PD ISO/IEC TR 30166:2020

BSI Standards Publication

Internet of things (IoT) — Industrial IoT

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020

National foreword

This Published Document is the UK implementation of ISO/IEC TR 30166:2020.

The UK participation in its preparation was entrusted to Technical Committee IOT/1, Internet of Things.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2020
Published by BSI Standards Limited 2020

ISBN 978 0 539 13786 6

ICS 35.240.50; 35.020; 25.040.40

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 May 2020.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020

ISO/IEC TR 30166

Edition 1.0 2020-04

TECHNICAL REPORT

colour inside

Internet of things (IoT) – Industrial IoT

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25-040-40; 35.020; 35.240.50

ISBN 978-2-8322-8251-9

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

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020

CONTENTS

FOREWORD 6
INTRODUCTION 7
1 Scope 10
2 Normative references 10
3 Terms and definitions 10
4 Abbreviated terms 10
5 IIoT systems and landscape, see [1] 12
5.1 Overview 12
5.1.1 General 12
5.1.2 Architecture 15
5.1.3 Implementation of IIoT systems 15
5.1.4 IIoT use case implementations 16
5.1.5 Edge (fog) computing in IIoT, see [2] 16
5.1.6 Interoperability and conformance 16
5.1.7 IIoT characteristics trustworthiness 17
5.1.8 Wearables in IIoT 18
5.1.9 Cross-cutting activities on IIoT 18
5.2 Analysis consideration on IIoT landscape of systems 19
5.2.1 General 19
5.2.2 IIoT systems and architecture 19
5.2.3 IIoT application (virtual/physical use case) 22
5.2.4 IIoT connectivity 23
5.2.5 IIoT interoperability focus 23
5.2.6 The IIoT user, see [20] 23
5.2.7 IIoT migration strategies, see [29] 24
5.3 General definition of IIoT and smart manufacturing (SM) 25
5.3.1 Definition of IIoT 25
5.3.2 Cyber physical systems differentiation in the IIoT 26
5.3.3 Industrial Internet to CPPS and CPS definition 26
5.3.4 Smart Manufacturing differentiation vs. IIoT 26
5.3.5 Verticals of IoT market 26
5.4 Smart Manufacturing and IIoT 28
5.4.1 General 28
5.4.2 The IIoT high-level view 28
5.4.3 Industrial products/services life cycle – in IIoT/Smart Manufacturing 30
5.4.4 Industrial manufacturing/automation through (IT/OT) standardization – CPPS 30
5.5 Collaboration considerations on an IIoT reference architecture for standardization (use case driven) 31
5.5.1 General 31
5.5.2 General comparison of RAs and models on IIoT, see [37] 31
5.5.3 IIoT systems characteristics: connectivity and communication aspects 31
5.5.4 IIoT semantic aspects: IIoT characteristics 32
5.5.5 Data scale in IIoT 37
5.5.6 Runtime integration of IIoT 37
5.5.7 Edge computing in IIoT 37
5.5.8 The endpoint – considerations on IIoT 37

AVA Documents
Document Sharing Hub

5.5.9 "Dependability" for IIoT systems (IEC TC 56) ... 38
6 Considerations for future standardization of IIoT ... 38
6.1 Main findings by this document on IIoT standardization ... 38
6.2 Risk for standards development on IIoT ... 39
6.2.1 General ... 39
6.2.2 Avoiding work duplication on IIoT standards development – across SDOs ... 39
6.2.3 Important to IIoT: "semantics above syntax", see [55] ... 39
6.2.4 Standards for handling the "ownership of data" in IIoT, see [56] ... 39
6.2.5 Vocabulary definitions – issues to IIoT ... 40
6.3 Perspective to development of standards for IIoT ... 40
6.3.1 "Digital twins" – as a generic concept in IIoT ... 40
6.3.2 (AI) Artificial Intelligence to be used by IIoT (ISO/IEC JTC 1/SC 42) ... 41
6.3.3 Federation of cloud in/between IIoT systems (DIN SPEC 92222) ... 42
6.3.4 Future standardization on: "microservices and micro-applications in IIoT" see [40] ... 42
6.3.5 "Blockchain technology" – future standardization in IIoT ... 42
6.3.6 "Wearables" (in IIoT) ... 43
6.3.7 Compatibility requirements and model – for devices – within IIoT systems ... 43
6.4 Roadmap perspective analysis for future standardization work for IIoT ... 45
6.4.1 Future standardization work for IIoT as a vertical domain of the IoT ... 45
6.4.2 ISO/IEC collaboration in relation to IIoT ... 47
Annex A (informative) Listing of all SDOs, non-SDOs, consortia, FOSS (free open source systems) in context of the IIoT mentioned in this document ... 50
A.1 SDOs recognized/identified as of interest to IIoT and also in relation to Clause 5 on standardization landscape in IIoT ... 50
A.1.1 General ... 50
A.1.2 3GPP 3rd Generation Partnership Project ... 50
A.1.3 ETSI (European Telecommunication Standards Institute) ... 51
A.1.4 IEEE (Institute of Electrical and Electronics Engineers) ... 51
A.1.5 ISO/IEC ... 52
A.2 IIoT related initiatives/engagements by national standardization bodies ... 61
A.2.1 General ... 61
A.2.2 Sweden – LISA ... 61
A.2.3 France – "Usine du Futur", see [67] ... 62
A.2.4 Germany – Industrie 4.0, see [68] ... 63
A.2.5 Korea – "Korea – Manufacturing Industry Innovation 3.0 strategy", ... 63
A.2.6 China – Industrial Initiatives (Standards Development) ... 64
A.2.7 Japan (RRI and IVI) ... 65
A.2.8 USA – CPS/CPPS/IIoT Standards Initiatives ... 67
A.2.9 IIoT activities by EC EU ... 69
A.3 Industrial consortia recognized/identified as being of interest on working about the IIoT ... 69
A.3.1 General ... 69
A.3.2 Alliance of Industrial Internet: "Chinese Model of Smart Manufacturing in context of program China Manufacturing 2025" [70] ... 70
A.3.3 5G-ACIA in IIoT, and Smart Manufacturing ... 70
A.3.4 China Edge Computing Consortium ECC ... 71
A.3.5 DMG (Data Mining Group) ... 71

