   1) Fully compatible. Cryptographic mechanisms enforce the consistent protection of data according to similar security objectives and using the same protocols and algorithms. These mechanisms constrain neither each other nor the functions of IIoT entities to which these policies apply. The cryptographic key management protocols and infrastructure are compatible.

   2) Compatible in regard to protocols and algorithms. Cryptographic mechanisms enforce the consistent protection of data according to similar security objectives and using the same protocols and algorithms. These mechanisms constrain neither each other nor the functions of IIoT entities to which these policies apply. The key management infrastructure needs to be implemented.

   3) Partially compatible. Consistent (and compatible) in regard to objectives of data protection. The IIoT entities set up the same or very similar requirements to the cryptographic protection of data. The same algorithms and protocols may be used, but are not all preferred by every party. Cryptographic mechanisms for at least one of these IIoT entities and key management infrastructure need to be implemented.

   4) Incompatible due to the objectives of implementing the cryptographic mechanisms.

5.2.4 Compatibility requirements for compliance

To ensure compatibility for IIoT entities with international standards, guidelines, laws and regulations required to comply with, the following requirements apply.

a) International compatibility. To ensure compatibility for IIoT entities with international standards, guidelines, laws and regulations required to comply with, the underlying technologies, equipment and software shall follow the same or similar objectives and principles of their design responding to these standards, guidelines, laws and regulations. Compatibility levels:

   1) Fully compatible. The underlying IIoT technologies, equipment and software follow the objectives and principles of their design that respond to the requirements of international standards, guidelines, laws, and regulations.

   2) Compatible. Level requirements not specified.

   3) Partially compatible. The underlying IIoT technologies, equipment and software follow the objectives and principles of their design that partially respond to the requirements of international standards, guidelines, laws and regulations.

   4) Incompatible. The underlying IIoT technologies, equipment or software do not follow the objectives and principles of their design that respond to the requirements of the international standards, guidelines, laws and regulations.

b) National compatibility. To ensure compatibility for IIoT entities with national standards, guidelines, laws and regulations required to comply with, the underlying technologies, equipment and software shall follow the same or similar objectives and principles of their design responding to these standards, guidelines, laws and regulations. Compatibility levels:

   1) Fully compatible. The underlying IIoT technologies, equipment and software follow the objectives and principles of their design that respond to the requirements of national standards, guidelines, laws and regulations.

   2) Partially compatible. The underlying IIoT technologies, equipment and software follow the objectives and principles of their design that partially respond to the requirements of national standards, guidelines, laws and regulations.

3) Incompatible. The underlying IIoT technologies, equipment or software do not follow the objectives and principles of their design that respond to the requirements of the national standards, guidelines, laws and regulations.

c) Industry compatibility. To ensure compatibility for IIoT entities with industry standards, guidelines, laws and regulations required to comply with, the underlying technologies, equipment and software shall follow the same or similar objectives and principles of their design responding to these standards, guidelines, laws and regulations. Compatibility levels:

1) Fully compatible. The underlying IIoT technologies, equipment and software follow the objectives and principles of their design that respond to the requirements of industry standards, guidelines, laws and regulations.

2) Partially compatible. The underlying IIoT technologies, equipment and software follow the objectives and principles of their design that partially respond to the requirements of industry standards, guidelines, laws and regulations.

3) Incompatible. The underlying IIoT technologies, equipment or software do not follow the objectives and principles of their design that respond to the requirements of the industry standards, guidelines, laws and regulations.

5.2.5 Compatibility requirements for safety

To ensure IIoT entities' compatibility for the safety aspect, the following recommendations apply.

a) Industrial system safety measures. Implemented IIoT systems should not interfere with the operation of enterprise safety related systems. Compatibility levels:

1) Fully compatible. The solution has no problems with ensuring the safety of the industrial system.

2) Partially compatible. The solution can be implemented in the industrial system if certain safety conditions are met.

3) Incompatible. The solution cannot be implemented in the enterprise.

6 Devices and data format compatibility requirements for IIoT connectivity

Clause 6 describes the procedure of data collection and data conversion for various IIoT protocols and other probable methods to provide connectivity between two or more IIoT systems.

For the purpose of compatibility, the algorithms embedded in IIoT devices format and generate transmission messages. These message formats are determined during a system development stage. The transmission message formats should be based on standardized protocols and technologies. When the system having the IIoT devices is placed in operations, the messages generated from the system shall include, but not be limited to, the following:

a) types of protocol used for transmitting the service information between the IIoT devices;

b) types of service command and service message format used;

c) data collection algorithm;

d) data storage regulations;

e) data access regulations;

f) policy of data protection; and

g) policy of quality of service (QoS).

