



中华人民共和国国家标准

GB/T 44809—2024/ISO/IEC 30162:2022

物联网 工业物联网系统设备兼容性 要求和模型

Internet of things (IoT)—Compatibility requirements and model for devices
within industrial IoT systems

(ISO/IEC 30162:2022, IDT)

2024-10-26 发布

2025-05-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 工业物联网兼容性层面和级别的描述	2
4.1 工业物联网兼容性层面	2
4.2 工业物联网兼容性级别	4
5 兼容性要求	5
5.1 连接功能兼容性层面	5
5.2 非连接功能兼容性要求	10
6 工业物联网连通性设备和数据格式兼容性要求	14
7 配备工业物联网网关的工业物联网系统模型	15
8 工业物联网兼容性测试的网络模型	16
9 工业物联网设备连接模型	17
9.1 直接连接	17
9.2 通过工业物联网网关的连接	18
9.3 通过工业控制系统的连接	19
附录 A(资料性) 工业物联网设备和服务兼容性核查表	21
附录 B(资料性) 不同工业物联网设备的负载测试场景	23
附录 C(资料性) 通信网络中工业物联网基础网络设施连接架构	28
C.1 概述	28
C.2 连接等级 1	30
C.3 连接等级 2	31
C.4 连接等级 3	31
C.5 连接等级 4	32
附录 NA(资料性) 本文件的相关缩略语	34
参考文献	36

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件等同采用 ISO/IEC 30162:2022《物联网 工业物联网系统设备兼容性要求和模型》。

本文件做了下列最小限度的编辑性改动：

——附录 C 中 C.2、C.3 和 C.5 分别增加了说明性注；C.5 中按照标准中的工业物联网系统设备兼容性模型，增加了各节点间连接技术与我国工业物联网设备兼容应用的示例；

——增加了资料性附录 NA，列出了本文件中使用的缩略语，便于使用。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息技术标准化技术委员会(SAC/TC 28)提出并归口。

本文件起草单位：中国电子技术标准化研究院、北京大学、深圳赛西信息技术有限公司、江苏赛西科技发展有限公司、北京大数据研究院、北京科技大学、中兴通讯股份有限公司、中国电力科学研究院有限公司、北京英智数联科技有限公司、北数智联(重庆)科技有限公司、重庆市质量和标准化研究院、浙江浙能能源服务有限公司、江苏中天科技股份有限公司、常州宝捷冲片有限公司。

本文件主要起草人：韩世豪、杨宏、苏静茹、郭雄、张学骞、卓兰、秦潮、张弛、刘云淮、苏玥琦、程超、霍佳皓、于金辉、高凯强、刘云浩、苗欣、黄永贵、张程、孙凡力、张承宇、杨桦、冯祥祥、秦俊琦、皇甫伟、黄新刚、关璐瑶、郑斌、孙成富。

物联网 工业物联网系统设备兼容性 要求和模型

1 范围

本文件从以下方面规定了工业物联网连通性网络模型以及工业物联网系统内的设备和网络的一般兼容性要求：

- 数据传输协议交互；
- 分布式数据互操作性和管理；
- 连通性框架；
- 连通性传输；
- 连通性网络；
- 用于工业物联网领域的最佳实践和指导。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

ISO 和 IEC 维护的用于标准化的术语数据库网址如下：

- ISO 在线浏览平台：<https://www.iso.org/obp>
- IEC 电工百科：<https://www.electropedia.org/>

3.1

共存性 co-existence

在与其他产品共享通用的环境和资源的条件下，产品能有效执行其所需的功能并且不会对其他产品造成负面影响的程度。

[来源：ISO/IEC 25010:2023, 4.2.3.1]

3.2

兼容性 compatibility

在共享相同的硬件或软件环境的条件下，产品、系统或组件能与其他产品、系统或组件交换信息，和/或执行其所需的功能的程度。

[来源：ISO/IEC 25010:2023, 4.2.3]

3.3

边缘网关 edge gateway

用于参与移动边缘主机数据处理等功能实现的异构物联网网关。

3.4

工业物联网兼容性 industrial internet of things compatibility

工业系统、信息资源或其他工业物联网实体在共享同一硬件、软件环境和网络的同时，能与其他

工业互联网实体交换信息,和/或执行其需求功能的程度。

注:兼容性包括互操作性和共存性,符合 ISO/IEC 25010:2023 的附录 A。

[来源:ISO/IEC 25010:2023,4.2.3,有修改]

3.5

工业互联网服务平台 industrial internet of things service platform

工业互联网平台的一部分,负责与工业互联网终端节点的交互,并向用户提供服务。

3.6

工业互联网 industrial internet of things;IIoT

以利用现有和新兴信息和通信技术实现工业转型方法为基础的物联网。

[来源:Rec.ITU-T Y.4003]

3.7

工业互联网连通性框架 industrial internet connectivity framework

用于开发应用程序的软件开发框架,这些应用程序负责各种工业互联网应用协议的相互兼容和兼容性模型语义方面的有效负载格式。

3.8

工业互联网网关 industrial internet of things gateway;IIoT gateway

工业互联网系统的用于互操作性的实体;即使在设备之间、设备与网络之间以及网络之间不兼容或部分兼容的情况下,也能在工业互联网系统内的一个或多个设备和外部网络之间提供互连。

注1:工业互联网网关也称为HG。

注2:工业互联网网关结合边缘网关和语义工业互联网网关共同解决问题,以确保各种通信技术和设备与网络间、其他网络间协议的兼容性,从而满足工业领域的要求。

3.9

互操作性 interoperability

两个或多个系统、产品或组件之间交换信息以及使用已交换信息的程度。

[来源:ISO/IEC 25010:2023,4.2.3.2]

3.10

语义工业互联网网关 semantic industrial internet of things gateway;SIIG

使工业互联网系统在语义方面兼容的工业互联网网关。

注:语义工业互联网网关主要是确保各种应用协议和工业互联网有效负载格式相互兼容。

3.11

控制器区域网络 controller area network;CAN

用于系统内智能设备联网的高完整性总线系统。

注:通常用于车辆或医疗设备的嵌入式网络。

[来源:ISO/IEC/IEEE 24765:2017,3.872]

4 工业互联网兼容性层面和级别的描述

4.1 工业互联网兼容性层面

4.1.1 概述

工业互联网兼容性要求是工业互联网各不同技术层面的总体要求中的一个独立部分。

工业互联网实体的兼容性用功能层面和非功能层面表述。如同 ISO/IEC 30141 所定义的,物联网和工业互联网设备的物理实体是传感器和执行器。4.1.2 和 4.1.3 提供的信息详见附录 A 中的核查表。

4.1.2 工业物联网实体的连接功能兼容性描述

为确定工业物联网实体的连通性功能兼容性要求,相应的工业物联网实体层面如下。

a) 物理层面

为确保工业物联网实体与所关注的数据传输媒体的兼容性,宜解决以下问题:在数据收发器的物理接口之间交换信号时使用相同的媒体,在物理信道上传输信号的格式(模拟、数字),以及确保电磁兼容。

[来源:ISO/IEC 7498-1,IEC 61000-1-2:2016]

b) 媒体访问控制层面

确保工业物联网实体在媒体访问控制子层的兼容性,宜对控制数据传输媒体的访问达成一致。解决检测和网络帧冲突等可能出现的问题,并为局域网中的节点分配地址。

[来源:ISO/IEC/IEEE 8802-1AC,IETF RFC 2637,IETF RFC 2341,IETF RFC 2661]

c) 逻辑链路控制层面

工业物联网实体在通过预先配置的逻辑链路传输数据时,宜确保其兼容性包括以下几点:

- 1) 有助于将不同拓扑结构的网络进行组合;
- 2) 当媒体访问控制子层数据传输过程中出现错误时,支持网络帧的生成和有效的纠错;
- 3) 便于对已建立的通信信道进行适当的数据传输控制。

[来源:ISO/IEC 8802-2:1998]

d) 网络层面

确保工业物联网实体在网络层的兼容性对于支持统一寻址方案和消息路由至关重要。这有助于质量控制,管理和重新配置网络逻辑拓扑。

[来源:ISO/IEC 7498-1,IETF RFC 791]

e) 传输层面

确保工业物联网实体间的兼容性宜考虑多路复用/多路分解的兼容性以及匹配选项的支持,例如,通过已建立的连接进行数据传输并控制等。

[来源:ISO/IEC 7498-1,ITU-T X.224,ITU-T X.225,ITU-T X.234,IETF RFC 1122]

f) 会话层面

确保工业物联网实体间的兼容性事宜考虑在全局网络上建立和完成通信会话的机制以及维护和同步会话的机制。

[来源:ISO/IEC 7498-1,ITU-T X.224,ITU-T X.225,ITU-T X.234,IETF RFC 1122]

g) 数据表示层面

确保数据展示层的兼容性宜通过使用专用协议来解决数据格式不同的问题,通过这些协议对数据进行编码/解码和在网络上传输前的数据压缩。

[来源:ISO/IEC 7498-1,W3C 可扩展标记语言(XML)1.0(第五版),IETF RFC 4506,IETF RFC 7303]

h) 应用层面

为确保应用层的兼容性宜解决访问网络服务、交换应用特定服务消息、错误检测和纠正等方面可能出现的问题。

[来源:ISO/IEC 7498-1]

i) 测量和自动化层面

确保工业物联网设备(传感器,执行器)的测量和自动化以及应用程序和服务的兼容性,宜保证工业物联网传感器/执行器的物理接口兼容,以解决异构传感器,执行器和工业物联网应用

程序和服务的互操作的问题。

[来源:ITU-T H.810,ITU-T H.811]

j) 语义层面

确保语义层面的兼容性宜解决工业物联网设备之间交换信息时语义正确解释的问题。

[来源:ITU-T Y.4111/Y.2076]

4.1.3 工业物联网实体的非连通性功能兼容性描述

为了确定工业物联网实体的非连通性功能兼容性要求,宜考虑以下层面。

a) 版本层面

确保版本兼容性宜旨在同一软件的任何早期或后期版本提供互操作能力(分别为后向和前向兼容性)。

[来源:ISO/IEC/IEEE 9945]

b) 服务质量管理层面

确保服务质量管理方法的兼容性宜解决处理数据及时性、不同类型数据处理及优化(如选择数据传递路径)时可能出现的问题。

[来源:ITU-T G.1010,IETF RFC 4594]

c) 保护和隐私层面

确保支持工业物联网实体安全方法的兼容性,宜解决保护机制的设计和实现中的差距,并确保这些解决方案的可信度,如数据的保密性和完整性,服务提供的可用性、可靠性、隐私、安全性和整体工业物联网基础设施的弹性。

[来源:ISO/IEC 27000~ISO/IEC 27008,ITU-T X.1362,ITU-T Y.4806]

d) 合规层面

确保与国际、国家和行业标准、指南、法律和法规的兼容性,有助于建立全球信息环境并促进技术转移,以符合特定国家、行政单位、社区或工业部门的相关法律要求。

e) 安全层面

确保工业物联网功能不会干预、破坏已实施的安全功能或影响已应用的安全措施。

[来源:IEC 62368-1:2023,IEC TR 63069:2019,IEC 61508]

4.2 工业物联网兼容性级别

宜定义以下工业物联网的兼容性级别。

a) 完全兼容:在工业系统中,信息资源或其他工业物联网实体应在共享环境中交换信息并执行其需求功能,而无需修改其输入和/或输出接口、协议、软件和硬件手段或引入转换设备(适配器、网关等)。

b) 兼容:在工业系统中,信息资源或其他工业物联网实体应能通过调整输入/输出接口、协议、软件和硬件手段,或者引入转换设备(适配器、网关等),在共享环境中交换信息并执行所需的功能。

c) 部分兼容:工业系统、信息资源或其他工业物联网实体应能在共享环境中一定程度上交换信息,并在此环境中执行一组受限的功能,可能需要借助额外的工具来统一或转换其输入/输出接口、协议、软件和硬件实现的程序。这种部分兼容性可通过各方协商可接受的功能约束来实现。

d) 不兼容:由于技术、功能或非功能需求等方面的巨大差异,工业系统、信息资源或其他工业物联网实体无法在共享环境中交换信息,且无法执行一组受限的需求功能。

5 兼容性要求

5.1 连接功能兼容性层面

5.1.1 物理层面兼容性要求

为了确保工业物联网实体在物理方面的兼容性,以下规定适用。

- a) 数据传输介质兼容性。任何网络节点宜支持在同一传输介质上进行数据传输/接收,或者宜具有适当的设备,以确保在不同介质(有线:电线、铜线、光纤;无线:无线电信道、激光等)上传输数据的网段互操作。关于数据传输介质支持的兼容性级别如下。
 - 1) 完全兼容。节点使用相同的数据传输介质。
 - 2) 兼容。使用特定的适配器来兼容网络中的节点。
- b) 数据传输/接收系统兼容性。连接到网络的节点的物理接口宜支持基于网络中选择的传输格式的数据传输/接收(模拟、数字)。兼容性级别如下。
 - 1) 完全兼容。网络节点使用相同的数据传输格式(例如:PSTN 设备—PSTN 设备,无线电发送器—无线电接收器)。
 - 2) 兼容。网络节点使用了数模转换器或模数转换器。
- c) 电磁兼容性。如果在特定的网络中使用无线数据传输介质进行数据传输,则需要根据 IEC 61000(所有部分)考虑网络设备的电磁兼容性。