AVA Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 30166:2020

A.3.6 eCl@ss ... 71
A.3.7 IIC (Industrial Internet Consortium) ... 73
A.3.8 International Data Spaces ... 73
A.3.9 Industrial Value Chain Initiative (IVI) ... 73
A.3.10 ISA (International Society of Automation) ... 74
A.3.11 oneM2M – also linked to ETSI above ... 74
A.3.12 OPC Foundation ... 74
A.3.13 Automation ML ... 75
A.3.14 OMAC (Organization for Machine Automation and Control), see [71] ... 75
A.3.15 IIoT Semantic: WiSE-IoT (Worldwide interoperability for semantics IoT), see [72] ... 75
A.4 RFC-based standards development recognized as being of interest to IIoT ... 76
A.4.1 General ... 76
A.4.2 IETF/IRTF on IT Section related standards development also in IIoT ... 76
A.4.3 OASIS – Organization for the Advancement of Structured Information Standards ... 77
A.4.4 OCF (Open Connectivity Foundation) ... 77
A.4.5 ODVA – Open DeviceNet Vendors Association ... 78
A.4.6 OGC (Open Geospatial Consortium) ... 78
A.4.7 OMG (Object Management Group) ... 79
A.4.8 OpenFog Consortium – former, now part of IIC ... 80
A.4.9 The Open Group ... 80
A.4.10 Project Haystack – IIoT Semantic ... 81
A.4.11 W3C – World Wide Web Consortium ... 81
A.5 Consortial work on standardization by reference ... 82
A.5.1 General ... 82
A.5.2 IIRA (by IIC) ... 82
A.5.3 Bluetooth SIG ... 83
A.5.4 IO-Link – on Wireless Industrial RealTime Communication ... 83
Bibliography ... 85

Figure 1 – Six typical features of IIoT ... 8
Figure 2 – IIoT mapping landscape description for SDO and non-SDO, consortia, FOSS ... 14
Figure 3 – Trustworthiness functional components as identified in ISO/IEC 30141:2018 ... 18
Figure 4 – Migration approach towards IIoT systems ... 25
Figure 5 – IoT SDOs and alliances landscape (vertical and horizontal domains) ... 27
Figure 6 – Layout of the overall view on IIoT in the SC 41 context – the IoT bird's eye view in ISO/IEC JTC 1/SC 41, see [34]. ... 29
Figure 7 – Diagram showing that the IIoT is part of the IoT applications domain (bird's eye view), see [35] ... 30
Figure 8 – IIoT connectivity stack from IICF, see [38] ... 32
Figure 9 – The semiotic triangle ... 33
Figure 10 – Semantics in IIoT meaning context, i.e. sensing ... 36
Figure A.1 – Structure of IEC TC 65 and ISO/TC 184 JWG 21 ... 58
Figure A.2 – ISO/IEC Taskforce Standards Map Smart Manufacturing ... 59
Figure A.3 – KOSF logo ... 64
Figure A.4 – Link reference on Chinese GB/T standards vs. OPC/UA ... 65

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 30166:2020

Figure A.5 – Robot Revolution & Industrial IoT Initiative 66
Figure A.6 – RRI and cooperative relationship 66
Figure A.7 – Industrial Value Chain Initiative (IVI) 67
Figure A.8 – NIST logo 68
Figure A.9 – eCl@ss in Context to other SDO's and institutions 72
Figure A.10 – Activities in the BIM domain: 72
Figure A.11 – Overview of the W3C WoT Building Blocks 82

Table A.1 – List of protocol for IIoT / SM use case by NC China 64

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020

INTERNET OF THINGS (IoT) – INDUSTRIAL IoT

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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 National Committees and ISO member bodies.

3) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC National Committees and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or 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 National Committees and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC, ISO or ISO/IEC publication and the corresponding national or regional publication should 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 marks of conformity. IEC or 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 publication.

7) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC National Committees or ISO member 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 of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.

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

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

The main task of IEC and ISO technical committees is to prepare International Standards. However, a technical committee may propose the publication of a Technical Report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

ISO/IEC TR 30166, which is a Technical Report, has been prepared by subcommittee 41: Internet of Things and related technologies, of ISO/IEC joint technical committee 1: Information technology.

The text of this Technical Report is based on the following documents:

Enquiry draft	Report on voting
JTC1-SC41/95/DTR	JTC1-SC41/113/RVDTR

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

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

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

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020

INTRODUCTION

The IIoT (Industrial Internet of Things) is an identified vertical of the IoT, as seen throughout this document in general.

It consists of Industrial (electronic) communication-capable electronic systems and devices, which can be recognized as the integration base, to allow seamless communication, data processing, data access and data exchange in regard to sensors (sensing), auto-ID (automatic (global, unique) identification), and actors (acting, steering).

This is connected based upon a homogeneous as well as heterogeneous – mostly, but not exclusively, IP based – networking structure, capable of being able to interact seamlessly, in a flat, mesh or hierarchical architecture.

This document is intended for those users who want to get a large-scale informative overview of the current standardization activities and standardization landscape of SDOs, consortia and open-source communities in the field of IIoT.

Therefore, it is primarily intended for standardization managers, system architects, OT and IT specialists with a substantial understanding of technical language in the context of discrete manufacturing and/or process industries and with a focus on future global advanced smart industries.

It lists also national and cooperative initiatives in regard to IIoT and the partly touching field of Smart Manufacturing – with at least distinct working activities on IIoT in terms of their capabilities and individual working scope. It also lists the identified ones in Annex A.

First of all, a definition is used based upon work by CESI in the whitepaper on IIoT from the China NC in 2017:

> "IIoT is a new industrial ecosystem of service driven built based on the network interconnection, data interoperability and system interoperability of industrial resources, to realize the flexible configuration of the manufacturing materials, the on-demand execution of the manufacturing process, the rational optimization of the manufacturing process and the rapid adaptation of the manufacturing environment, and to achieve the efficient utilization of the resources.
>
> IIoT shows six typical features: intelligent perception, ubiquitous connectivity, precise control, digital modelling, real-time analysis and iterative optimization. (See Figure 1.)
>
> Intelligent perception. It is the base of IIoT. The massive data generated from industrial production, logistics, sales and other industrial chain links are the information data of different dimensions in the industrial life cycle obtained by IIoT in such perceptual means as the sensor and RFID, including: State information about industrial resources, such as personnel, machines, raw materials, processes and environment.
>
> Ubiquitous connectivity. It is the precondition of IIoT. Industrial resources are connected or linked to the Internet through wired or wireless ways, forming a convenient and efficient information channel for IIoT and realizing interconnection and intercommunication of industrial resource data, and the breadth and depth of the connection between machines and machines, machines and people, machines and the environment are expanded.
>
> Digital modelling. It is the method of IIoT. Digital modelling maps industrial resources into digital space, and simulates industrial production processes in a virtual world, which can realize the abstract modelling of all elements in industrial production process by virtue of the powerful information processing ability in digital space and provide effective decision-making for the operation of industrial chain of IIoT entities.