Semantic Industrial Internet of Things gateway (SIIG) should be used for an applied solution for industrial Internet connectivity framework (IICF) SW (software) implementation. This gateway should be installed within the framework of a single IoT solution and perform conversion between IIoT protocols.

A sample implementation of a hardware and software set which connects, using an SIIG, various sub-networks functioning on the basis of different IIoT protocols is shown in Figure 1.

A general SIIG architecture is presented in Figure 2. The SIIG is a set of software and hardware modules with two or more industrial network interfaces (i.e. network interfaces), functioning on the basis of an operating system (OS). The SIIG supports both networking functions for each of the network interfaces (i.e. middleware) and production environment virtualization (i.e. virtualization). Various applications and services can be provided on the basis of a virtualized production environment, including IICF SW.

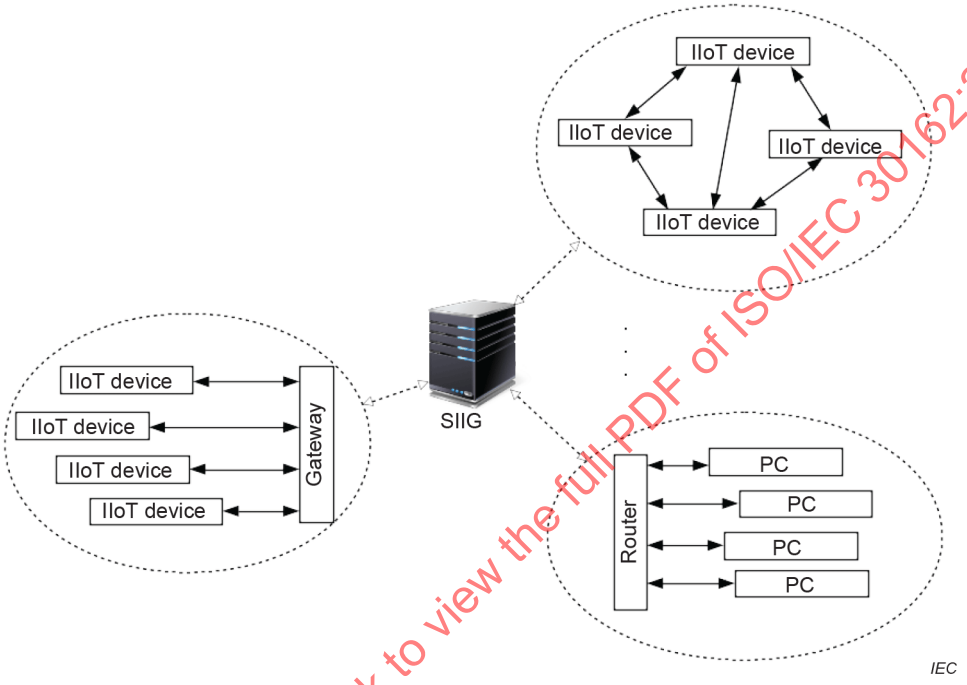


Figure 1 – A sample software/hardware set performing conversion between IIoT protocols using semantic Industrial Internet of Things gateway (SIIG)

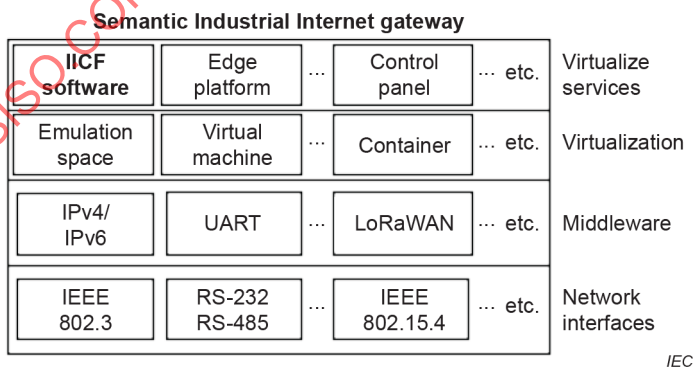


Figure 2 – SIIG architecture example

7 IIoT system models with IIoT gateways

Common model of the Industrial IoT system with compatibility ensuring functions by special IIoT gateways to process heterogeneous data to a common data format to support the IIoT platform is shown in Figure 3. Such a special IIoT gateway is called "heterogeneous gateway".