5.1.2 媒体访问控制层面兼容性要求

为确保工业物联网在媒体访问控制子层的兼容性,以下规定适用。

- a) 媒体访问兼容性。为了正确访问数据传输媒体,连接到公共媒体的网络节点的传输/接收网络接口应具有公共数据传输媒体访问同步系统。兼容性级别如下。
 - 1) 完全兼容。访问数据传输媒体的节点基于相同的数据传输媒体访问控制技术(例如:CSMA/CA—CSMA/CA)。
 - 2) 不兼容。访问数据传输媒体的节点基于不同的数据媒体访问控制技术(例如:DTDMA—CSMA/CA)。
- b) 框架兼容性。为了保证媒体访问控制子层数据交换的正确性,需要为所有连接到网络的节点提供一个通用的单一寻址框架。兼容性级别如下。
 - 1) 完全兼容。网络节点遵守通用的单一链路层寻址框架(例如:MAC-48—MAC-48)。
 - 2) 兼容。网络节点具有不同的链路层寻址框架,但是提供了转换机制(例如:EUI-48—EUI-64)。
 - 3) 不兼容。网络节点遵循不同的不兼容链路层寻址框架(例如:IAB—EUI-64)。
- c) 检测和调解数据传输冲突程序的兼容性。为了正确检测和调解数据传输冲突,需要通过同步数据冲突检测和调解协议(算法)来确保所有网络设备上的冲突控制系统的正确互操作。兼容性级别如下。
 - 1) 完全兼容。用于网络节点的数据冲突检测和调解协议(算法)完全相同(例如:里德-所罗门码—里德-所罗门代码)。
 - 2) 兼容。此级别通过使用附加的软件或硬件设备来考虑冲突避免策略。
 - 3) 不兼容。用于网络节点的数据冲突检测和调解协议(算法)不兼容(例如:Turbo 卷积码—里德-所罗门码)。

5.1.3 逻辑链路控制层面兼容性要求

为了确保工业物联网实体在通过预配置的逻辑链路控制子层进行数据传输时的兼容性,以下规定适用。

- a) 网络拓扑的兼容性,包括交换过程。兼容性级别如下。
 - 1) 完全兼容。网络支持相同或一致的拓扑。
 - 2) 兼容。网络支持不同的拓扑结构,可通过使用协议扩展来集成(例如:ISO/IEC/IEEE 8802-1q)。
 - 3) 不兼容:网络支持实质上不同且无法集成的拓扑结构。
- b) 网络帧生成和解释的兼容性。为了在网络上正确传输数据,需要确保所有网络设备都使用通用的网络帧格式,以正确执行数据传输/接收流程、网络帧生成和解释。兼容性级别如下。
 - 1) 完全兼容。网络节点支持相同的生成和解释网络帧的技术(例如:ISO/IEC/IEEE 8802-3—ISO/IEC/IEEE 8802-3)。
 - 2) 兼容。网络节点支持不同的网络帧生成和解释的技术,但是帧格式彼此兼容(例如:ISO/IEC/IEEE 8802-3—ISO/IEC/IEEE 8802-11)。
 - 3) 不兼容。网络节点支持不同的网络帧生成和解释的技术,但是帧格式彼此不兼容(例如:ISO/IEC/IEEE 8802-3—ISO/IEC/IEEE 8802-15-4)。
- c) 在已建立的通信信道上的数据传输控制程序的兼容性。为了确保数据的正确传输,宜在所有网络节点实施通用的单一数据传输控制程序。兼容性级别如下。
 - 1) 完全兼容。网络节点支持在已建立的通道上进行数据传输的相同管理程序(例如:ISO/IEC/IEEE 8802-3/IP LLC—ISO/IEC/IEEE 8802-3/IP LLC)。
 - 2) 不兼容。网络节点支持在建立的通道上进行数据传输的不同管理程序(例如:ISO/IEC/IEEE 8802-3/IP LLC-6LoWPAN)。

5.1.4 网络层面兼容性要求

为了确保工业物联网实体在全局联网方面的兼容性,以下要求适用。

- a) 路由兼容性。为了将数据准确地传输到工业物联网实体,需要确保所有工业物联网实体(作为网络节点)在节点标识,查找数据传输路径以及在互操作实体间建立连接等方面的协同运行。路由器和类似设备是将单独的网络连接成全局空间,提供互连能力的主要设备。因此,要确保网络层兼容。兼容级别如下。
 - 1) 完全兼容。实现其功能的路由器为每个相互操作的节点对提供了计算最优路径的环境,无需额外操作(例如:所有交互节点均实现 IPv4)。
 - 2) 兼容。实现其功能的路由器为每个相互操作的节点对提供了计算最优路径的环境,但需要使用附加设备或软件。
 - 3) 部分兼容。路由器在实现其功能时,为每个相互操作的节点对提供了计算路由的环境,但会限制可用地址的数量以及其他协议功能,如加密、服务质量保证等(例如:IPv4—IPv6)。
 - 4) 不兼容。执行其功能的路由器提供的环境无法为每对相互操作的节点计算路由(例如:IPv4—LoRaWAN)。
- b) 网络协议兼容性。由于网络层提供了将分离网络统一到单一网络环境中的能力,因此需要定义关于网络协议的兼容性。兼容性级别如下。
 - 1) 完全兼容。工业物联网实体实施的协议在网络层执行的功能方面是互补的(例如:IP—

ICMP)。网络协议可在网络中和脱离网络的设备上支持联合操作。

- 2) 兼容。工业物联网实体实施的协议可在网络中共存,并通过引入额外的软件和设备支持与其他网络协议的联合操作。网络协议既支持网络中设备的协同操作,也支持与网络分离的设备的协同操作。
- 3) 不兼容。工业物联网实体实施的协议不支持协同操作。
- c) 标识符兼容性。为了确保正确的数据交换,需要在协议栈的网络层提供对相同标识/寻址方案的支持。兼容性级别如下。
 - 1) 完全兼容。工业物联网实体支持相同的寻址方案和标识符格式。
 - 2) 兼容。工业物联网实体支持不同的寻址方案,但标识符能轻松地一对一映射。
 - 3) 部分兼容。一个或多个工业物联网实体支持提供更大地址空间的地址方案,但并非所有使用的标识符都存在来自另一个空间的相应标识符,或者无法找到这样的标识符。
 - 4) 不兼容:工业物联网实体使用不同的标识系统。

5.1.5 传输层面兼容性要求

为了确保工业物联网实体在传输支持层面的兼容性,以下要求适用。

- a) 多路传输/解多路传输兼容性。为了确保向工业物联网实体实施的应用和服务正确地传送数据,传输层的地址宜包含足够的附加信息,以便在工业物联网实体之间传送多路复用/解复用消息。兼容性级别如下。
 - 1) 完全兼容。工业物联网实体在传输层支持相同的复用/解复用方案和通道标识符的格式。
 - 2) 兼容。工业物联网实体支持不同的复用/解复用方案,但标识符能轻松地一对一映射。
 - 3) 部分兼容。工业物联网实体之一支持多路复用/解多路分解方案,该方案提供更大范围的标识符,而不是为该空间中的所有标识符提供或能找到另一空间中的相应标识符。
 - 4) 不兼容。工业物联网实体使用无法彼此映射的不同复用/解复用系统。
- b) 传输选项兼容性。为了确保工业物联网实体在网络之间正确及时地传递数据,需要确保这些实体支持的传输层选项兼容,例如连接支持,错误检测和更正,传递保证等。兼容性级别如下。
 - 1) 完全兼容。用于互操作的工业物联网实体的传输层协议相同(例如:TCP—TCP)。
 - 2) 兼容。适当的协议提供的传输层选项允许组合(可能通过转换)这些协议,而不会失去对该层数据传输的任何参数和模式的支持。
 - 3) 部分兼容。适当的协议提供的传输层选项允许组合(可能通过转换)这些协议,但不能保证支持此层的所有参数和数据传输方式。
 - 4) 不兼容。互操作性工业物联网实体的传输协议不同,并且不支持互操作性功能(例如:SCTP—UDP)。

5.1.6 会话层面兼容性要求

为了确保工业物联网实体在会话支持和管理方面的兼容性,以下要求适用。

- a) 会话传递和支持的兼容性。为了实现工业物联网实体之间的数据交换能力,并在确定的会话中向这些实体提供的服务交付数据,需要确保寻址节点、服务和会话兼容。兼容性级别如下。
 - 1) 完全兼容。工业物联网实体使用的网络,传输和会话协议是相同的,并且它们的实现方式并不限制这些实体根据会话的既定要求在每个会话之间进行完整、及时和准确的数据交换所需的关键功能。

- 2) 兼容。工业物联网实体使用的网络、传输和会话协议并不相同,但可通过转换的方式,根据已建立的会话要求,支持这些实体之间的完整和准确的数据交换。
 - 3) 部分兼容。但它们的实现限制了在会话期间支持这些实体之间数据交换的某些选项的能力(例如,在数据仍在工业物联网实体之间传输时请求特定服务的可能性,或者在已标识会话期间向服务传输数据的准确性)。
 - 4) 工业物联网实体或其实现使用的网络、传输和会话协议限制了这些工业物联网实体之间数据交换所需的关键功能。
- b) 会话控制协议兼容性。为了确保控制两个互操作的工业物联网实体之间的会话控制,需要提供会话协议兼容性。兼容性级别如下。
- 1) 完全兼容。工业物联网实体用于互操作节点的会话协议相同。
 - 2) 兼容。工业物联网实体使用的会话协议非常相似,但是它们重叠的功能集受到限制(例如,定时或服务选项可能不同)。
 - 3) 不兼容。用于互操作工业物联网实体的会话协议是不同的,不支持所需类型的互操作功能(例如:SCP—H.245)。

5.1.7 数据表示层面的兼容性要求

为了确保工业物联网实体在数据表示方面的兼容性,需要满足以下要求。

- a) 数据编码/解码和压缩协议的兼容性。为了正确地将应用层协议和应用程序接收到的数据转换为适合在网络上传输的数据格式,需要确保工业物联网实体中实施的数据编码/解码和压缩协议与其他工业物联网实体中实施的协议兼容。兼容级别如下。
- 1) 完全兼容。互操作的工业物联网实体之间的数据编码/解码和压缩协议完全相同。
 - 2) 兼容。互操作的工业物联网实体之间的数据编码/解码和压缩协议不完全相同,但可通过协商参数或使用转换机制相互转换。
 - 3) 不兼容。互操作的工业物联网实体之间的数据编码/解码和压缩协议不同,并且不支持相互转换功能。
- b) 加密/解密协议兼容性。为了建立一个安全的连接并确保通过该链接正确传输数据,需要加密/解密协议兼容。兼容性级别如下。
- 1) 完全兼容。工业物联网实体使用的加密/解密协议是相同的,它们的实现不影响其联合使用,并规定了相同的算法、参数和密钥要求。
 - 2) 兼容。工业物联网实体使用的加密/解密协议是相同的,但它们的实现或对算法、参数或加密密钥的要求在某种程度上限制了它们的共同使用,但仍保留了一些满足各方最低要求的选项(因此各方宜就可用选项进行协商)。
 - 3) 部分兼容。工业物联网实体使用的加密/解密协议是相同的,但它们的实现或对算法、参数或加密密钥的要求在某种程度上限制了它们的联合使用,而没有留下响应一方或多方最低要求的选项(即它们宜协商改变风险最低的值或拒绝通信)。
 - 4) 不兼容。用于互操作的工业物联网实体的加密/解密协议不同,并且不支持互操作性功能。