AVA Documents
Document Sharing Hub

Real-time analysis. It is the means of IIoT. The perceived industrial resource data can be processed in real time in in digital space by means of technical analysis, to obtain the internal relationship between the state of industrial resources in the virtual and the real space; in addition, the abstract data can be further visualized to complete the real-time response of external physical entities.

Precise control. It is the purpose of IIoT. Through the processes of state perception, information interconnection, digital modelling, real-time analysis, etc. of industrial resources, the precise control can be converted into the control commands that the industrial resource entities can understand based on the decision formed in virtual space, and then practical operation shall be conducted to achieve precise information interaction and seamless collaboration of industrial resources.

Iterative optimization. It is the effect of IIoT. IIoT system can learn and upgrade itself continuously. It can form effective and inheritable knowledge base, model base and resource base by processing, analyzing and storing industrial resource data. It can iterate and optimize till the optimal goal facing industrial resource manufacturing raw materials, manufacturing processes, manufacturing processes and manufacturing environment."

SOURCE: CESI

Figure 1 – Six typical features of IIoT

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 30166:2020

IoT is causing dramatic technological changes to the classical manufacturing and process world: New technological and methodological manufacturing concepts like predictive maintenance, adaptive MES/ERP management, big data analysis, augmented reality, Twin-models (Digital), 3D printing, smart grid, intelligent maintenance systems, Artificial Intelligence, CPS (cyber physical systems), CPPS [cyber physical production systems (the 5C's: connection, conversion, cyber, cognition and configuration)] and many more are the drivers of this technological shift. This highlights the urgent need for standardization to enable coexistence, interoperability, in seamless functionality across all these aspects to the IIoT, often also called the "fourth industrial revolution".

However, there is a strong "crossover" in public recognition between "IIoT" and "Smart Manufacturing" (SM) recognized by all in global advanced manufacturing and Smart Manufacturing and in IoT engaged SDOs, organizations and other interested groups.

It is truly difficult to set or identify a hard border-line between both these topics of interest and ongoing development because the overlap shows that often three out of four named topics are handled on both the SM side and the IIoT side, which leads to about 75 % overlapping space being identified.

As this is still an ongoing process of development, it will be considered for review in all future revisions to this document.

IIoT can be defined upon the IoT reference architecture (ISO/IEC 30141), as described later on.

This document has three main focused outcomes:

a) IIoT definition (domains, as well as IIoT systems and landscapes: This provides a structural analysis of all the materials collected and analysed, restructured by subclauses in Clause 5 and outlining different characteristics, technical aspects and functional as well as non-functional elements of the IIoT structure surrounded by appropriate analytic views and comments on standardization to it.
b) Considerations about future standardization in IIoT: This document takes a look at the future of standardization regarding IIoT in Clause 6. Therein it describes the standardization perspective and the necessary risk analysis to be undertaken. It analyses identified problems, challenges and lists potential work items for standardization as well.
c) An overview of identified relevant standards and industrial initiative in relation to IIoT: Listing all the identified SDOs, non-SDOs, and former smart manufacturing and global advanced manufacturing initiatives as input for further development on standardization in the IIoT field in collaboration with Smart Manufacturing, which is the field having the nearest scope to IIoT. Even knowing that these standards are huge in number and mostly related to smart manufacturing as well as global advanced manufacturing, they establish a baseline in relation to each other as well as with regard to new upcoming IIoT related standards.

Clause 6 covers the main conclusions, considerations and outlook to normative roadmapping.

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020

INTERNET OF THINGS (IoT) – INDUSTRIAL IoT

1 Scope

This document describes the following:

- general Industrial IoT (IIoT) systems and landscapes which outline characteristics, technical aspects and functional as well as non-functional elements of the IIoT structure and a listing of standardizing organisations, consortia and open-source communities with work on all aspects on IIoT;
- considerations for the future standardization perspective of IIoT including risk analysis, new technologies and identified collaborations.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

No terms and definitions are listed in this document.

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

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

4 Abbreviated terms

3D	Three Dimensional (mostly in CAD/CAE)
5G-ACIA	5G Alliance for Connected Industries and Automation
AAS	Asset Administration Shell (often shortened to Administration Shell)
AI	Artificial Intelligence
AIOTI	The Alliance for the Internet of Things Innovation
ASMT	American Society for Testing and Materials
AutomationML	Automation (Domain Language) Markup Language (like XML)
CCSA	China Communications Standards Association
CESI	China Electronics Standardization Institute
CIM	Computer Integrated Manufacturing
CPPS	Cyber Physical Production System
CPS	Cyber Physical System
CT	Communication Technology
DDS	Data Distribution Service
DIN	Deutsches Institut für Normung (German MB to ISO)
DKE	Deutsche Kommission für Elektrotechnik (German NC to IEC)
e@Class	(electronic) @ Classification and Product description
EC	Edge Computing