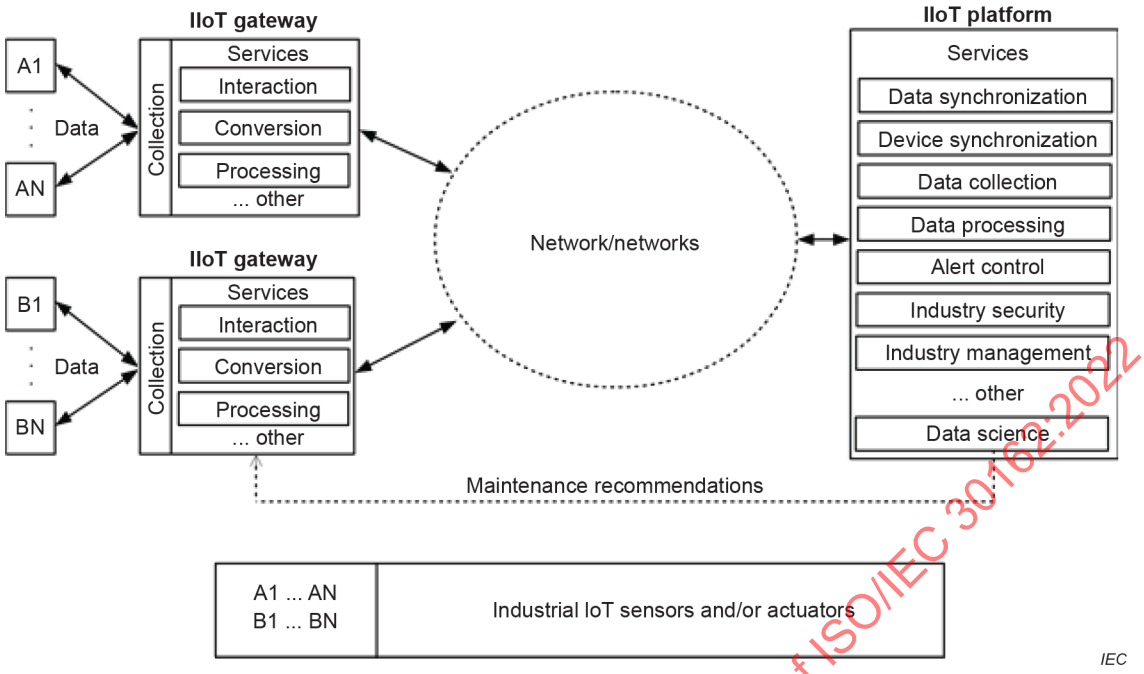


Figure 3 – IIoT system model with heterogeneous gateways

As defined in Rec. ITU-T Y.4101/Y.2067, an IoT gateway is a unit in the Internet of Things which interconnects the devices with the communication networks. It performs the necessary translation between the protocols used in the communication networks and those used by devices.

An IIoT gateway, also known as a heterogeneous IoT gateway, is an entity in the Internet of Things which interconnects the devices that use different communication technologies and protocols between themselves, the Internet and other communication networks.

As specified in ETSI GS MEC 001:

a) mobile edge platform is the collection of functionalities that is required to run mobile edge applications on a specific mobile edge host virtualization infrastructure and to enable them to provide and consume mobile edge services, and that can provide itself a number of mobile edge services;

b) mobile edge application is the application that can be instantiated on a mobile edge host within the mobile edge system and can potentially provide or consume mobile edge services; and

c) mobile edge host is the entity that contains a mobile edge platform and a virtualization infrastructure which provides compute, storage and network resources to mobile edge applications.

As defined in 3.3, an edge gateway is the heterogeneous IoT gateway that takes part in functionality of mobile edge host, especially its data processing functions.

As specified in Rec. ITU-T Y.4113, IoT platform is a technical infrastructure that provides integration of generic and specific capabilities [Rec. ITU-T Y.4000]. These capabilities, in conjunction with capabilities of the core network, may be exposed to one or more IoT application servers. The core network provides communication functionalities to support the data transfer to devices and gateways via access network. Some of those functionalities can be used by service providers.

An IIoT platform is the IoT platform that is used for industrial purposes and consists of various services, including data collection, storing and processing functions. An example of the performance testing scenarios and test sheets of the IIoT gateways and servers can be found in Annex B.