5.1.8 应用层面兼容性要求

为了确保工业物联网实体在应用方面的兼容性,需要满足以下要求。

- a) 应用层协议和应用程序的兼容性。为了使应用层协议正确运行,需要确保此类协议与使用它们的应用程序兼容。兼容性级别如下。

- 1) 完全兼容。应用程序专门为选定的应用协议实现部分功能。
 - 2) 兼容。工业物联网实体使用的应用层协议在功能和/或规格上相似,即使使用了协议转换器或网关,但也仅提供这些协议的受限功能集供所有实体使用。
 - 3) 部分兼容。应用程序不使用所选的应用程序协议来实现其功能的一部分,而是提供用于将所选协议转换为某种其他协议或数据格式的转换机制。
 - 4) 不兼容。应用程序既未使用所选的应用程序协议来实现其部分功能,也没有提供任何特定机制来转换由于功能目的或规范的巨大差异而产生的协议。
- b) 应用协议与网络套件的兼容性。为了将数据从应用协议格式转换为数据传输格式,需要确保应用协议与网络服务(网络套件)兼容。兼容性级别如下。
- 1) 完全兼容。这种应用协议与较低 OSI 层的网络服务完全兼容。
 - 2) 兼容。未规定此级别的要求。
 - 3) 部分兼容。给定的协议与较低 OSI 层的网络服务不兼容,但是具有将这种协议转换为与网络套件兼容的另一个应用程序协议的特殊机制。
 - 4) 不兼容。给定的协议与较低 OSI 层的网络服务不兼容。
- c) 应用程序协议兼容性。为了确保在相互操作的工业物联网实体之间运行的应用程序之间进行正确的数据交换,需要确保此类协议之间的应用协议兼容。兼容性级别如下。
- 1) 完全兼容。用于工业物联网实体交互的应用程序协议完全相同,并支持这些工业物联网实体运行的应用程序的全面协同工作。
 - 2) 兼容。工业物联网实体之间的应用协议不完全相同,但是已建立起特殊的相互转换机制,用于解释彼此接收的消息,并支持由工业物联网实体运行的应用程序的全面协同工作。
 - 3) 部分兼容。工业物联网实体之间的应用协议并不完全相同,但是由工业物联网实体运行的应用程序能够执行一些协同工作,但并不全面。
 - 4) 不兼容。由于所支持协议存在显著差异,工业物联网实体运行的应用程序无法协同工作。

5.1.9 测量和自动化方面的兼容性要求

为了确保工业物联网实体在测量方面的兼容性以及自动化的适当和一致支持,需要满足以下要求。

- a) 与测量设备的交互协议兼容性。为了与传感器/执行器正确交互,要求控制设备(CD)的物理接口兼容性要求与测量设备(MD)支持的接口兼容性要求相匹配。兼容性级别如下。
- 1) 完全兼容 CD 具有与 MD 兼容的物理接口,并支持与 MD 互操作的协议。
 - 2) 兼容。未规定此级别的要求。
 - 3) 部分兼容。CD 没有与 MD 互操作所需的物理接口,或者不支持与此类设备的互操作协议。在这种情况下,可通过将特定的转换单元连接到 CD 来使用此类测量设备进行操作。
 - 4) 不兼容。CD 没有用于与 MD 或专用转换单元一起操作的物理接口。

5.1.10 语义方面的兼容性要求

为了确保工业物联网实体的语义兼容性,需要满足以下要求。

- a) 会话理解和范围兼容性。为了确保工业物联网实体正确的语义交互,需要确保它们对会话范围识别和理解的方法相同或相似。兼容性级别如下。
- 1) 完全兼容。工业物联网实体以完全相同的方式定义会话概念,包括会话参数及其解释。

- 2) 兼容。工业物联网实体以稍微不同的方式定义会话概念,但对会话是什么以及宜支持哪些会话参数的一般描述方法以及一般方法基本一致。
- 3) 不兼容。工业物联网实体以完全不同的方式定义会话,因此即使某些参数相同,也无法将这些实体的会话概念进行匹配。
- b) 消息格式解释方法的兼容性。为了正确解读设备、用户、系统和服务之间的数据,需要确保从给定的工业物联网实体中实现相互解读消息格式。兼容性级别如下。
 - 1) 完全兼容。在相互操作的工业物联网实体之间进行数据交换时,消息格式及其参数的解释方法完全相同。
 - 2) 兼容。用于互操作的工业物联网实体之间的数据交换的消息格式与这些消息及其参数的解释方法相似,可能相互支持,可能通过转换机制实现,不会丢失任何参数。
 - 3) 部分兼容。互操作的工业物联网实体之间数据交换的格式和对这些消息及其参数的解释方法可能相互支持,可能通过转换机制实现,但会丢失一些可选参数。
 - 4) 不兼容。工业物联网实体支持的消息格式以及这些消息的解释方法及其参数无法相互转换。
- c) 数据解释方法的兼容性。为了正确感知和呈现从测量设备接收到的信息,需要确保现有工业物联网系统中的实体对这些信息进行正确的解释。兼容性级别如下。
 - 1) 完全兼容。不同的工业物联网实体对数据的感知、解释和呈现方式相同。
 - 2) 兼容。不同工业物联网实体对数据的感知和解释方式相同,或者数据可轻松转换以获得所需的解释。信息的呈现方式可能不同。
 - 3) 不兼容。不同工业物联网实体对数据的感知和解读方式存在显著差异。这些类型的解读无法相互转换。

5.2 非连接功能兼容性要求

5.2.1 版本兼容性的兼容性要求

为了确保工业物联网解决方案版本间的兼容性,宜满足以下要求。

- a) 后向兼容。一个新的解决方案版本宜具有确保与同一解决方案的早期版本正确互操作的功能。兼容级别如下。
 - 1) 完全兼容。给定的解决方案具有某些方法来确保与先前版本向后兼容。
 - 2) 不兼容。给定的解决方案没有方法来确保与先前版本向后兼容。
- b) 前向兼容。早期版本的解决方案宜具有确保与同一解决方案的后续版本正确交互的功能。兼容级别如下。
 - 1) 完全兼容。给定的解决方案具有某些或其他方法来确保与工业物联网解决方案的更高版本的向前兼容性。
 - 2) 不兼容。给定的解决方案没有方法来确保与后续版本向前兼容。

5.2.2 服务质量管理的兼容性要求

为了确保工业物联网实体在服务质量方面的兼容性,宜满足以下要求。

- a) 服务质量管理的兼容性等级如下。
 - 1) 完全兼容。工业物联网实体的服务质量管理方法相同。
 - 2) 兼容。QoS 管理方法相似,可稍作调整以共同使用,不会丢失构成管理主题的任何参数。
 - 3) 部分兼容。QoS 管理方法相似,可稍作修改以共同使用,但会丢失部分构成管理主题的参数。

- 4) 不兼容。所选的应用协议与解决方案中正在使用的服务质量管理方法不兼容,并且没有自己的服务质量管理体系。

5.2.3 安全和隐私方面的兼容性要求

由于工业物联网实体间的目的和安全目标可能存在差异,安全和隐私的兼容性要求宜满足以下要求:

- a) 安全策略兼容性是指在两个工业物联网实体中支持安全规则和约束的能力,这些规则和约束将以一致的方式组合或集成,并且不会干扰两个系统的功能目的、隐私策略、安全和其他可信度方面及非功能性要求;
- b) 隐私政策的兼容性是指在两个工业物联网实体中支持存储和处理个人数据的规则和约束的能力,这些规则和约束将以一致的方式组合或集成,并且不会干扰功能目的、安全政策、安全和其他可信度方面及非功能性要求。

功能规范层面提供了安全政策和隐私约束层次的兼容性。

虽然安全策略和隐私策略在逻辑上是分开的,甚至可能追求相反的目标,但它们的实施方法通常是相似的。支持安全和隐私的方法和技术能力在一定程度上与工业物联网实体的架构设计和通信协议相关联。如果安全策略和隐私策略一致,则他们通常由相同或类似技术手段实施。

因此,安全级别上进一步的兼容性和隐私上的兼容性被视为一个整体(称之为安全级别的兼容性)。

为确保工业物联网实体在安全级别的兼容性,宜满足以下条件。

- a) 安全策略的兼容性。兼容性级别如下。
 - 1) 完全兼容。相同类型的安全性机制会强制执行一致的安全性策略,这些策略既不相互约束,也不约束应用这些策略的工业物联网实体的功能。
 - 2) 兼容。工业物联网实体在安全策略的实施方面是兼容的。实施安全策略的安全机制可通过以下方式进行配置,使这些策略既不相互约束,也不约束应用这些策略的工业物联网实体的功能。
 - 3) 部分兼容。工业物联网实体设置了一致的安全策略。工业物联网实体的安全机制可能会相互限制或者由于功能、环境或其他限制而不允许一起使用。同时,安全策略允许通过为这些解决方案新引入的控制来联合实施。
 - 4) 由于安全策略而不兼容。

以下是关于安全策略兼容性的一般考虑事项。

安全策略的一致性和兼容性。如果两个工业物联网实体支持不同的安全策略,则它们的一致(并因此是兼容的)的安全策略应代表构成这些策略的规则和约束的交集。如果兼容规则集不允许任何内容,则初始安全策略不兼容。如果兼容的安全策略与工业物联网实体的其他功能或非功能要求不一致,则工业物联网实体由于其安全策略而不兼容。

工业物联网实体在安全策略上实现的兼容性。工业物联网系统实现和配置宜与其安全策略一致。如果两个工业物联网实体中至少一个的实现和配置与其兼容的安全策略不一致,则这些工业物联网实体由于其安全策略而不兼容。

关于兼容安全策略的协商。检查安全策略的兼容性和协商兼容的安全策略可通过以下方法之一来执行。

- 1) 第一种,分散式方法要求使用特定协议在工业物联网实体之间交换参数以协商安全机制。
- 2) 第二种,集中式方法是基于使用中央设备或网关从其他解决方案接收参数,并根据适合所有环境的选项来设置安全机制。

实施兼容的安全策略。在需要兼容性的工业物联网实体的整个功能上实施兼容安全策略通常是无效的。合理的方法是识别互补约束并将其应用于来自另一种工业物联网解决方案的控制和信息流。

对于分散式方法,每个工业物联网解决方案都负责实施兼容的安全策略,同时交换信息和/或参与与其他解决方案的控制关系。这种方法能仅在通信的接收方一侧强制执行兼容的安全策略。因此,它可能会给安全性提供较少的保证。

对于集中式方法,中央设备或网关负责信息流和控制流的分离以及对这些流实施兼容的安全策略。这种方法能透明且独立于通信的任何方面实施兼容的安全策略。因此,它有可能为安全性提供更严格的保证。

实施兼容安全策略的网关宜实现以下基本功能。

- a) 根据在这些域中有效的安全策略,将工业物联网实体的通信环境划分为网域(或网段):
 - 1) 验证安全策略的一致性和兼容性;
 - 2) 验证安全策略实现的兼容性;
 - 3) 协商兼容的安全策略;
 - 4) 根据这些域中工业物联网实体的兼容安全策略,验证这些域之间的控制和信息流;
 - 5) 验证消息或其他通信单元的兼容安全策略是否完成。
- b) 通信和连接安全功能的兼容性是指支持安全且可信赖的信息交换的功能,这些功能符合兼容工业物联网实体的合并安全目标。兼容性级别如下。
 - 1) 完全兼容。实现通信保护功能的安全机制可协商他们认为安全和可信赖的信息交换参数。
 - 2) 兼容。在安全策略方面保持一致(并兼容)。工业物联网实体在通信和连接性方面具有相同的关注点和目标。根据这些关注点和目标,实现安全可靠的信息交换需要至少对通信双方中的一方实施通信的安全机制。
 - 3) 不兼容。工业物联网实体在通信和连接性方面具有相同的关注点和目标,满足这些关注点和目标,将会约束彼此或者至少其中一个解决方案的主要功能。
- c) 特定服务安全功能的兼容性是指有助于由服务提供商提供并由其他兼容工业物联网实体使用的服务的应用程序级安全性和可信度的特征。兼容性级别如下。
 - 1) 完全兼容。实施服务特定安全功能的安全机制可加入到安全解决方案中,工业物联网解决方案可作为一个整体来执行符合所有工业物联网服务需求的安全策略。
 - 2) 兼容。安全策略方面保持一致(并兼容)。工业物联网实体在服务提供方面具有相同的安全问题和目标。
 - 3) 不兼容。工业物联网实体在服务提供方面存在安全关注点和目标,满足这些关注点和目标,将会约束彼此或者至少其中一个服务实现的应用程序级功能受到约束。
- d) 安全集成功能的兼容性是指减轻与兼容的工业物联网实体集成过程相关的风险。兼容性级别如下。
 - 1) 完全兼容。支持工业物联网实体的集成过程的安全集成能力(软件 and 设备的完整性和真实性控制,供应链的验证)与这些工业物联网实体一致,并且不限制其预期的功能和共同使用的可能性。
 - 2) 不兼容。支持工业物联网实体之一的集成过程而实现的安全集成能力极大地限制了联合使用这些解决方案的可能性。
- e) 身份认证和授权功能的兼容性是指可使用相同的方案,因素,协议和技术手段,提供对兼容工业物联网实体功能授权访问的可能性。兼容性级别如下。
 - 1) 完全兼容。工业物联网实体的身份认证和授权机制实现了相同或非常相似的方案、因