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020

ECC	Edge Computing Committee (China)
ETSI	European Telecommunications Standards Institute
FOAF	(Friend of a Friend) [ontology]
FOSS	Free Open Source Systems
GD	Gateway Devices
GIoT	Green IoT (A LPWAN IoT total solution provider)
GSMA	GSM Association
GUI	Graphic user interface
H2020	Horizon 2020 (EC/EU Founding Research program)
HMI	Human–Machine Interface
I4.0	Industrie 4.0
ICT	Information and Communication Technology
IDSA	International Data Spaces Association
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIC	Industrial Internet Consortium
IIoT	Industrial Internet of Things
IIRA	Industrial Internet Reference Architecture
Industrial CPS	Industrial Cyber-Physical-System
IoT	Internet of Things
IP	Internet Protocol
IRTF	Internet Research Task Force
ISA	International Society of Automation
ISG	ETSI Industry Specification Group – for cross-cutting Context Information Management
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunications Union
ITU-T	ITU Telecommunication Standardization Sector
IVI	Industrial Value-Chain Initiative (Japan)
JWG	Joint working group
LNI	Labs Network Industrie 4.0 (Standardization Council I4.0 DIN/DKE/VDE)
MB	Member Body (ISO)
M2M	Machine-to-machine
NC	National Committee (IEC)
NIST	National Institute of Standards and Technology
NRM	Normative Roadmap Rev. 3.0 (defined by SCI, see below)
OMG	Object Management Group
OneM2M	One Machine to Machine collaboration – by different NBs (USA, EU/EC, JP, China, Korea)
OPC	OLE (object linking and embedding) for Process Control
OSI	Open Systems Interconnection Model
OT	Operational Technology

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020

PLC	Programmable Logic Controller
QoS	Quality of Service
RA	Reference Architecture
RAMI 4.0	Reference Architecture Model Industrie 4.0 (IEC PAS 63088:2017)
R&D	Research and Development
RDF	Resource Description Framework
RTLS	Real-Time-Locating-System
SAG	Strategic Advisory Group
SCI	SCI 4.0 (Standardization Council Industrie 4.0)
SDN	Software Defined Network
SDN	Software Defined Networking
SDO	Standards Developing Organization
SEG	Strategy Evaluation Group
Semanz4.0	Semantics for I4.0
SG	Study Group
SM	Smart Manufacturing
SM/IIoT	Smart Manufacturing/IIoT (Common View)
SmartM2M	Smart Machine to Machine (Focus: Communication)
SOA	Service Oriented Architecture
TC	Technical Committee
TCP	Transmission Control Protocol
TDIA	Telecommunication Development Industry Alliance
TMBG	Technical Management Board Group
ToR	Terms of reference
TSN	Time Sensitive Networking
UA	Unified Architecture
UdF	Usine de Future (France NB)
VDE	Verband der Elektrotechnik, Elektronik und Informationstechnik (Germany NC in IEC)
W3C	World Wide Web Consortium
WSDL	Web Services Description Language

5 IIoT systems and landscape, see [1]

5.1 Overview

5.1.1 General

Figure 2 depicts a structural view of IIoT as the big picture, showing how IIoT is constructed.

Figure 2 should give a base impression of the complexity and structural setup of IIoT, intended as a common view; all technical details and aspects shown therein are explained in the following clauses and subclauses.

It shows up a static as well as dynamic layered view consistently built up from the bottom (the OT Operation Technology World) to the top (the IT-World).

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020

In this way, analog values are converted into digital information, streamed upwards and downwards through the IP centric medial structures (Middleware, Fog-, Edge-) up towards the Business layers, in which this information is analysed, processed, streamed back down to the OT side again, resulting in business outcome with the highest flexibility and lot-size-zero profitable capable results.

All of this is accompanied by vertical organized intersectional elements of checks and balanced control like: Security, Safety, Trustworthiness, Life cycle, as well as vertical management functionalities across all of these.

"Dynamic" in this regard means that all of these structural elements can be seen layered, recursive and paralleled in their being and instantiation like Hardware and software development systems to generate exactly this entire infrastructure are explained in the CESI whitepaper cited in the Introduction.