8 Network model for IIoT compatibility testing

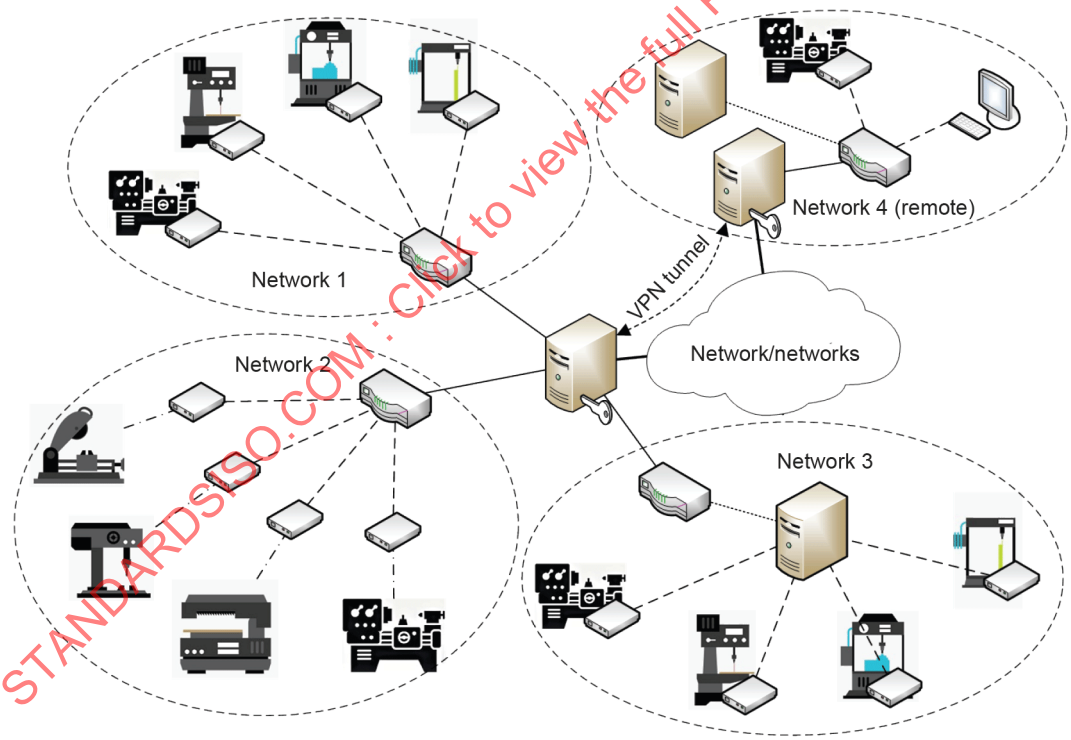
The network model shown in Figure 4 includes four sub-network types.

a) Network 1 – This network consists of industrial equipment that includes computer appliances for its management. These computer appliance devices cannot communicate with special industrial management systems.

b) Network 2 – This network consists of industrial equipment that has no digital devices to control it through the networks. This equipment is controlled by the special computer appliance having sensors and actuators.

c) Network 3 – This network consists of industrial equipment that includes computer appliances for its management. These computer appliance devices communicate with special industrial management systems.

d) Network 4 – This network consists of special server computer appliance, user terminal and optionally some industrial equipment with digital computer appliance controller. This remote sub-network connects to other segments by a special computer appliance that builds a virtual private network tunnel.



	Industrial equipment		Computer appliance		Computer appliance for VPN tunneling
etc.	Industrial equipment with computer appliance		Switch/router/edge gateway		Server computer appliance to control industrial systems

IEC

Figure 4 – Network model for IIoT compatibility testing

More specific vendor and technology information about connectivity protocols can be found in Annex C.

9 IIoT device connectivity models

9.1 Direct connectivity

The model shown in Figure 5 describes a way to connect non-digital industrial equipment (NDIE) with an IIoT service platform. This NDIE is connected to a digital controller (PC, microcontroller, microcomputer, etc.) through a sensor(s) installed on the NDIE. The digital controller directly connects to an IIoT service platform with an IP-compatible network interface without special gateways.

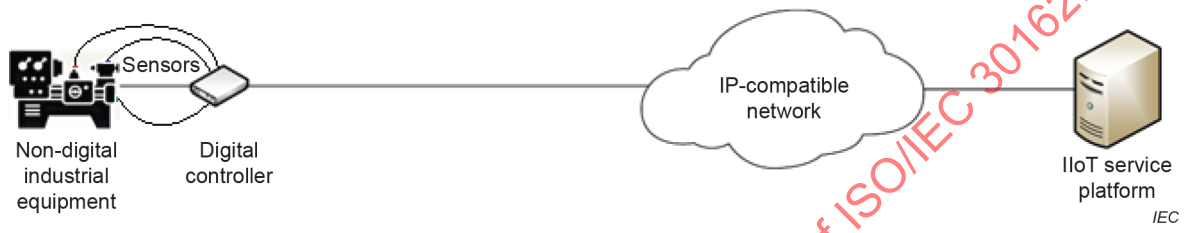


Figure 5 – Direct connectivity

NDIE is connected to an IIoT service platform after completing the following steps.

1) It is necessary to choose and install required sensors on the NDIE.
2) These sensors should be connected to a digital controller.
3) It is necessary to upload software to digital controller where the software is responsible for data collection, conversion and transmission of sensor data to the IIoT service platform.
4) This digital controller should be registered (with a unique identifier) on IIoT services provided by the IIoT service platform. The service responds to the data collected from the sensors on the NDIE.
5) An operator should run a test procedure to check the connection and to measure the connection parameters.
6) If the test procedure fails, the operator should reconfigure the system connectivity and repeat Steps 1 to 5.
7) If the test procedure is successful, the operator may start a regular IIoT system work procedure.