素、协议和功能,以提供对这些工业物联网实体功能的授权访问。

- 2) 兼容。在身份验证和授权策略方面是一致的(并兼容)。对工业物联网实体功能的授权访问要求实施方案、因素、协议和身份验证功能,以允许它们通过至少一种解决方案的新引入机制共同实施。
 - 3) 不兼容。对工业物联网实体之一功能的授权访问要求实施方案、因素、协议和身份验证功能,这些功能至少不适用于这些解决方案中的一种,反之亦然。
- f) 安全审计功能的兼容性,安全审计能力的兼容性,事件和参数的可追溯性以及根据综合结构整合日志条目的可能性。兼容性级别如下。
- 1) 完全兼容。由工业物联网实体实现的安全审计能力提供了其兼容审计策略所需的所有数据,并允许共同使用记录的与安全相关事件。
 - 2) 不兼容。由工业物联网实体实现的安全审核功能要么无法提供这些解决方案兼容审核策略所需的所有数据,要么不允许共同使用记录的安全相关事件。
- g) 加密手段的兼容性是指各种目的(用于加密数据,验证源真实性等)加密协议,加密算法及其参数的兼容性。密码算法和协议的实现宜提供有关参数及其配置的协商,这些参数及其配置应符合当地法律以及计划使用兼容解决方案的州和地区的出口限制。兼容性级别如下。
- 1) 完全兼容。密码机制根据相似的安全目标并使用相同的协议和算法,对数据进行一致的保护。这些机制既不相互制约,也不约束这些策略所适用的工业物联网实体的功能。密码密钥管理协议和基础结构相同。
 - 2) 在协议和算法方面兼容。密码机制根据相似的安全目标并使用相同的协议和算法,对数据进行一致的保护。这些机制既不相互制约,也不约束这些策略所适用的工业物联网实体的功能。关键管理基础架构需要实现。
 - 3) 部分兼容。在数据保护目标方面保持一致(和兼容)。工业物联网实体对数据的密码保护设置了相同或非常相似的要求。可使用相同的算法和协议,但并非所有各方都喜欢它们。需要为这些工业物联网实体和密钥管理基础架构中的至少一个实施加密机制。
 - 4) 不兼容。加密机制的实施目标不同。

5.2.4 合规性的兼容性要求

为确保工业物联网实体与国际标准、指南、法律和法规兼容,以下要求适用。

- a) 国际兼容性。为确保工业物联网实体与需要遵守的国际标准、指南、法律和法规相兼容,工业物联网底层技术、设备和软件应遵循与这些标准、指南、法律和法规相同或相似的设计目标和原则。兼容性级别如下。
- 1) 完全兼容。底层的工业物联网技术,设备和软件遵循其设计目标和原则,这些目标和原则遵循国际标准、指南、法律和法规要求。
 - 2) 兼容。未规定此级别的要求。
 - 3) 部分兼容。底层的工业物联网技术,设备和软件遵循其设计目标和原则,这些目标和原则部分遵循国际标准、指南、法律和法规的要求。
 - 4) 不兼容。底层的工业物联网技术,设备和软件未遵循其设计目标和原则,这些目标和原则不遵循国际标准、指南、法律和法规的要求。
- b) 国家兼容性。为确保工业物联网实体与需要遵守的国家标准、指南、法律和法规相兼容,工业物联网底层技术、设备和软件应遵循与这些标准、指南、法律和法规相同或相似的设计目标和原则。兼容性级别如下。
- 1) 完全兼容。底层的工业物联网技术,设备和软件遵循其设计目标和原则,这些目标和原

则遵循国家标准、指南、法律和法规要求。

- 2) 部分兼容。底层的工业物联网技术,设备和软件遵循其设计目标和原则,这些目标和原则部分遵循国家标准、指南、法律和法规的要求。
 - 3) 不兼容。底层的工业物联网技术,设备和软件未遵循其设计目标和原则,这些目标和原则不遵循国际标准、指南、法律和法规的要求。
- c) 行业兼容性。为确保工业物联网实体与需要遵守的行业标准、指南、法律和法规相兼容,工业物联网底层技术、设备和软件应遵循与这些标准、指南、法律和法规相同或相似的设计目标和原则。兼容性级别如下。
- 1) 完全兼容。底层的工业物联网技术,设备和软件遵循其设计目标和原则,这些目标和原则遵循行业的标准、指南、法律和法规要求。
 - 2) 部分兼容。底层的工业物联网技术,设备和软件遵循其设计目标和原则,这些目标和原则部分遵循行业的标准、指南、法律和法规的要求。
 - 3) 不兼容。底层的工业物联网技术,设备和软件未遵循其设计目标和原则,这些目标和原则不遵循国际标准、指南、法律和法规的要求。

5.2.5 安全兼容性要求

为了确保工业物联网实体在安全方面的兼容性,以下建议适用。

工业系统安全措施。实施的系统不宜干扰企业安全系统的运行。兼容性级别如下。

- a) 完全兼容。工业物联网解决方案在确保企业安全方面没有任何问题。
- b) 部分兼容。如果满足某些安全条件,则能在企业中实施工业物联网解决方案。
- c) 不兼容。工业物联网解决方案无法在企业中实施。

6 工业物联网连通性设备和数据格式兼容性要求

本章描述了为两个或多个工业物联网系统提供连接的各种工业物联网协议中数据收集和数据转化的过程以及其他可能的方法。

为了实现兼容性,嵌入工业物联网设备的算法将格式化和生成传输消息。这些传输消息的格式是在系统开发阶段确定的。传输消息的格式宜基于标准化的协议及技术。当拥有工业物联网设备的系统投入运行时,从该系统中生成的消息应包括但不限于以下内容:

- a) 用于在工业物联网设备间传输服务信息的协议类型;
- b) 所使用的服务命令和服务消息格式类型;
- c) 数据收集算法;
- d) 数据存储规则;
- e) 数据访问规则;
- f) 数据保护策略;
- g) 服务质量策略。

语义工业物联网网关宜用作工业互联网连接框架中软件实现的一种解决方法,这种网关宜部署在单一工业物联网解决方案框架内,执行工业物联网协议之间的转换。

图 1 展示了一个硬件和软件集的示例,该硬件和软件集使用语义物联网网关连接基于不同工业物联网协议运行的各种子网络。

图 2 给出了一种通用的语义工业物联网网关体系结构示例。语义工业物联网网关是一组拥有两个或多个工业网络接口(即网络接口)的软件和硬件模块,基于操作系统运行。语义工业物联网网关支持每个网络接口的网络功能(即中间件)和生产环境的虚拟化(即虚拟化)。在一个虚拟化的生产环境

的基础上,能提供各种应用程序和服务,包括工业互联网连通性框架软件。

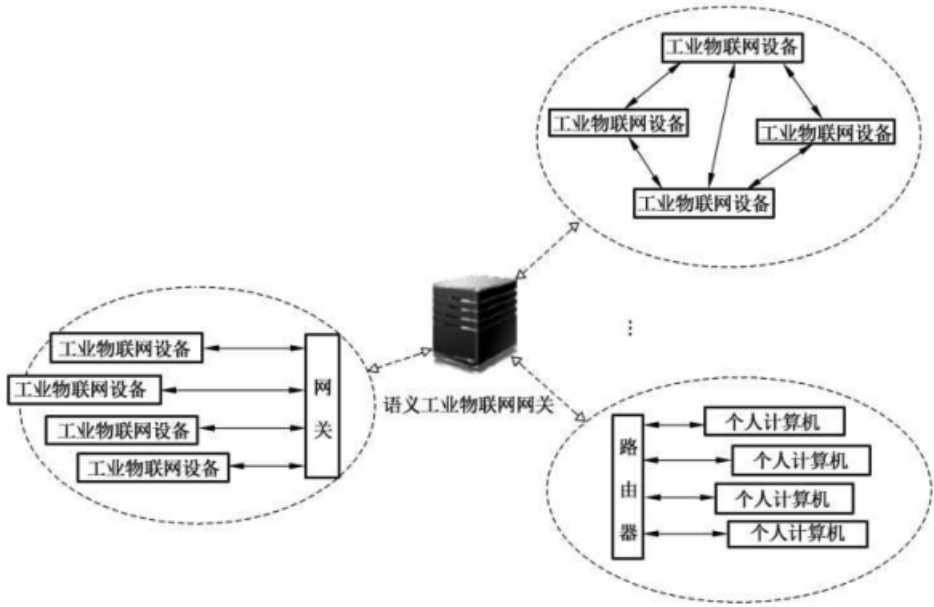


图 1 使用语义工业互联网网关进行工业互联网协议间转换的软件/硬件示例

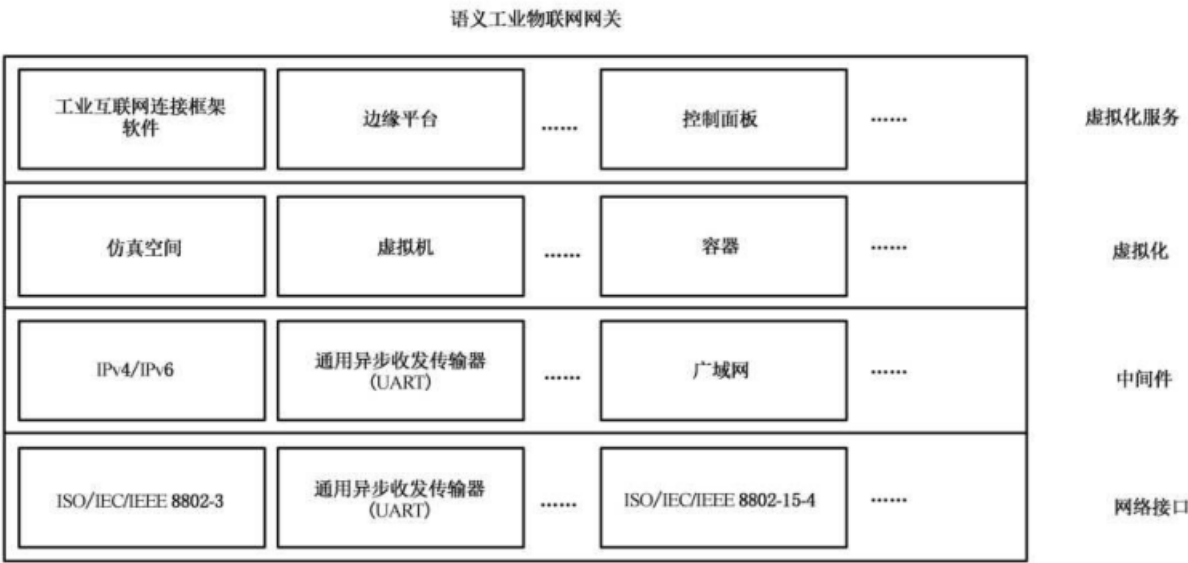


图 2 语义工业互联网网关架构示例

7 配备工业互联网网关的工业互联网系统模型

工业互联网系统通用模型如图 3 所示,通过工业互联网网关,将异构数据处理成通用数据格式以支持工业互联网平台,这种工业互联网网关被称为“异构网关”。

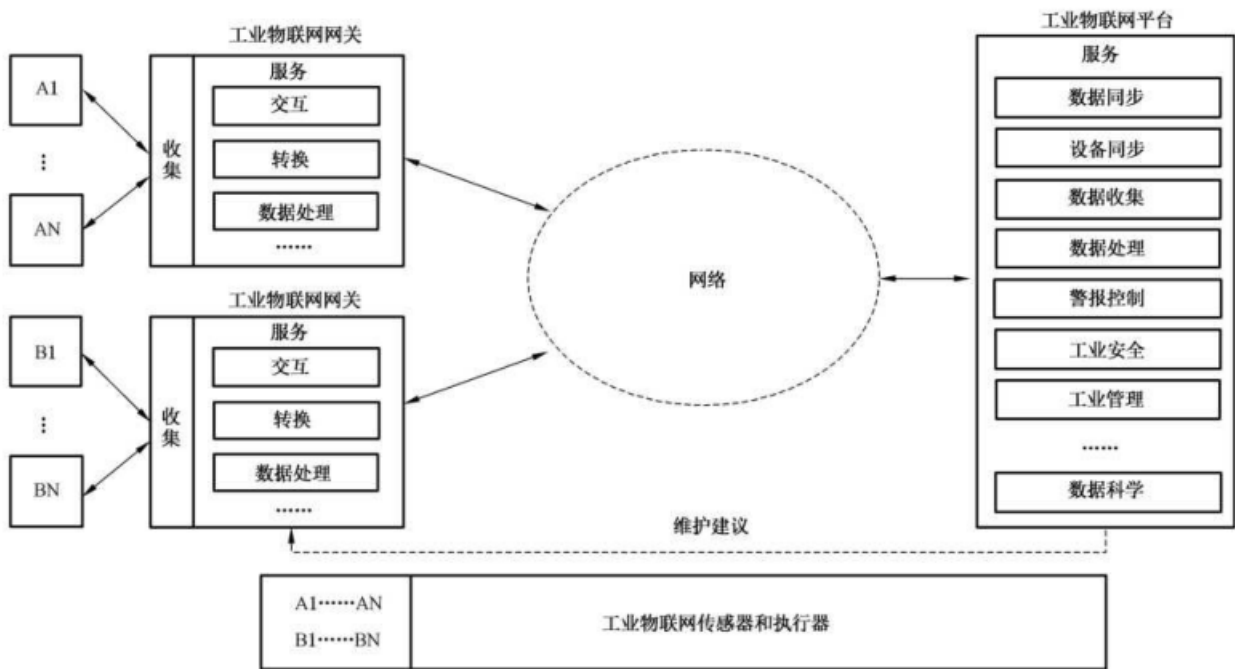


图 3 包含异构网关的工业物联网系统模型

如 Rec.ITU-T Y.4101/Y.2067 所定义的,物联网网关指的是物联网中的一个单元,它能使设备和通信网络互相连接。并且,它还能在通信网络中使用的协议和设备使用的协议之间起到必要的转换作用。