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020

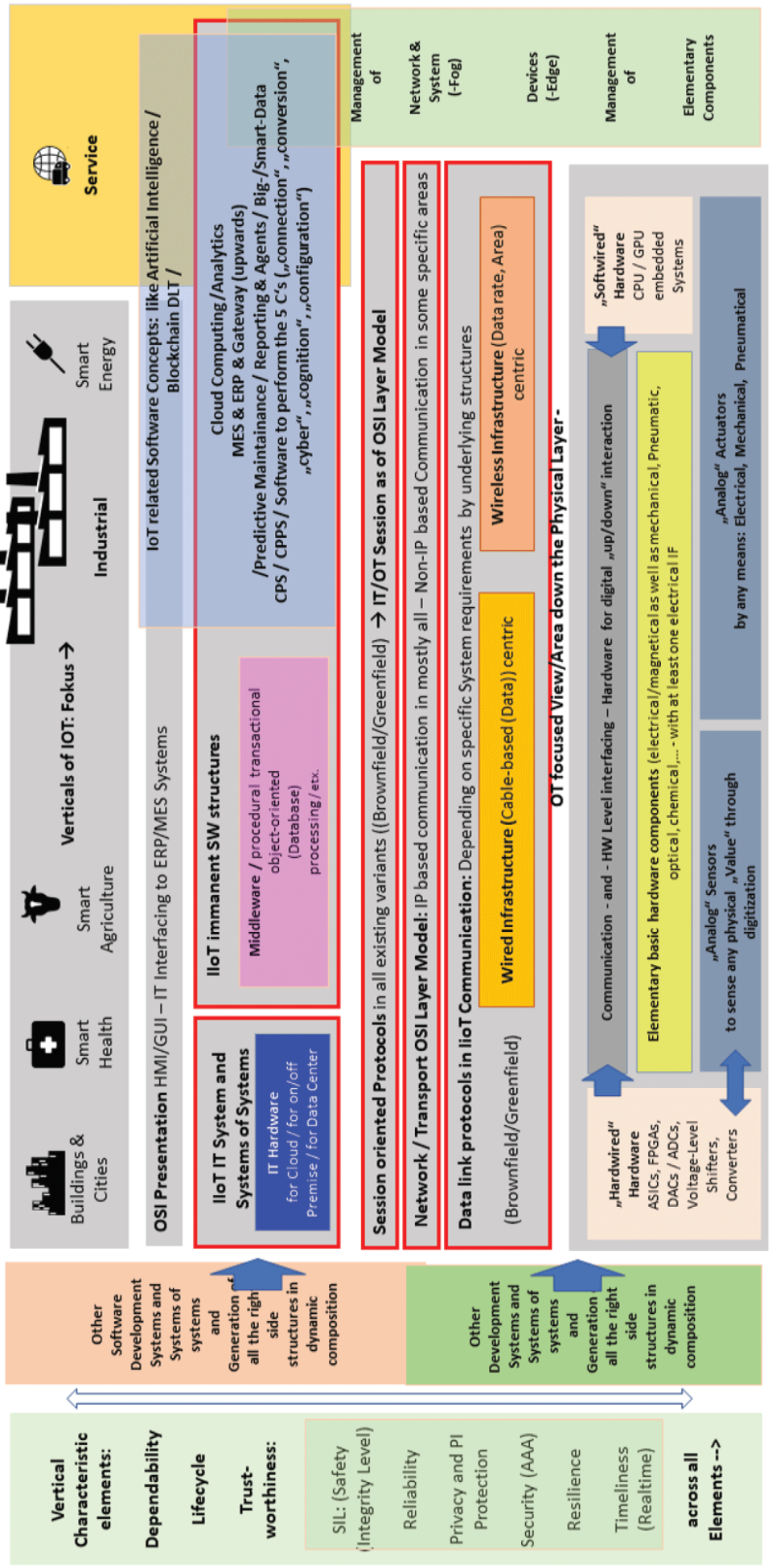


Figure 2 – IIoT mapping landscape description for SDO and non-SDO, consortia, FOSS

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 30166:2020

For the rationale of a general overview to this document, the focus should be on a structured mapping of existing SDO and non-SDO, consortia, FOSS with strong working emphasis on standardization development in IIoT – seen as a vertical of the IoT.

The mapping analysis identifies the following focus areas.

5.1.2 Architecture

This area identifies work with respect to common IIoT vocabulary, frameworks, and architecture that is meant to serve as a common technology ecosystem across various industrial sectors. This focus area considers effort to specify a range of industry-driven requirements that support design, deployment, integration, connectivity, and other scenarios for machinery, equipment, and devices, which are utilized across a broad spectrum of industrial verticals.

EXAMPLE 1 (reference architecture): Edge computing Security reference architectures (ECC); reference architecture of a security gateway for the exchange of industry data and services (IDSA); architecture analysis (oneM2M); OpenFog Reference Architecture (OpenFog Consortium); Service Oriented Architecture SOA – (the Open Group); etc.

EXAMPLE 2 (vocabulary): ISA96.01 Terminology for Actuators.

EXAMPLE 3 (reference model): IVI (Japan) investigates scenarios where companies naturally collaborate in order to gather a broader understanding of more general connection models (reference models).

EXAMPLE 4 (requirements): The Industrial Internet Reference Architecture (IIC); system requirements (ISA); product as a part of the automation solution (ISO/TC 184 / IEC TC 65 – JWG 21).

5.1.3 Implementation of IIoT systems

This focus area identifies matches with respect to implementation and other guiding concepts for the development of IIoT systems and industrial applications.

In particular, it includes the standardization activities with reference to:

– the implementation of industrial control and automation systems, industrial products, and cyber-physical production systems (i.e. machinery, equipment, devices, etc.) in general;
– the implementation of connectivity technologies such as industrial platforms, middleware, identification processes, e.g. to automatically discover, compose and integrate heterogeneous industrial components;
– the development of the coherent ontologies in various industrial domains;
– networking specifics, including vertical and horizontal interoperability concepts;
– system and software engineering that covers the processes, supporting tools and supporting technologies for the engineering of software products and systems for industrial needs;
– the development of IIoT systems and processes and their life cycles
– the implementation of IIoT systems and processes that are influenced by societal and human factors, including human-in-the-loop, trustworthiness aspects of IoT based services to humans, cultural change of the organization under redefined role of humans, etc.;
– the transformation of IIoT systems within a digital factory including such topics as migration strategies, new business models, enterprise domains and value chain specifics.

EXAMPLE 1 (industrial automation and control systems): the control and automation centre (largely standardized within IEC TC 65); modern means for industrial automation scenarios focused on network-based wireless indoor use cases (ITU).

EXAMPLE 2 (industrial product): product as a part of the automation solution (ISO/TC 184 / IEC TC 65 – JWG 21).

EXAMPLE 3 (life cycle dependencies): Integration of life-cycle data for process plants including oil and gas production facilities (ISO 15926 from ISO TC 184).

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020

EXAMPLE 4 (societal and human factors): modelling the front end of software applications (OMG); personal data and personal data protection to the various categories of stakeholders (AIOTI); human role in Industrie 4.0 (SCI 4.0 Standardization Council Industrie 4.0); self-improvement adaptive system including human-in-the-loop (ISO TC 184 / IEC TC 65 – JWG 21).

EXAMPLE 5 (vertical and horizontal interoperability): analyse new business and development models related to communication technologies (former IEC SEG 8, now converted to IEC SyC SM); vertical interoperability such as IIoT systems' integration in industrial cloud environment and federation concepts (DIN SPEC 92222); horizontal interoperability with respect to logistics, conceptualization, design, procurement, construction, commission production, development, and other (ISO TC 184 / IEC TC 65 – JWG 21).

EXAMPLE 6 (migration strategies): conceptual development and trends in the manufacturing sector (Plattform Industrie 4.0); holistic migration approach based on a stepwise process (PERFoRM Horizon 2020 research and innovation program under grant agreement No. 680435).

EXAMPLE 7 (ontology dictionary): IEC CDD according to IEC 61360 series developed by IEC SC 3D is supporting multiple dictionary domains such as process instruments according to IEC 61987, (an application of IEC 61360-1), developed by IEC SC 65E and switchgear and controlgear according to IEC 62683 developed by IEC SC 121A. Several ISO and IEC TCs are currently preparing new dictionaries to be hosted by IEC CDD.

NOTE Many of the newer industrial models (RAMI 4.0 and SGAM for Smart Grid) are based on the Purdue model, which was later standardized as IEC 62264 and IEC 61512. This original hierarchical model is widely used in industry and thus needs to be considered in the IIoT context.

5.1.4 IIoT use case implementations

This focus area includes standardization activities in the area of IIoT use cases, (Virtual/Physical) applications and guidelines in terms of automation (Virtual/Physical) applications and digitized production processes, and other identified technologies that are applied in the industrial fields, e.g. industrial big data, Artificial Intelligence applications.

EXAMPLE 1 (use cases): Industrial use cases (IEC TC 65); Maps of use cases and best practice examples from Germany, France, Japan (Plattform Industrie 4.0).

EXAMPLE 2 (production applications): Integration of technical processes and business processes (DIN, DKE/VDE); digital twin industrial systems (IIC); Standards updates on IoT services enabling technologies (oneM2M and ETSI TC SmartM2M, ISG CIM, etc.).