9.2 Connectivity through IIoT gateway

The model shown in Figure 6 describes the ways to connect digital industrial equipment (DIE) with an IIoT service platform. The DIE is controlled by applications on the user control system (personal computer, microcontroller, microcomputer, etc.). The user control system (UCS) is connected to an IIoT service platform by an IIoT gateway. The IIoT gateway accumulates the packets from the applications, and it responds by creating control messages and converts them to an IP packet format.

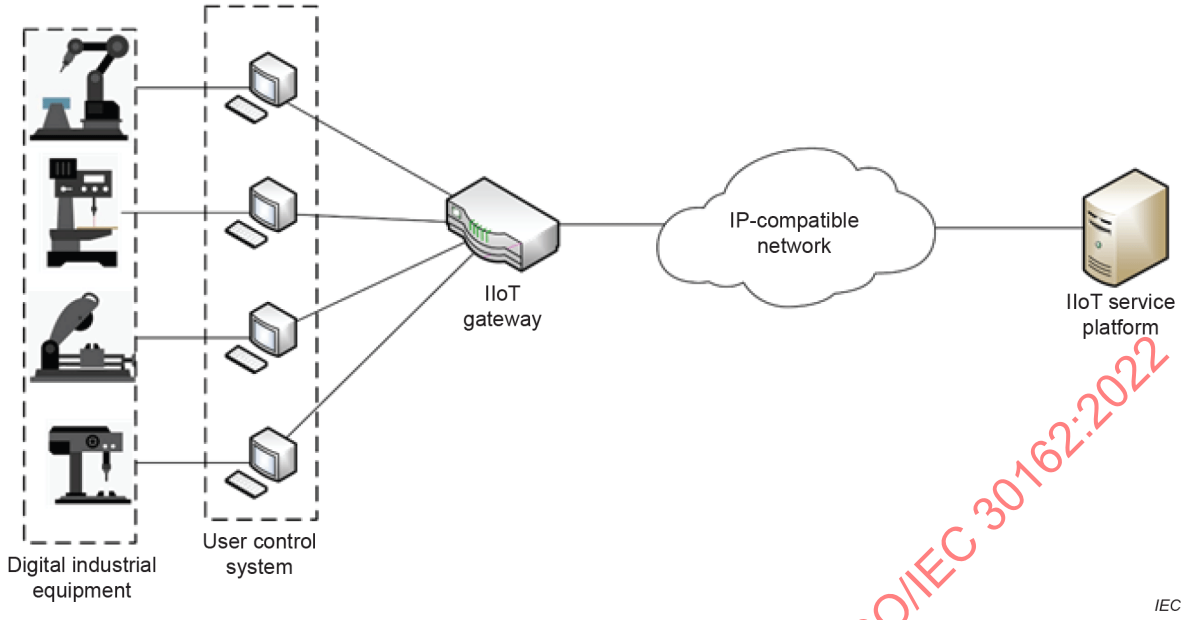


Figure 6 – Connectivity with IIoT gateway.

Digital industrial equipment is connected to an IIoT service platform after completing the following steps.

1) It is necessary to connect the DIE to the UCS.
2) The operator should check the DIE sensors data collection function system (from DIT sensors) on every UCS connected to the DIE.
3) After the data collection function is checked out, the UCS's should be connected to an IIoT gateway.
4) The operator should run a registration and connection test procedure.
5) If the test procedure fails, the operator should reconfigure the system connectivity and repeat Steps 1 to 4.
6) If the test procedure successfully completed, the operator should register the IIoT gateway with the IIoT services on the IIoT service platform. Every DIE (or DIE's sensors) should also be registered with the IIoT services.
7) After the registration and connection test procedure, the operator should run a test procedure to check connections, to measure connection parameters and to confirm the IIoT protocols conversion at the IIoT gateway.
8) If the test procedure fails, the operator should reconfigure the system as described in Steps 6 and 7.
9) If the test procedure successfully completes, the operator may start a regular IIoT system work procedure.

9.3 Connectivity through industrial control systems

This model, shown in Figure 7, describes the ways to connect collection and management industrial systems (C&M IS), which are responsible for managing a group of different industrial equipment to an IIoT service platform. In this case DIE is connected by a special C&M IS. This system is connected to an IIoT service platform by a special client application on C&M IS which is connected to an IIoT gateway.