工业物联网网关(又名异构物联网网关)是物联网中的一个实体,它能让使用不同通信技术和协议的设备,互联网以及其他通信网络互相连接。

如 ETSI GS MEC 001 所规定:

- a) 移动边缘平台指的是在特定的移动边缘主机虚拟化基础架构上运行移动边缘应用程序并使它们能提供和使用移动边缘服务所需的功能集合,与此同时平台自身也能提供一系列的移动边缘服务;
- b) 移动边缘应用程序指的是能在移动边缘系统内的移动边缘主机上实例化的应用,它能潜在地提供或使用移动边缘服务;
- c) 移动边缘主机指的是包含移动边缘平台和虚拟基础架构的实体,它能为移动边缘应用程序提供计算,存储和网络资源。

边缘网关是一种异构的物联网网关,它参与了移动边缘主机的功能实现,尤其是数据处理功能。

如 Rec.ITU-T Y.4113 所定义的,物联网平台是一种技术性的基础设施,它能提供通用和特定功能的集成[见 Rec.ITU-T Y.4000]。这些与核心网络的功能相结合的功能可被暴露给一个或多个物联网应用服务器。核心网络提供通信功能,以支持通过访问网络而进行的向设备和网关的数据传输。而其中的一些功能也能被服务提供者使用。

工业物联网平台是用于工业的物联网平台,它由多种服务组成,包括数据收集、存储和处理功能。附录 B 中提供了工业物联网网关和服务器的性能测试场景和测试表的样例。

8 工业物联网兼容性测试的网络模型

图 4 中展示的网络模型包含 4 个子网络类型。

- a) 网络 1——此网络由工业设备组成,这些设备包括用于其管理的计算机设备。该计算机设备不能与工业管理系统通信。
- b) 网络 2——此网络由工业设备组成,这些设备不能使用数字设备来通过网络控制。它们由具有传感器和执行器的计算机设备控制。
- c) 网络 3——此网络由工业设备组成,这些设备包括用于其管理的计算机设备。该计算机设备与工业管理系统通信。
- d) 网络 4——此网络专用服务器计算机设备、用户终端和可选的一些带有数字计算机设备控制器的工业设备组成。这个远程子网络通过特定的计算机设备和其他网段连接,以建立虚拟私有网络通道。

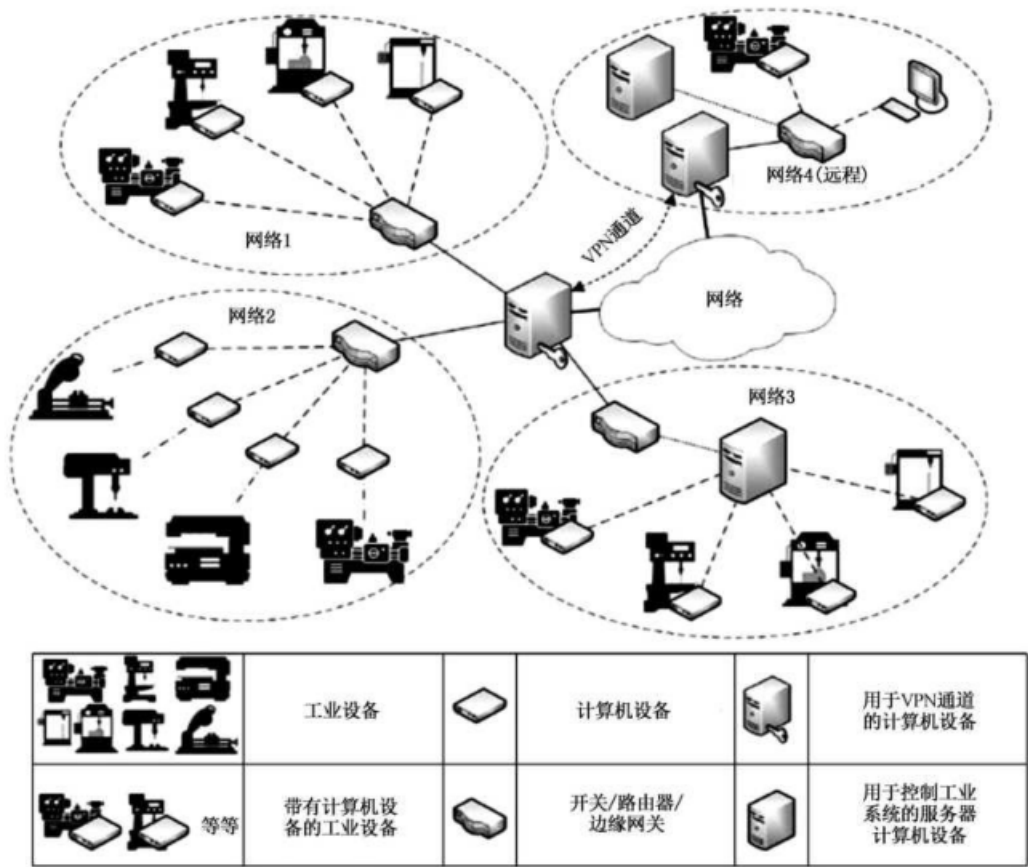


图 4 用于工业物联网兼容性测试的网络模型

更多特定的有关连接协议的供应商和技术信息,见附录 C。

9 工业物联网设备连接模型

9.1 直接连接

图 5 所示的模型描述了一种连接非数字工业设备和工业物联网服务平台的方法。这种非数字工业设备通过安装在它上面的传感器和数字控制器(如个人计算机、微型控制器、微型计算机等)连接。数字控制器通过一个 IP 兼容网络接口直接连接到一个工业物联网服务平台,而不需要经过网关。

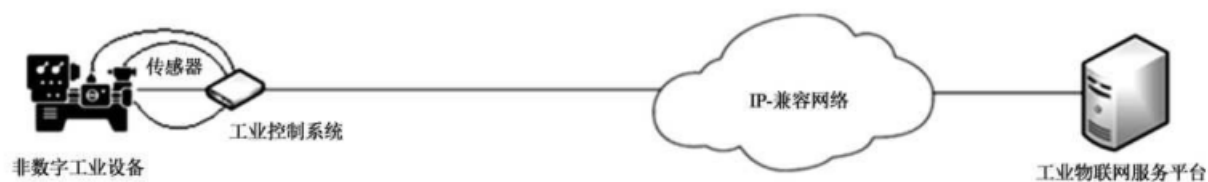


图 5 直接连接

完成以下操作后,非数字工业设备将与工业物联网服务平台建立连接:

- a) 非数字工业设备上选择并安装需要的传感器;
- b) 传感器与数字控制器连接;
- c) 软件上传到数字控制器,在这里软件负责面向工业物联网服务平台的传感器数据的收集、转换和传输;
- d) 数字控制器在平台提供的工业物联网服务上注册,且拥有唯一的标识符。而该服务响应非数字工业设备上的传感器收集到的数据;
- e) 运行一个测试程序来检测连接并且测量连接参数;
- f) 如果测试过程失败,重新配置系统连接并满足条件 a)~e);
- g) 如果测试程序成功,可开始常规的工业物联网系统工作流程。

9.2 通过工业物联网网关的连接

图 6 所示的模型描述了一种连接数字工业设备和工业物联网服务平台的方法。数字工业设备由安装在用户控制系统(如个人计算机、微型控制器、微型计算机等)上的程序控制。用户控制系统通过一个工业物联网网关和工业物联网服务平台连接。工业物联网网关收集来自这些程序的数据包,并且通过创建控制消息进行响应并将其转换为 IP 数据包格式。

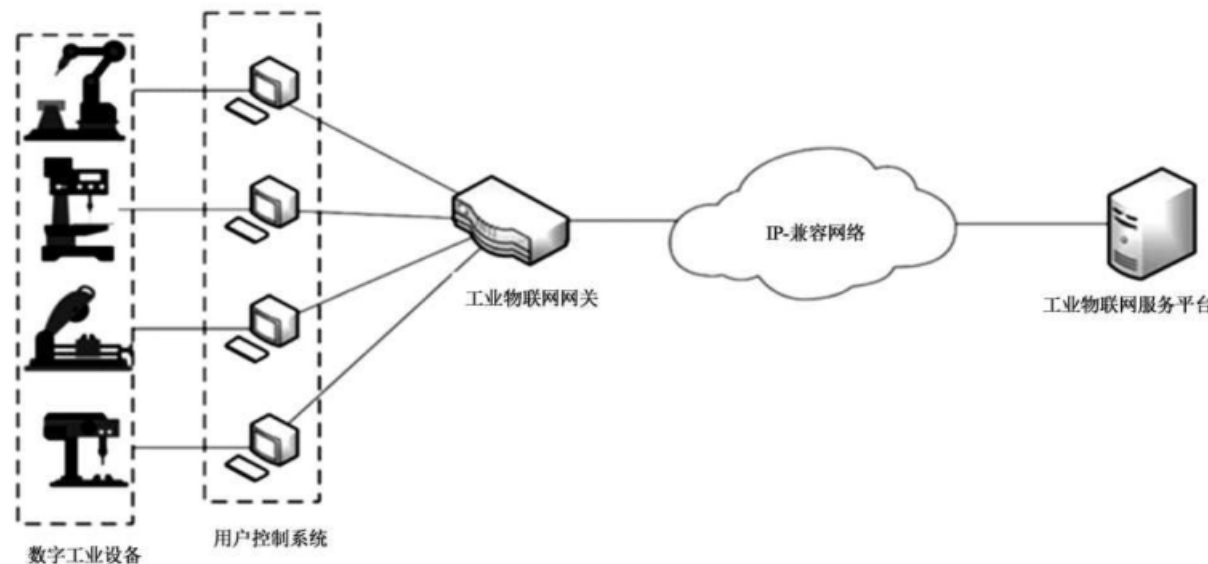


图 6 通过工业物联网网关连接

完成以下操作后,数字工业设备将与工业物联网服务平台建立连接:

- a) 数字工业设备需要和用户控制系统连接;

- b) 宜在每个和数字工业设备连接的用户控制系统上检验数字工业设备传感器数据收集功能系统；
- c) 在数据收集功能校验完毕之后,用户控制系统和工业物联网网关连接；
- d) 宜执行注册和连接测试程序；
- e) 如果测试失败,宜重新配置系统连接并满足条件 a)~d)；
- f) 如果测试成功完成,宜在工业物联网服务平台上向工业物联网服务注册工业物联网网关；
- g) 完成注册和连接测试程序之后,宜执行测试程序来检测连接,测量连接参数并确认工业物联网网关上的工业物联网协议转换；
- h) 如果测试失败,宜重新配置系统并满足条件 f)~g)；
- i) 如果测试成功完成,可开始常规的工业物联网系统工作流程。

9.3 通过工业控制系统的连接

图 7 所示的模型描述了连接收集和管理工业系统的方法,该系统负责将一组不同的工业设备管理至一个工业物联网服务平台。在这种情况下,数字工业设备通过连接特定的收集和管理工业系统。该系统通过连接到一个工业物联网网关的收集和管理工业系统上安装的特殊客户端应用程序与工业物联网服务平台连接。