EXAMPLE 3 (big data applications): analysis reports and standardization activities referring big data (NIST).

5.1.5 Edge (fog) computing in IIoT, see [2]

This focus area identifies standardization activities with respect to edge and fog technologies, services and applications at the edge of the industrial network. This includes deployment models and specific functions of IIoT devices that address patterns for edge (fog) computing, enhancing the functionality of IIoT devices and applications in various industrial scenarios.

EXAMPLE (edge (fog) computing): the edge computing industry cooperative platform that advances sustainable development of the edge computing industry (ECC); security gateway for the exchange of industry data and services (IDSA).

5.1.6 Interoperability and conformance

This area focuses on standardization activities towards interoperability and conformance, including objectives such as the following:

– general interoperability frameworks and communication layers;
– network connectivity aspects, including wireless and wired technology standards, industrial networks (in general), industrial interfaces and real-time communication aspects, etc.;
– semantic interoperability, industrial data, integration of life-cycle data, information models, etc.;
– verification, validation and testing (software, hardware) as well as general activities concerning development of test environments and test beds.

EXAMPLE 1 (interoperability frameworks): framework for data exchange in the engineering process of production systems (AutomationML); OSI-Layer protocols for packet-oriented exchange of data (IRTF/IETF).

AVA Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020

EXAMPLE 2 (semantic interoperability): standards and research activity in the area of semantic and ontology-based interoperability (ETSI); data, information and knowledge exchange inside and outside of organizations/companies (ISO TC 184 / IEC TC 65 – JWG 21); product data representation and exchange (ISO 10303 by ISO TC 184); product description models (eCl@ss) based on the dictionary and semantic modelling according to ISO 13584-42 / IEC 61360-2 (IEC CDD) – CDD is not only used for smart manufacturing, it is used by many ISO and IEC technical committees to identify properties; Field Device Integration (IEC 62769), intelligent device management (IEC TR 63082), and representation of data properties (IEC 61987) which provides lists of properties for the Common Data Dictionary, CDD; as well as data mining standards (DMG).

EXAMPLE 3 (industrial interfaces): OPC UA initiated by OPC UA Foundation; (OPC UA is standardized as a number of standards issued by IEC SC 65E); invoice, settlement and payment Interfaces (GSMA); HMI (ISA 77.60).

EXAMPLE 4 (verification and validation): certification of mobile communication technology (5G-ACIA); standardization of the IDS (Industrial Data space) trusted Connector and certification (IDSA); certification program (oneM2M).

5.1.7 IIoT characteristics trustworthiness

This focus area includes activities referring the general trustworthiness characteristics of the IIoT systems (security, resilience, reliability, privacy, etc.), and activities exploring the role of blockchain and distributed ledger technologies that can be applied across industry networks.

EXAMPLES: Big-Data security (e.g. NIST), edge computing security (ECC); security gateway for exchange of industry data and services (IDSA); Industrial Automation and Control Systems Security (ISA 99); secure protocols (DDS by OMG); web security (W3C).

The IEC report on trustworthiness, see [3] currently in development provides further references on IIoT. This document regards trustworthiness as an entire concept and recognizes the importance to adopt industry best practices in this area.

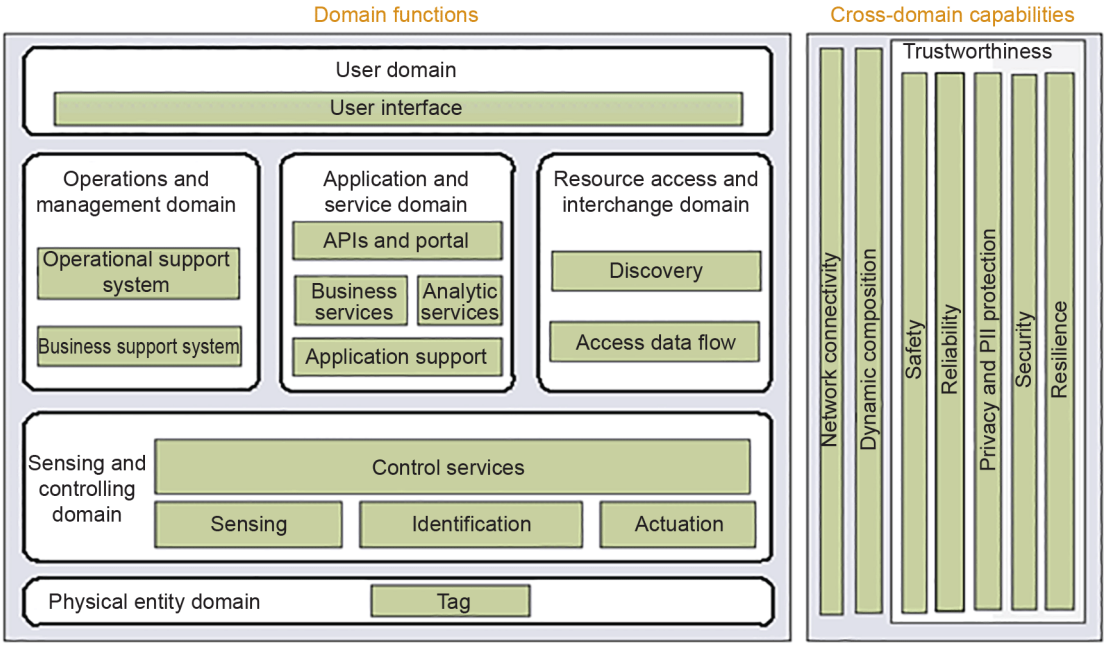
NIST defines trustworthiness as: "the degree of confidence one has that the system performs as expected with characteristics including safety, security, privacy, reliability and resilience in the face of environmental disruptions, human errors, system faults and attacks", see [4].

ISO/IEC 30141 has an almost identical definition in 7.2.1, with ISO/IEC 20924 given as the source.

Figure 3 shows trustworthiness functional components as identified in ISO/IEC 30141:2018.

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020



SOURCE: ISO/IEC 30141:2018, Figure 15.

Figure 3 – Trustworthiness functional components as identified in ISO/IEC 30141:2018

Second ref: by ISO/IEC JTC 1/SG 5 “Trustworthiness”, see [5].