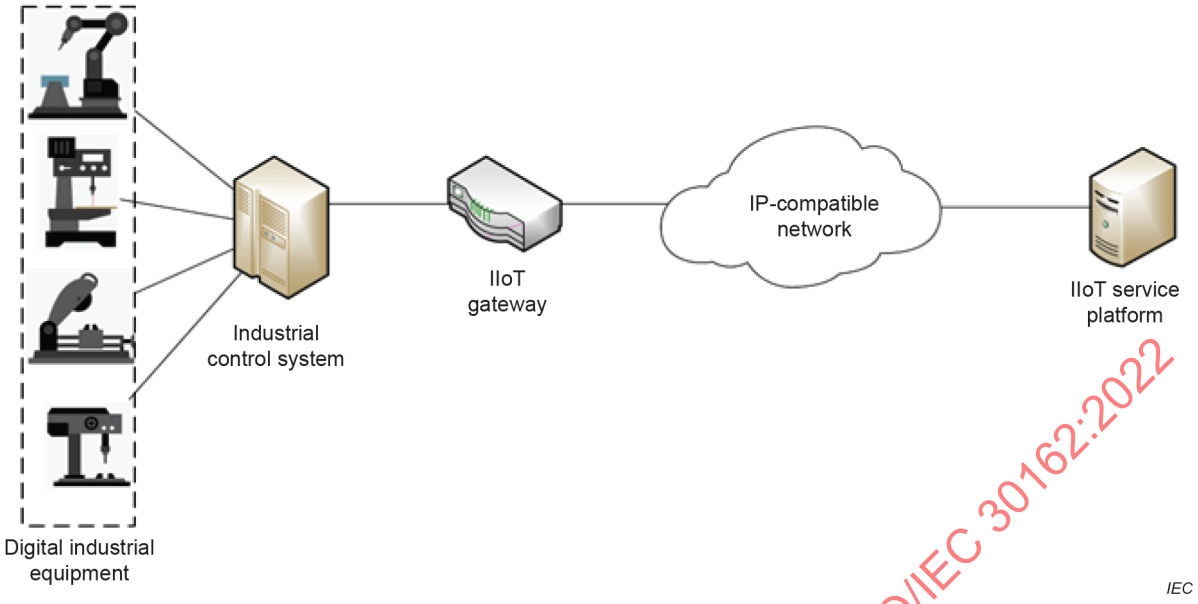


Figure 7 – Connectivity with an industrial control system

DIE can be considered as connected to an IIoT system device through a C&M IS after the following actions.

1) First of all, the operator should connect DIEs to a C&M IS and then the C&M IS should be tested on data collection and management procedures. If this test fails, the operator should reconfigure this connection.
2) Then the C&M IS should be registered and connected with an IIoT gateway. This gateway may connect one or more C&M IS to IIoT system.
3) The operator should conduct test procedure to check format conversion from different C&M IS.
4) If the test procedure fails, the operator should reconfigure the system as described in Steps 1 to 3.
5) If the test procedure successfully completes, the operator should register the IIoT gateway at the IIoT service platform and every DIE (or DIE's sensors) should be registered on the IIoT service platforms with it.
6) After this, the operator should run a test procedure to check connection, measure connection parameters and IIoT protocols conversion on the IIoT gateway.
7) If the test procedure fails, the operator should reconfigure the system as described in Steps 5 and 6.
8) If the test procedure successfully completes, the operator should start a regular IIoT system work scenario.

Annex A
(informative)

Compatibility checklist for devices and services IIoT systems

The checklist shown in Table A.1 lists the basic compatibility parameters of the Industrial Internet of Things (IIoT) systems. On the basis of this checklist, verification can be performed both in a manual and an automated mode by running the appropriate tests. The test results will indicate whether or not the IIoT devices will correctly interact with the corresponding systems: cloud services, predictive analytics, etc.

Table A.1 – Compatibility checklist for devices and services IIoT systems

Compatibility aspects			Fully compatible	Compatible	Partially compatible	Incompatible
Functional compatibility requirements	Physical aspect	Data transmission media compatibility				
		Data transmit/receive system compatibility				
		Electromagnetic compatibility				
	MAC aspect	Media access compatibility				
		Addressing framework compatibility				
		Compatibility of procedures to detect and mediate data transmission collisions				
	LLC aspect	Compatibility of the network topologies, including switching procedures				
		Compatibility of network frame generation and interpretation				
		Compatibility of the data transmission control procedure over the established communications channel				
	Network aspect	Routing compatibility				
		Network protocol compatibility				
		Identifier compatibility				
	Transport aspect	Multiplexing/demultiplexing compatibility				
		Transport options compatibility				
	Session aspect	Session delivery and support compatibility				
		Session control protocol compatibility				

Compatibility aspects			Fully compatible	Compatible	Partially compatible	Incompatible
	Data presentation aspect	Compatibility of data encoding/decoding and compression protocols				
		Encryption/decryption protocols compatibility				
	Application aspect	Application layer protocols' and applications' compatibility				
		Compatibility of an application protocol with network suite				
		Application protocol compatibility				
	Measuring and automation aspect	Compatibility of interoperation protocol with measuring devices				
	Semantic aspect	Session understanding and scope compatibility				
		Compatibility of message format interpretation approach				
		Compatibility of the approach to data interpretation				