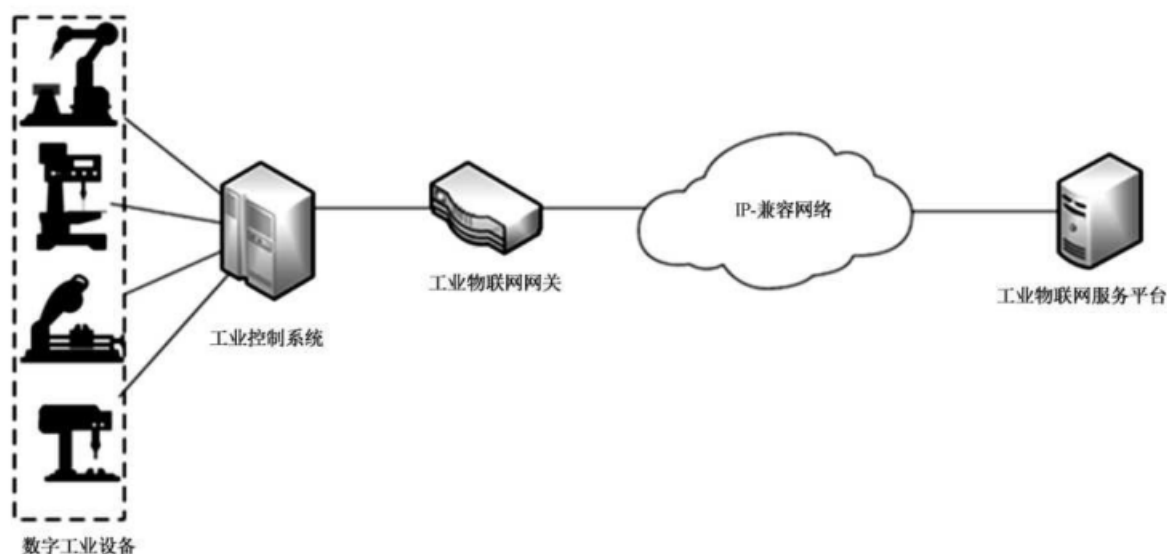


图 7 通过工业控制系统的连接

在完成了以下操作后,数字工业设备被视为通过收集和管理工业系统连接到了工业物联网系统设备。

- a) 首先,现场人员宜将数字工业设备与收集和管理工业系统相连接。随后,测试收集和管理工业系统的数据收集和管理程序。如果测试失败那么操作员宜重新配置连接。
- b) 收集和管理工业系统宜进行登记,并且与工业物联网网关连接。这样一个网关可将一个或多个收集和管理工业系统与工业物联网系统连接。
- c) 宜执行测试程序,以检测来自不同收集和管理工业系统的格式转换。
- d) 如果测试程序失败,宜重新配置系统并满足 a)~c)。
- e) 如果测试成功完成,宜在工业物联网服务平台注册工业物联网网关,并且每个数字工业设备(或其传感器)都宜在工业物联网服务平台上注册。

- f) 在上述操作之后,宜执行检测程序来检测连接,测量连接参数以及工业物联网网关上的工业物联网协议转换。
- g) 如果测试程序失败,宜重新配置系统并满足 e)~f)。
- h) 如果测试程序成功,宜开始常规的工业物联网系统工作流程。

附录 A

(资料性)

工业物联网设备和服务兼容性核查表

工业物联网系统的基本兼容性参数如表 A.1 所示。在此核查表的基础上,能通过手动模式和自动模式进行适当的测试,以验证兼容性。测试结果将表明工业物联网设备是否能正确地与相应的系统交互,如云服务、预测分析等。

表 A.1 工业物联网系统设备和服务兼容性核查表

兼容性			完全兼容	兼容	部分兼容	不兼容
功能兼容性要求	物理层	数据传输介质兼容性				
		数据传输/接收系统兼容性				
		电磁兼容性				
	媒体访问控制子层	媒体访问兼容性				
		框架兼容性				
		检测和调解数据传输冲突程序的兼容性				
	逻辑链路控制子层	网络拓扑的兼容性(包括交换过程)				
		网络帧生成和解释的兼容性				
		在已建立的通信信道上的数据传输控制程序的兼容性				
	网络层	路由兼容性				
		网络协议兼容性				
		标识符兼容性				
	传输层	多路传输/解多路传输兼容性				
		传输选项兼容性				
	会话层	会话传递和支持的兼容性				
		会话控制协议兼容性				
	表示层	数据编码/解码和压缩协议的兼容性				
		加密/解密协议兼容性				
	应用层	应用层协议和应用程序的兼容性				
		应用协议与网络套件的兼容性				
		应用程序协议兼容性				
	测量和自动化方面	与测量设备的交互协议兼容性				
	语义方面	会话理解和范围兼容性				
		消息格式解释方法的兼容性				
		数据解释方法的兼容性				

表 A.1 工业物联网系统设备和服务兼容性核查表 (续)

兼容性			完全兼容	兼容	部分兼容	不兼容
非 功 能 兼 容 性 要 求	版本兼容性定义	后向兼容性				
		前向兼容性				
	服务质量管理的兼容性	服务质量管理的兼容性				
	安全和隐私方面	安全策略的兼容性				
		通信和连接安全功能的兼容性				
		特定服务安全功能的兼容性				
		安全集成功能的兼容性				
		身份认证和授权功能的兼容性				
		安全审计功能的兼容性				
		加密手段的兼容性				
	合规性方面	国际兼容性				
		国家兼容性				
		行业兼容性				
	安全方面	工业系统安全措施				

附 录 B

(资料性)

不同工业物联网设备的负载测试场景

表 B.1~表 B.3 展示了异构工业物联网网关、边缘服务器和云服务器的负载测试场景。

表 B.1 基于现有网络的工业物联网边缘服务器运行测试

#	动作	描述	结果
“基于现有网络的工业物联网边缘服务器运行测试”方案			
1	连接和配置工业物联网边缘服务器(ES)	a) 边缘服务器通过网络接口连接到正在测试的网络	边缘服务器已准备就绪,可测试
		b) 边缘服务器需要配置相应的链路层协议和网络层协议	
		c) 检查边缘服务器对于联网设备的可访问性及响应时间	
		d) 所有支持的查询处理函数都经过验证	
		e) 测试CPU负载、RAM使用量和处理时间的应用程序通过边缘服务器本地网络接口在后台执行。此测试在没有传入请求的情况下执行	
2	连接和配置工业物联网(TG)	a) TG通过网络接口连接到被测网络	TG已准备就绪,可测试
		b) 根据链路层协议和网络层协议配置TG	
		c) 检查TG对于联网设备的可访问性及响应时间	
		d) 正在配置TG	
		e) 测试工业物联网TG。使用本地网络包分析器来确认TG的操作	
3	测试边缘服务器	a) 将TG生成的元数据格式与边缘服务器生成的元数据格式进行比较。如果比较的结果是不可接受的,生成器元数据的格式将更改为服务器接受的格式	边缘服务器在被测试网络中已准备就绪,可工作
		b) 在负载测试期间,通过TG中越来越多的虚拟设备(例如1,5,10,50,250,⋯,N个设备),对所有已测试功能执行一系列边缘服务器的处理时间、CPU负载和RAM负载的测量	
		c) 测试的结果用于为被测网络中的电子设备的运行提出建议	

边缘服务器(ES)是执行 ETSI GS MEC 001 中所定义的移动边缘平台功能的设备。

云服务器(CS)是执行第 7 章中所述的 IIoT 平台功能的设备。

表 B.2 基于现有网络测试边缘设备与工业物联网云服务器的交互

#	动作	描述	结果
“基于现有网络测试边缘服务器和工业物联网云服务器之间的交互”方案			
1	工业物联网 ES 连接和配置	a) ES连接因特网	ES已准备就绪,可测试
		b) 所有支持的查询处理函数都经过验证	

表 B.2 基于现有网络测试边缘设备与工业物联网云服务器的交互（续）

#	动作	描述	结果
1	工业物联网 ES 连接和配置	c) 后台应用程序在 ES 的本地网络接口上运行以测试 CPU 负载, RAM 使用量以及请求处理时间。在没有任何传入请求的情况下执行 ES 的测试	ES 已准备就绪, 可测试
2	工业物联网 CS 配置	a) CS 的配置是为了确保通过特殊的 CS 交互工具与 ES 进行交互 b) 所有支持的查询处理函数都经过验证	CS 已准备就绪, 可测试
3	ES 和 CS 的连接配置	a) 对 ES 和云服务器生成的元数据格式进行比较。当比较结果不能接受时, 边缘服务器元数据格式将更改为 CS 格式 b) ES 根据 CS 器设置的规则建立连接	ES 和 CS 已经准备好发送和接收请求
4	ES 和 CS 交互测试	a) 在负载测试期间, 将通过由 ES 上的特殊基准测试工具创建越来越多的虚拟设备对所有测试功能的执行处理时间(含网络时延), CPU 负载和 RAM 使用负载测量, 以及可达到的最大测试设备数和流量, 例如 1, 5, 10, 50, 250, …, N 个设备 b) 测试的结果用于为 ES 和 CS 的交互提供建议	ES 和 CS 已准备就绪, 可进行交互

表 B.3 基于现有网络的对于异构工业物联网网关的工业物联网应用协议转换测试

#	动作	描述	结果
“基于现有网络的对于异构工业物联网网关的工业物联网应用协议转换测试”方案			
1	连接和配置 HG	a) HG 通过网络接口连接到被测网络 b) HG 已针对链路层和网络层协议进行相应配置 c) 检查 HG 对于联网设备的可访问性 d) 使用 HG 的本地网络接口上运行的服务器和客户端应用程序检查协议转换。在检查期间, 将测量转换时间 e) 通过 HG 本地网络接口在后台执行用于测试 CPU 负载和 RAM 使用量的应用程序。无需负载即可进行测试	HG 已准备就绪, 可测试
2	在 HG 上配置工业物联网边缘服务器	a) ES 的测试应用程序正在配置 b) ES 在本地网络接口上启动 c) 检查以下基本功能: 工业物联网设备注册、数据接收和保存、数据读取 d) HG 与 ES 的运行应用程序的测试是通过使用 CPU 和 RAM 负载测量应用程序来执行的	边缘服务器已准备好接收网络数据包
3	连接和配置工业物联网 TG	a) TG 通过网络接口连接测试网络 b) TG 已针对链路层和网络层协议进行了相应配置 c) 检查 TG 对于联网设备的可访问性 d) 测试工业物联网 TG 已执行。本地网络数据包分析器用于确认 TG 的操作	TG 已准备就绪, 可使用

表 B.3 基于现有网络的对于异构工业物联网网关的工业物联网应用协议转换测试 (续)

#	动作	描述	结果
4	测试 TG 和 ES 之间的数据传输和接收	a) 针对由 TG 和 ES 组成的系统(使用 ES 支持的应用协议)测试网络数据包的接收和传输。网络数据包流是由一个虚拟设备针对 TG 支持的每种流量类型生成的	由 HG 和 EG 组成的系统已准备就绪,可接收和发送数据
5	在异构物联网网关上测试协议转换	a) 在 TG 上的虚拟设备(例如 1,5,10,50,250,⋯,N 个设备)越来越多的情况下,对 TG 应用程序协议支持的每个 HG 的处理时间、CPU 和 RAM 负载进行一系列测量	HG 已经准备好进行工业物联网应用协议的转换
		b) 在 5a) 中描述的一系列测量是通过一个虚拟 TG 设备为多个应用协议生成多个网络数据包来实现的	
6	测试 HG 和服务器的在被测试网络中的功能	a) 将 HG 生成的元数据格式与现有网络中的边缘服务器和/或云服务器生成的元数据格式进行比较。如果比较的结果是不可接受的,HG 元数据的格式将更改为服务器可接受的格式	HG 在被测试网络中已准备就绪,可开始工作
		b) HG 的应用协议的转换正在测试中	
		c) 测试结果用于为测试网络中的 HG 操作提出建议	

表 B.4 显示了测试表的格式,根据表 B.1~表 B.3 中所述的情况,能用于测量设备的各种参数。表 B.5 中给出了填写此表的示例。

表 B.4 负载测试方案的测试表格式

测试场景: _____									
测试设备: _____									
使用设备: _____									
DUT 参数: _____									
置信概率: _____%									
测试时间: _____									
#	测试用例	虚拟测试设备的数量	平均数据包到达率 s	到达数据包抖动 s	DUT	CPU 负载 %	RAM 负载 %	平均处理时间 s	数据包丢失率 %
1		_____	_____ ± _____	_____	_____	_____	_____	_____ ± _____	_____
	...								
	...								
	...								
	...								
	...								
N		_____	_____ ± _____	_____	_____	_____	_____	_____ ± _____	_____

表 B.5 测试表填写示例

测试场景：现有网络的边缘和云服务器负载测试									
测试设备：边缘服务器、云服务器									
使用设备：流量（查询）生成器、以太网交换机、以太网路由器									
DUT 参数：边缘服务器——dual 2,0 GHz ARM core, 4 Gb RAM; 云服务器——quad 3,2 GHz x86_64 core, 16 Gb RAM									
置信概率：95%									
测试时间：30 s									
#	测试用例	虚拟测试设备的数量	平均数据包到达率 s	到达数据包抖动 s	DUT	CPU 负载 %	RAM 负载 %	平均处理时间 s	数据包丢失率 %
1	—	0	—	—	边缘服务器	12	11	—	—
					云服务器	25	30	—	—
2	发送数据查询	1	0.177±0.032	0.144	边缘服务器	12	11	0.002 3±0.000 4	0
					云服务器	25	31	0.001 0±0.000 1	0
3		10	0.017±0.001	0.004	边缘服务器	13	15	0.002 6±0.000 5	0
					云服务器	25	31	0.001 1±0.000 1	0
.....									
n	请求数据查询	1	0.133±0.004	0.029	边缘服务器	11	11	0.002 4±0.000 3	0
					云服务器	24	30	0.001 2±0.000 1	0
.....									
n+m	发送统计查询	500	0.003 7±0.000 4	0.001	云服务器	35	57	0.002 9±0.000 4	0
.....									