5.1.8 Wearables in IIoT

This area depicts standardization work in the area of industrial wearables focusing on smart devices; near-, on-, in-body electronics; and electronic textiles applied in industrial applications.

Wearables are linked together by a communication (view) based technical implementation through mostly wireless technologies in near proximity-based infrastructures (ISM and Non-ISM (licensed) Bands) such as: WLAN, WSAN, BLE, Bluetooth®[1], Wireless-IO, 3G/4G, 5G, etc.

Examples of standardization activities on wearable smart devices are IEC TC 100, Audio, video and multimedia systems and equipment, and IEC TC 124, Wearable electronic devices and technologies.

5.1.9 Cross-cutting activities on IIoT

This area includes various cross-cutting actions focusing coordination and harmonization activities of the involved standards development organizations and industrial initiatives and consortia. These include such important activities as monitoring, consolidation, harmonization, recommendations, evaluations, and gap analysis.

EXAMPLES: Cooperation and work together to contribute to the creation and development of the Industrial Internet (OneM2M and IIC); German Standardization Roadmap Industrie 4.0 (NB DIN to ISO, DKE to IEC in common with

[1] Bluetooth is a registered trademark of Bluetooth SIG, Inc. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC.

AVA Documents Document Sharing Hub

SCI 4.0 Standardization Council Industrie 4.0), SCI 4.0 is a joint initiative by DIN and DKE, validation of standardization work in test beds (LNI 4.0); harmonization activities with regard to Smart Manufacturing (IEC SyC SM); and ISO SMCC – evaluation of industrial platforms (IVI) [Japan].

5.2 Analysis consideration on IIoT landscape of systems

5.2.1 General

The following analysis focuses on various IIoT areas and aims to describe current challenges and needs of the IIoT standardization landscape as seen from the standards' user perspective. The analysis is based on the current research results conducted to reach seamless connectivity of flexible and reconfigurable production systems and application in the manufacturing environment, see [6], [7]

The analysis identifies six focus areas:

– IIoT System – focuses on general characteristics, compositional representation and semantic requirements for IIoT systems.

– IIoT Application – focuses on pure software applications that provide added value for connected IIoT systems or other IIoT applications.

– IIoT Connectivity – focuses on requirements for connectivity technologies (e.g. industrial middleware) and distributed system architecture requirements to support various characteristics of IIoT systems, e.g. reconfiguration or plug-and-produce capability.

– IIoT Interoperability – focuses on interoperability requirements, referring to integration of industrial communication protocols and specifics of the real-time message transfer in the industrial environment.

– IIoT User – focuses on requirements of software and hardware systems interfacing to a human in the industrial environment to convey information and trigger operations.

– IIoT Migration Strategies – focuses on possibilities for the end-user to easily adopt IIoT requirements in the industrial facilities.

5.2.2 IIoT systems and architecture

5.2.2.1 General

Subclauses 5.2.2.2, 5.2.2.3 and 5.2.2.4 refer to RA Definitions and typical System Characteristics of IIoT systems.

5.2.2.2 IIoT reference architecture

Inherent to IIoT, the IIoT reference architecture needs to consider several respective industry-driven requirements:

a) consideration of value-added processes in relation to the entire value-added chain, see [8];

b) inter-company networking perspectives and their integration through value networks, see [9];

c) consideration of specific industrial system aspects according to system specifics, such as automation devices, field devices, fieldbuses, PLC, operating devices, mobile devices, servers, workstations, etc. see [9];

d) consideration of industrial software application perspectives: sharing applications between multiple companies; machine data specifics, etc. see [9];

e) consideration of product-machine communication as communication and data exchange takes place not only between machines but also between product and machine or the I4.0 components, see [10];

f) cyber-security against external attacks to protect sensitive data.

This document uses ISO/IEC 30141 with extension to vertical mapping to IIoT needs and requirements.

AVA Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020

5.2.2.3 Service-oriented architecture and microservices

On the one hand, the IIoT solutions strongly rely on the use of applications. On the other hand, these solutions should also guarantee that the user data is secured by the service provider. To avoid the case that this security is not enough (e.g. the data should not be stored by a service provider located abroad), it should be possible to manage the data by means of well-defined software architecture, see [11].

Possible architectural solutions that can be applied in industrial environment to overcome such challenges are the service-oriented architectures that allow independence from service providers.

Microservice architecture is a service-based solution that follows the principles of distributed functionalities and separates functionalities in fine-grained services. Contrary to monolithic architectures, microservices guarantee independence from individual technologies or platforms, which can help to reach flexibility in IIoT applications. Other important characteristics are:

- composed of compact services, each with only one dedicated task;
- each service can be written in a different programming language;
- status-free modules that interact orchestrated or choreographed;
- scaling by creating additional service instances;
- complete replacement of modules instead of customization;
- fail-safe due to redundancy;
- requires stable infrastructure (disadvantage).

5.2.2.4 IIoT system considerations

5.2.2.4.1 General

Considerations as seen by/to the IIoT system are the subject of this subclause.

5.2.2.4.2 Life cycle records and I4.0 component

During the life cycle of a product, a large amount of information is accumulated (e.g. operational, maintenance or repair data) that is usually difficult to extract and, further, to match to a specific individual product. As a result, a life cycle is closed with insufficient information about a product.

The challenge is how to decompose an I4.0 component, in which all relevant information can be preserved to contribute to a life cycle record of a product. Thus, I4.0 components consist of an asset (hardware, software or a simple worker) and the administration shell (AAS).

5.2.2.4.3 Recognizability of IIoT systems

To support communication, presentation and recognizability among IIoT systems, a classification of these systems to respective classes will be required.

German industrial initiatives, see [12], present different degrees for classification of communication and identification capability and propose to express the membership of a system by a combined numeric notation CP XY:

– Communication capability (X-digit):

  4 – capable of I4.0 conform communication;

  3 – capable of active communication;

  2 – capable of passive communication;

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020

1 – not capable of communication.

– Degree of familiarity (Y-digit):

4 – managed as entity;

3 – individually known;

2 – anonymously known;

1 – unknown.

EXAMPLE: A simply monitored system throughout its life cycle that is not able to communicate can be presented as: CP14.

5.2.2.4.4 Identity management in IIoT systems

To safeguard authenticity and preserve integrity, secure identity management framework is recurred to verify relationship between man and industrial machine.