Compatibility aspects			Fully compatible	Compatible	Partially compatible	Incompatible
Non-functional compatibility requirements	Version compatibility definition	Backward compatibility				
		Forward compatibility				
	QoS management aspect	Compatibility of QoS management methods				
	Security and privacy aspect	Compatibility of security policy				
		Compatibility of communications and connectivity security capabilities				
		Compatibility of service specific security capabilities				
		Compatibility of secure integration capabilities				
		Compatibility of authentication and authorization capabilities				
		Compatibility of security audit capabilities				
		Compatibility of cryptographic means				
	Compliance aspect	International compatibility				
		National compatibility				
		Industry compatibility				
	Safety aspect	Industry safety measures				

Annex B
(informative)

Load testing scenario for different IIoT devices

Table B.1, Table B.2 and Table B.3 show the load testing scenarios for the heterogeneous IIoT gateway, edge server, and cloud server.

Table B.1 – The Industrial Internet of Things edge server operation testing based on existing network

#	Action	Description	Result
Scenario "The IIoT edge server operation testing based on existing network"			
1	Connecting and configuring the IIoT edge server (ES)	a) The ES is connected to the network under test via a network interface.	The ES is ready for testing.
		b) The ES is configured accordingly for the link layer and network layer protocols.	
		c) Checking the ES accessibility for network devices.	
		d) All supported query processing functions are validated.	
		e) The application for testing the CPU load, the amount of RAM used, and the processing time is executed in the background through the ES local network interface. This test is performed without the incoming requests.	
2	Connecting and configuring the IIoT traffic generator (TG)	a) The TG is connected to the network under test via a network interface.	The TG is ready for testing.
		b) The TG is configured accordingly for the link layer and network layer protocols.	
		c) Checking the ES accessibility for network devices.	
		d) The TG is configured.	
		e) Testing of the IIoT TG is performed. A local network packet analyser is used to confirm the operation of the TG.	
3	Testing the edge server (ES) operation	a) The comparison of the metadata format generated by the TG and that of the ES is carried out. If the result of the comparison is not acceptable, the format of the generator metadata is changed to the format accepted by the server.	The ES is ready to work in the tested network.
		b) A series of measurements of processing time, CPU load, and RAM load of the ES is performed for all tested functions during load testing by an increasing number of virtual devices from the TG, e.g. 1, 5, 10, 50, 250, …, N devices.	
		c) The results of the tests are used to develop recommendations for the operation of the ES in the tested network.	

An edge server (ES) is a device that performs the mobile edge platform functions described by ETSI GS MEC 001.

A cloud server (CS) is a device that performs the IIoT platform functions described in Clause 7.

Table B.2 – Testing of interaction between edge and cloud Industrial Internet of Things servers, based on the existing network

#	Action	Description	Result
Scenario "Testing of interaction between edge and cloud IIoT servers, based on the existing network"			
1	IIoT edge server (ES) connection and configuration	a) ES connects to the Internet.	The ES is ready for testing.
		b) All supported query processing functions are validated.	
		c) The background application runs to test the CPU load, the amount of RAM used, and the request processing time on the local network interface of the ES. Testing of the ES is performed without any incoming requests.	
2	IIoT cloud server (CS) configuration	a) Configuration of the CS is carried out to ensure interaction with the ES by the special CS interaction tools.	The CS is ready for testing.
		b) All supported query processing functions are validated.	
3	ES and CS connection configuration	a) The comparison of the format of metadata generated by the ES and the CS is performed. The ES metadata format is changed to the CS format in a case when the result of the comparison was not acceptable.	The ES and CS are ready to send and receive requests.
		b) The ES establishes the connection according to the rules set by the CS.	
4	ES and CS interaction testing	a) Alternately, several measurements of the processing time, the CPU load, and the RAM load used are performed for all tested functions during load testing by an increasing number of virtual devices that were created by the special benchmark tool on the ES, e.g. 1, 5, 10, 50, 250, …, N devices.	The ES and CS are ready to interact.
		b) The results of the tests are used to develop recommendations for the interactions of the ES and the CS.	

Table B.3 – The Industrial Internet of Things application protocols conversion testing for the heterogeneous IIoT gateways and based on the existing network

#	Action	Description	Result
Scenario "The IIoT application protocols conversion testing for the heterogeneous IIoT gateways (HG) and based on the existing network"			
1	Connecting and configuring the heterogeneous IIoT gateway (HG)	a) The HG connects to the network under test via the network interface.	The HG is ready for test.
		b) The HG is configured accordingly for the link layer and network layer protocols.	
		c) Check the HG accessibility for network devices.	
		d) Check the protocol conversion using the server and client applications running on the local network interface of the HG. During the check, the conversion time is measured.	
		e) The application for testing the CPU load and the amount of RAM used is executed in the background through the HG local network interface. The test is performed without any load.	