附录 C
(资料性)

通信网络中工业物联网基础网络设施连接架构

C.1 概述

图 C.1 展示了通信网络中工业物联网基础网络设施的连接架构。

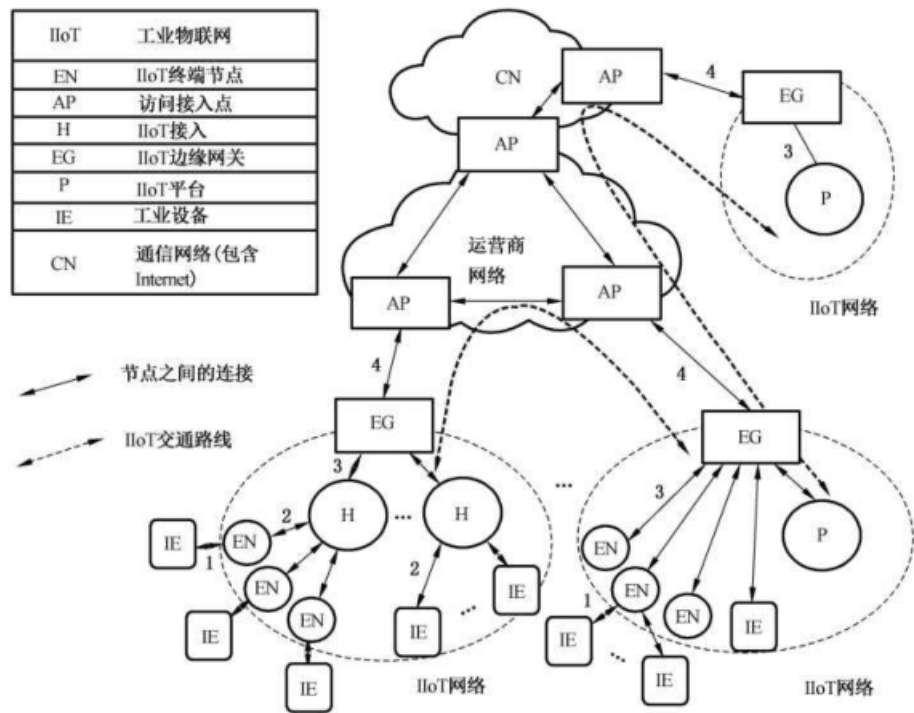


图 C.1 通讯网络中工业物联网基础网络设施的连接架构

图 C.1 所示的连接结构中包含以下组成节点：

- 工业设备(IE)：在工业企业中使用的设备；
- 工业物联网终端节点(EN)：负责使 IE 和整个企业工作自动化的计算设备；
- 工业物联网接入(H)：负责将 IE 接入到企业网络的设备；
- 工业物联网平台(P)：在本文件第 7 章中所描述的设备；
- 工业物联网边缘网关(EG)：在本文件第 7 章中被称作“边缘网关”的设备；
- 访问接入点(AP)：提供外部网络访问服务的设备。

图 C.1 中所描绘的结构同时展示了等级 1 到等级 4 的连接等级。为了在典型的企业控制系统中描述这些设备，本附录将适当改编 IEC 62264(所有部分)中所描述的对应该模型和各层次职能。IEC 62264 中第 1 部分到第 6 部分对企业控制系统集成给出了详细描述，同时这些部分也描绘了企业控制系统中的模型和功能性层次。这些层次(第 0 层到第 4 层)，以及每个层次的具体职能在图 C.2 中给出了进一步的适当改编和详述。

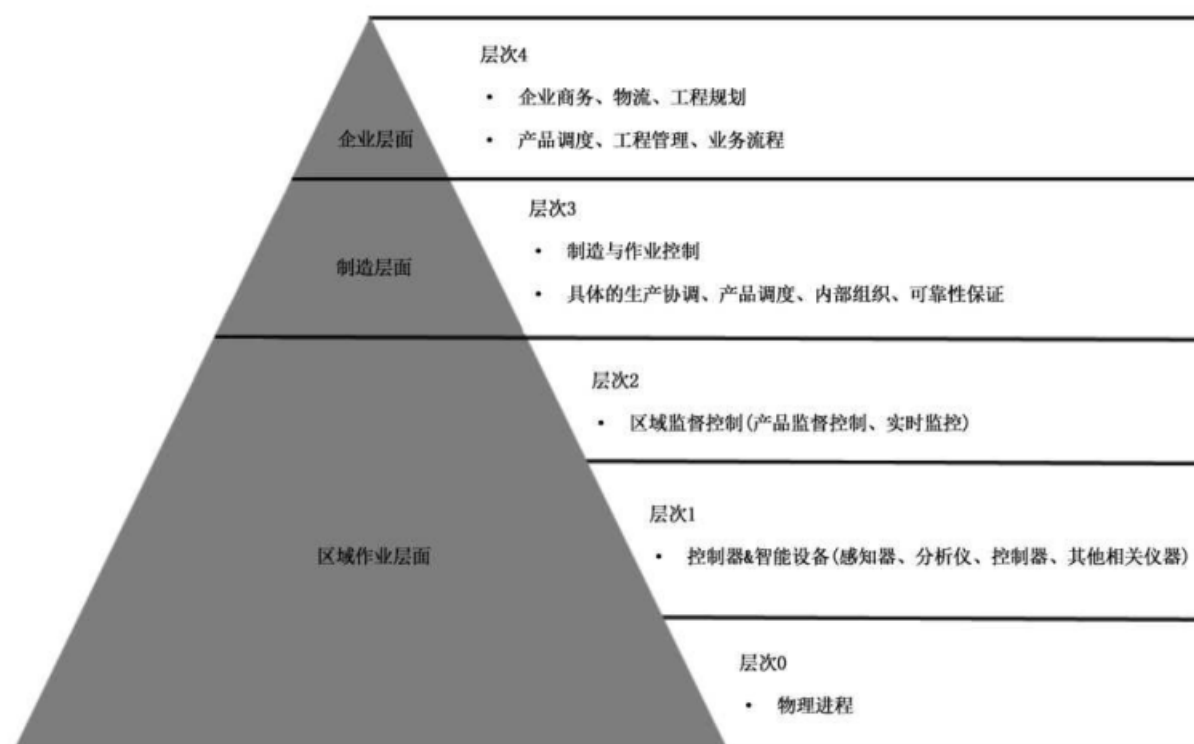


图 C.2 传统的普渡模型

IEC 62264(所有部分)中的这五个等级以及它们的具体职能总结如下。

- 层次 0:物理进程(Physical Process)。该层次定义了实际的物理进程。
- 层次 1:智能设备(Intelligent Devices)。该层次包含那些感知和操作物理进程的进程控制设备。这些设备包括进程传感器、分析仪、执行器以及其他相关仪器。
- 层次 2:控制系统(Control Systems)。该层次对控制系统进行了封装,并提供了对控制器的监督控制和监测。该层次包含监督控制和数据获取(SCADA)软件、人机接口(HMI)设备、警报系统以及控制室工作站,所有层次 2 中的设备均可与层次 1 中的系统进行交互。
- 层次 3:制造与操作系统(manufacturing and operating systems)。该层次的设备管理控制装置的运行,包括应用程序、服务程序和系统,如数据历史、可靠性保证、生产调度与反馈、工程工作站和远程访问服务等。这些系统通过一片“隔离区(demilitarized zone)”与层次 4 进行交互,该隔离区是一个介于工业网和企业网络之间的子网,为受信任的网络提供一个附加的安全层。
- 层次 4:商业物流系统(Business and Logistics Systems)。该层次应用于企业层面,覆盖商业物理系统,有时也被视为组织的 IT 端。该层次包含反馈、调度、库存管理、容量规划、运营和维护管理,以及电子邮件和电话业务。

虽然 IEC 62264(所有部分)并未对交互网络模型以及连接等级做出特别描述,IEC 62264(所有部分)所描述的企业控制系统网络中的各个功能性层次能与本文档描述的交互网络模型的连接等级进行映射。为了更好地描述映射关系,图 C.1 中的各个节点实体(工业物联网、EN、AP 等)将与 IEC 62264(所有部分)中的各个功能性层次进行关联。表 C.1 详细描述了这种关联。

表 C.1 图 C.1 中的网络与节点实体向 IEC 62264(所有部分)各功能性层次的映射关系

IEC62264 功能性层次	图 C.1	
	实体	网络
层次 4	P,AP	CN
层次 3	IE,P,AP	运营商网络,CN
层次 2	AP,IE,P	运营商网络,CN
层次 1	EN,IE,EG,H	工业物联网网络,CN
层次 0	工业物联网(物理实体域下的真实进程)	工业物联网网络,CN

五个功能性层次之间的连接可能被分配对应的连接等级,由于 IEC 62264(所有部分)的模型与本文档描述的模型有所不同,IEC 62264(所有部分)的功能性层次与网络连接等级之间的映射仅有可能是一种近似映射。表 C.2 给出了这种近似映射的关系。

表 C.2 网络连接等级到 IEC 62264(所有部分)的映射

IEC 62264(所有部分)功能性层次	网络连接等级
层次 0 与层次 1 之间	等级 1
层次 1 与层次 2 之间	等级 2 和/或等级 3
层次 2 与层次 3 之间	等级 3 和/或等级 4
层次 3 与层次 4 之间	等级 3 和等级 4

在图 C.1 中,连接等级表明哪些技术能用来确保两个对应的系统节点之间的连接。这四个连接等级已经在图中依托系统实体与网络以图像的形式作出了描述。下面给出每一层次能用于节点连接的技术示例。

C.2 连接等级 1

IE 与 EN 节点之间的连接。能用于该类型连接的部分技术如下:

- GPIO 接口;
- RS-232 接口;
- RS-485 接口;
- RS-422 接口
- SPI 接口;
- I2C 接口;
- CAN 协议;
- Modbus ASCII/RTU 协议;
- HART 协议等。

注:还包括以下协议或接口:如 RS-422 接口、Modbus ASCII/RTU 协议、CANopen 协议、AUTBUS 协议、EtherCAT 协议、Ethernet/IP 协议、Profinet 协议、IEC 101/102/103/104 协议、DL/T 645 协议、S7-200/S7-300/S7-1200/S7-1500 协议、DNP 协议等。

C.3 连接等级 2

IE/EN 与 H 节点之间的连接。能用于该类型连接的部分技术如下：

- Ethernet 接口——ISO/IEC/IEEE 8802-3；
- WiFi 接口——ISO/IEC/IEEE 8802-11；
- ZigBee/6LoWPAN 接口——ISO/IEC/IEEE 8802-15-4；
- LoRaWAN¹⁾/Sigfox 接口——ISO/IEC/IEEE 8802-15-4；
- eMTC 接口—LTE Cat M1；
- NB-IoT 接口—LTE-M NB1；
- RS-232 接口；
- RS-485 接口；
- SPI 接口；
- I2C 接口；
- DASH7 接口；
- Ingenu 接口；
- CAN 协议；
- Modbus ASCII/RTU/TCP 协议；
- HART/WirelessHART 协议；
- CoAP 协议；
- MQTT 协议；
- OPC UA 协议；
- HTTP restful 协议；
- AMQP 协议；
- XMPP 协议；
- DDS-RTSP 协议等。

注：还包括以下协议和接口，如 RS-422 接口、CANopen 协议、AUTBUS 协议、EtherCAT 协议、Ethernet/IP 协议、Profinet 协议、IEC 101/102/103/104 协议、DL/T645 协议、S7-200/S7-300/S7-1200/S7-1500 协议、DNP 协议等。

C.4 连接等级 3

IE/EN/H/P 与 EG 节点之间的连接。能用于该类型连接的部分技术如下：

- Ethernet 接口；
- ZigBee 接口；
- eMTC 接口；
- LoRaWAN 接口²⁾；
- Sigfox 接口；
- DECT-2020 NR；
- 5G/IMT-2020
- NB-IoT 接口；
- NB-Fi 接口；
- Open-UNB 接口；

1) 在俄罗斯联邦,使用 LoRaWAN RU 规范。

2) 具体应用技术取决于各个国家的规章制度。

- TS-UNB 接口；
- Wi-Sun 接口；
- SNBWAN 接口；
- DASH7 接口；
- Ingenu 接口；
- ModBus TCP 协议；
- WirelessHART 协议；
- CoAP 协议；
- MQTT 协议；
- OPC UA 协议；
- HTTP restful 协议；
- AMQP 协议；
- XMPP 协议；
- DDS-RTSP 协议等。

C.5 连接等级 4

EG 与 AP 节点之间的连接。能用于该类型连接的部分技术如下：

- Ethernet 接口——ISO/IEC/IEEE 8802-3(包括百兆、千兆、万兆接口等)；
- PON 接口(包括 EPON、GPON、XEPON、XGSPON、50GPON 等)；
- GPRS 接口；
- UMTS 接口；
- eMTC 接口；
- LoRaWAN 接口；
- Sigfox 接口；
- NB-IoT 接口；
- NB-Fi 接口；
- Open-UNB 接口；
- TS-UNB 接口；
- Wi-Sun 接口；
- SNBWAN 接口；
- VSAT 接口；
- DASH7 接口；
- Ingenu 接口；
- DVB-T2 接口等。

示例：

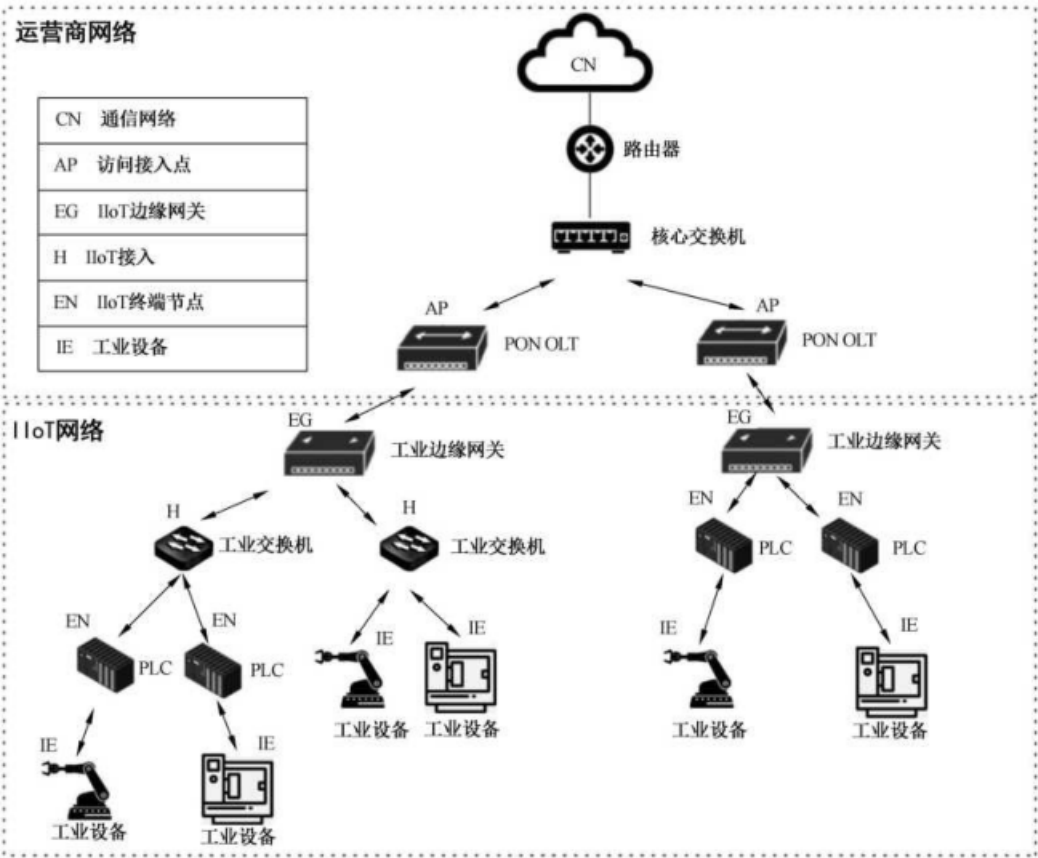


图 C.1 的应用示例见图 C.3,各节点连接的部分技术如下：

- 交换机与 PON OLT(50G PON OLT/10G PON OLT)之间可采用以太网协议；
- PON OLT(50G PON OLT/10G PON OLT)与工业网关之间可采用 50G PON 协议、10G PON 协议；
- 工业边缘网关与以太网交换机之间可采用以太网协议；
- 工业边缘网关与 PLC 之间可采用 S7-200/S7-300/S7-1200/S7-1500 等协议；
- 以太网交换机与 PLC 之间可采用 S7-200/S7-300/S7-1200/S7-1500 等协议；
- 工业交换机与 IE 之间可采用 Profinet/EtherCAT 等协议。

附录 NA

(资料性)

本文件的相关缩略语

下面列出了本文件所使用的相关缩略语,以便于对本文件的理解。

AMQP:高级消息队列协议(Advanced Message Queuing Protocol)
CAN:控制器区域网络(Controller Area Network)
CD:控制设备(Controlling Device)
CoAP:约束应用协议(Constrained Application Protocol)
CPU:中央处理器(Central Processing Unit)
CS:云服务器(Cloud Server)
CSMA/CA:带有冲突避免的载波侦听多路访问(Carrier Sense Multiple Access with Collision Avoid)
DDS-RTSP:数据分发服务实时串流传输协议(Data Distribution Service RealTime Streaming Protocol)
DTDMA:分布式时分多址(Distributed Time-Division Multiple-Access)
DUT:待测试的设计(Design Under Test)
eMTC:增强机器类通信(enhanced Machine-Type Communication)
ES:边缘服务器(Edge Server)
EUI:扩展唯一标识符(Extended Unique Identifier)
HG:异构工业物联网网关(Heterogeneous IIoT Gateway)
ICMP:因特网控制报文协议(Internet Control Message Protocol)
IIOT:工业物联网(Industrial Internet of Things)
IP:网际互联协议(Internet Protocol)
IPv4:网际互联协议版本 4(Internet Protocol version 4)
IPv6:网际互联协议版本 6(Internet Protocol version 6)
MAC:媒体访问控制(Media Access Control)
MD:测量设备(Measuring Device)
MQTT:消息队列遥测传输(Message Queuing Telemetry Transport)
NB-IoT:窄带物联网(Narrow Band Internet of Things)
OPC UA:OPC 统一架构(OPC Unified Architecture)
OSI:开放系统互连(Open System Interconnect)
PSTN:公共电话交换网络(Public Switched Telephone Network)
QoS:服务质量(Quality of Service)
RAM:随机存取存储器(Random Access Memory)
SCP:会话控制协议(Session Control Protocol)
SCTP:流控制传输协议(Stream Control Transmission Protocol)
SPI:串行外设接口(Serial Peripheral Interface)
TCP:传输控制协议(Transmission Control Protocol)
TG:流量生成(Traffic Generator)
UDP:用户数据报协议(User Datagram Protocol)

VPN:虚拟专用网络(Virtual Private Network)

XMPP:可扩展消息处理现场协议(the eXtensible Messaging and Presence Protocol)

6LoWPAN:低功耗无线个域网上的IPv6(IPv6 over Low power Wireless Personal Area Networks)

参 考 文 献

- [1] DL/T 645—2007 多功能电能表通信协议
- [2] ISO/IEC 7498-1 Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model
- [3] ISO/IEC 25010:2023 Systems and software engineering—Systems and software Quality Requirements and Evaluation (SQuaRE)—Product quality model
- [4] ISO/IEC 27000 Information technology—Security techniques—Information security management systems—Overview and vocabulary
- [5] ISO/IEC 27001 Information security, cybersecurity and privacy protection—Information security management systems—Requirements
- [6] ISO/IEC 27002 Information security, cybersecurity and privacy protection—Information security controls
- [7] ISO/IEC 27003 Information technology—Security techniques—Information security management systems—Guidance
- [8] ISO/IEC 27004 Information technology—Security techniques—Information security management—Monitoring, measurement, analysis and evaluation
- [9] ISO/IEC 27005 Information security, cybersecurity and privacy protection—Guidance on managing information security risks
- [10] ISO/IEC 27006 Information security, cybersecurity and privacy protection—Guidance on managing information security risks
- [11] ISO/IEC 27007 Information security, cybersecurity and privacy protection—Guidelines for information security management systems auditing
- [12] ISO/IEC TS 27008 Information technology—Security techniques—Guidelines for the assessment of information security controls
- [13] ISO/IEC/IEEE 8802-1AC Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Part 1AC: Media access control (MAC) service definition
- [14] ISO/IEC/IEEE 8802-1q Telecommunications and exchange between information technology systems—Requirements for local and metropolitan area networks—Part 1Q: Bridges and bridged networks
- [15] ISO/IEC 8802-2:1998 Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical link control
- [16] ISO/IEC/IEEE 8802-3 Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 3: Standard for Ethernet
- [17] ISO/IEC/IEEE 8802-11 Telecommunications and information exchange between systems—Specific requirements for local and metropolitan area networks—Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications
- [18] ISO/IEC/IEEE 8802-15-4 Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 15-4:

Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs)

- [19] ISO/IEC 30141 Internet of Things(IoT)—Reference architecture
- [20] ISO/IEC/IEEE 9945 Information technology—Portable Operating System Interface (POSIX_e) Base Specifications, Issue 7
- [21] ISO/IEC/IEEE 24765 Systems and software engineering—Vocabulary (Second Edition)
- [22] IEC 61000(all parts) Electromagnetic compatibility (EMC)
- [23] IEC 61000-1-2:2016 Electromagnetic compatibility (EMC)—Part 1-2: General—Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena
- [24] IEC 61508(all parts) Functional safety of electrical/electronic/programmable electronic safety-related systems
- [25] IEC 62264 (all parts) Enterprise-control system integration
- [26] IEC 62368-1:2023 Audio/video, information and communication technology equipment—Part 1: Safety requirements
- [27] IEC 62541 (all parts) OPC unified architecture
- [28] IEC TR 63069:2019 Industrial-process measurement, control and automation—Framework for functional safety and security
- [29] Rec.ITU-T Y.4000 Overview of the Internet of things
- [30] Rec.ITU-T Y.4003 Overview of smart manufacturing in the context of the industrial Internet of things
- [31] Rec.ITU-T Y.4101/Y.2067 Common requirements and capabilities of a gateway for internet of Things applications
- [32] Rec.ITU-T Y.4111/Y.2076 Semantics based requirements and framework of the Internet of things
- [33] Rec.ITU-T Y.4113 Requirements of the network for the Internet of Things
- [34] Rec.ITU-T Y.4806 Security capabilities supporting safety of the Internet of things
- [35] Rec.ITU-T X.224 Information technology—Open Systems Interconnection—Protocol for providing the connection-mode transport service
- [36] Rec.ITU-T X.225 Information—Open Systems Interconnection—Connection-oriented Session protocol: Protocol specification
- [37] Rec.ITU-T X.234 Information Technology—Protocol for providing the OSI connectionless-mode
- [38] Rec.ITU-T X.1362 Simple encryption procedure for Internet of things (IoT) environments
- [39] Rec.ITU-T G.1010 End-user multimedia Qos categories
- [40] Rec.ITU-T H.810 Interoperability design guidelines for personal connected health systems; Introduction
- [41] Rec.ITU-T H.811 Interoperability design guidelines for personal connected health systems; Personal Health Devices interface
- [42] IETF RFC 791 Internet Protocol
- [43] IETF RFC 1122 Requirements for Internet Hosts—Communication Layers
- [44] IETF RFC 2341 Cisco Layer Two Forwarding (Protocol)"L2F"

- [45] IETF RFC 2637 Point-to-Point Tunneling Protocol (PPTP)
 - [46] IETF RFC 2661 Layer Two Tunneling Protocol "L2TP"
 - [47] IETF RFC 4506 XDR: External Data Representation Standard
 - [48] IETF RFC 4594 Configuration Guidelines for DiffServ Service Classes
 - [49] IETF RFC 7303 XML Media Types
 - [50] ETSI GS MEC 001 Multi-access Edge Computing(MEC);Terminology
 - [51] "Design and Build Productive and Secure Industrial Systems" Kenneth Crowther and Robert M. Lee, December 2018, <https://www.iiotconnection.com/a-grim-gap-cybersecurity-of-level-1-field-devices>
-