#	Action	Description	Result
2	Configuring the IIoT ES on the HG	a) The test application of the ES is configured.	The ES is ready for receiving network packets.
		b) The ES is started on the local network interface.	
		c) Check the following base functions: IIoT device registration, data receiving and saving, and data reading.	
		d) The test of the HG with the running applications of the ES is performed by using the application for the CPU and RAM load measurements.	
3	Connecting and configuring the IIoT TG	a) The TG connects with the test network via the network interface.	The TG is ready for use.
		b) The TG is configured accordingly for the link layer and network layer protocols.	
		c) Check the access of the TG for network devices.	
		d) Testing of the IIoT TG is performed. A local network packet analyser is used to confirm the operation of the TG.	
4	Testing data transmission and reception between the TG and the ES	Network packet reception and transmission is tested for a system consisting of the TG and the ES (using ES-supported application protocols). The flow of network packets is generated by one virtual device for each of the types of traffic supported by the TG.	A system consisting of an HG and an EG is ready to receive and transmit data.
5	Testing protocol conversion on the HG	a) Alternately, a number of measurements are taken of the processing time and the CPU and RAM loads of each HG supported by the traffic generator application protocols with an increasing number of virtual devices on the TG, e.g. 1, 5, 10, 50, 250, …, N devices.	HG is ready for the conversion of the IIoT application protocols.
		b) A series of measurements described in 5 a) is carried out with the generation of multiple network packets for several application protocols by one virtual TG device.	
6	Testing the HG together with the server functioning in the tested network	a) The comparison of the format of metadata generated by the HG and that of the ES and/or the CS in the existing network is performed. If the result of the comparison is not acceptable, the format of the HG metadata is changed to the format accepted by the server.	HG is ready to work in the tested network.
		b) The conversion of application protocols for the HG is being tested, as described in No. 1 in this table.	
		c) The results of the tests are used to develop recommendations for the HG operation in the tested network.	

Table B.4 shows the format of the test sheet, which can be used to measure various parameters of devices, according to the scenarios described in Table B.1, Table B.2 and Table B.3. An example of filling in this table is given in Table B.5.

Table B.4 – Format of the test sheet for load testing scenarios

Testing scenario: _____									
Device/devices under test: _____ _____									
Using devices: _____ _____									
DUT parameters: _____ _____									
Confidence probability: _____ %									
Test time: _____									
#	Test case	Number of virtual testing devices	Mean packets arrival rate (s)	Arrival packets jitter (s)	DUT	CPU load (%)	RAM load (%)	Mean processing time (s)	Packet loss (%)
1	_____	_____	___ ± ___	_____	_____	_____	_____	___ ± ___	_____
	. . .								
	. . .								
	. . .								
	. . .								
	. . .								
n	_____	_____	___ ± ___	_____	_____	_____	_____	___ ± ___	_____

Table B.5 – Example of filling the test sheet defined in Table B.4

Testing scenario: Edge and cloud server load testing for existing network									
Device/devices under test: edge server, cloud server									
Using devices: traffic (query) generator, Ethernet switch, Ethernet router									
DUT parameters: edge server – dual 2,0 GHz ARM core, 4 Gb RAM; cloud server – quad 3,2 GHz x86_64 core, 16 Gb RAM									
Confidence probability: 95 %									
Test time: 30 seconds									
#	Test case	Number of virtual testing devices	Mean packets arrival rate (s)	Arrival packets jitter (s)	DUT	CPU load (%)	RAM load (%)	Mean processing time (s)	Packet loss (%)
1	–	0	–	–	Edge server	12	11	–	–
					Cloud server	25	30	–	–
2	Send data query	1	0,177 ± 0,032	0,144	Edge server	12	11	0,002 3 ± 0,000 4	0
					Cloud server	25	31	0,001 0 ± 0,000 1	0
3		10	0,017 ± 0,001	0,004	Edge server	13	15	0,002 6 ± 0,000 5	0
					Cloud server	25	31	0,001 1 ± 0,000 1	0
. . .									
n	Request data query	1	0,133 ± 0,004	0,029	Edge server	11	11	0,002 4 ± 0,000 3	0
					Cloud server	24	30	0,001 2 ± 0,000 1	0
. . .									
n+*m*	Send statistic query	500	0,003 7 ± 0,000 4	0,001	Cloud server	35	57	0,002 9 ± 0,000 4	0
. . .									