Identified technical committee to this aspect: ISO/IEC JTC 1/SC 31 (see [13]) and ISO/IEC JTC 1/SC 27 (see [14]) are working on those topics in standardization, and are in current liaison to ISO/IEC JTC 1/SC 41 on joint working efforts to solve these challenges in IIoT.

EXAMPLE: In the chemical industry, the personal login of a worker to a machine is usual to imply more transparency of, for example, who worked on which product and where, see also [10].

5.2.2.4.5 Re-configurability and pluggability of IIoT systems

Identified technical committee to this aspect: IEEE TC, see [15], on Industrial Agents (WG 2660.1) – IEEE TC on Industrial CPS.

IIoT systems must support re-configuration aspects in order to achieve a flexible manufacturing environment based on the rapid and seamless re-configuration (e.g. of machinery and robots) as response to operational or business events.

EXAMPLE: One of the common ways to support re-configuration is the development of scalable agent-based systems that support dynamic, seamless and on-the-fly reconfiguration and pluggability in a production environment including several different modular production processes, see [18].

5.2.2.4.6 Information modelling of IIoT systems

The engineering process of industrial systems is becoming more complex regarding a heterogeneity of data models and applied modelling tools. This often leads to inconsistency of system's information models, interoperability challenges among various systems and usually results in additional modelling effort for a system as well as for a connectivity technology connecting various systems.

5.2.2.4.7 Other additional characteristics of IIoT systems

Other requirements that should be taken into consideration:

– availability;

– latency;

– adaptability;

– scalability;

– precision;

– maintenance.

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020

5.2.3 IIoT application (virtual/physical use case)

5.2.3.1 General

Subclauses 5.2.3.2 and 5.2.3.3 refer to general aspects and requirements of IIoT systems.

5.2.3.2 General aspects on IIoT application (virtual/physical use case)

Industry-specific applications demand primary focus on the following specifications:

– Cross-border interoperability among various (virtual/physical use case) applications;
– Portability of services in manufacturing ecosystems;
– Serviceability concepts for enterprise-control systems;
– Integration of legacy systems / adapters: Work on this subject is being done within ISO/IEC JTC 1/SC 41 as ISO/IEC 30162 (under development) led by NB Russian Federation.

5.2.3.3 IIoT application (virtual/physical) use case considerations

5.2.3.3.1 General

Seen as IIoT aspects – driven by industrial application and the constraints they got:

5.2.3.3.2 Industrial use case aspects

The IIoT application offers its services in the industrial domain, uses industrial deployment architectures (e.g. event-driven and time-driven) and has industry-focused requirements which are mandatory for use within those types of OT industries and often differs from IT industries.

5.2.3.3.3 Real-time aspects in IIoT (timeliness)

An IIoT application must possess on-time delivery characteristics with regard to its services and data.

NOTE There is currently TSN joint IEEE-IEC work in IEC SC 65C and IEEE 802.1 TG 60802, in project PT 60802 on time-sensitive networking profile for industrial automation, based on IEEE 802.1 and IEEE 802.3.

EXAMPLE: A delayed delivery of the production data can cause significant overload and unexpected stops in the production life cycle.

The former, now disbanded, SC 41 Editing-Group (EG) SC 41/SG 11 has released a report on "Real-Time" in the context of IoT [16].

5.2.3.3.4 Portability aspects in IIoT

Portability is one of the essential requirements of an IIoT application. It describes a characteristic of different applications to be shared and used on other systems. This is possible if cross-manufacturer standards are established for the design of IIoT applications.

5.2.3.3.5 Data anonymization aspects in IIoT

Due to the rapidly growing demand for big-data analytics, industrial applications undergo increased risks for data disclosure and privacy violations. Thus, a standardized approach/framework is required that takes the sensitivity of data into account.

EXAMPLE: Several industrial companies share the use of the same application and need access to big-data analytics data for various reasons. This predicts existence of a large number of users with different access privileges. To achieve anonymization of data, special roles need to be taken into consideration and analysed.

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020

5.2.4 IIoT connectivity

The IIoT connectivity to/by edge- and multiple clouds (i.e. by federation)

There currently exist a big number of heterogeneous solutions for IIoT connectivity technologies, usually known as the Industrial Middleware Technology, see [17], or I4.0 plattform, see [12].

As a result, the multiple heterogeneous architectures make it difficult for the end-user to manufacture products as well as to develop or connect in-house or other manufacturing applications to heterogeneous middleware solutions.

To close possible gaps a revision of industrial middleware solutions is required to provide an IIoT connectivity framework with regards to IIoT reference architecture. ISO/IEC 30141 as developed in JTC 1/SC 41 could be taken as a base for this reference architecture.

Special attention should also be drawn to such issues as interoperability among multiple middleware solutions, scalability and security, see 6.3.3 and 6.3.7.

In Plattform I4.0, a joint AG1/AG3 “Secure Communication for Industrie 4.0” sub-group on “OPC/UA Security in Industrie 4.0” has been established for this purpose and has generated publicly available whitepapers on this aspect, see [19].

5.2.5 IIoT interoperability focus

IIoT interoperability is focused on the following aspects:

– RA components interoperability:
  - system-to-system interoperability;
  - system-to-human interoperability;
  - system-to-application interoperability;
  - application-to-application interoperability;
  - company-to-company interoperability.
– Real-time communication to be interoperable.
– Harmonization of message transfer formats applying industrial protocols.
– Minimization and definition of recommended standards for IIoT interoperability to reduce complexity.

5.2.6 The IIoT user, see [20]

Industrial systems are becoming highly automated and with capabilities for self-configuration, self-adjustment and self-optimization. In spite of the increased level of technology, the role of human worker still remains in IIoT systems, see [9].

Workers operate with increasing levels of complexity and need to flexibly adapt to the dynamics of the new production systems, see [21], also related to the product customization. The type of control humans have on the process involves more cognitive and emotional effort, see [22].

Workers are expected to deal with complex tasks, to interact with robots and other devices and to be always able to handle exceptional and unexpected situations, such as failures or hazards, to the extent of adhering to the myth of the “magic human”, see [23].

Work connected systems and human characteristics have to be jointly designed and assessed, see [24], to offer the workers the most adequate services.

AVA Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020

Such characteristics of the manufacturing environment have several implications in terms of communications:

– Identification mechansims: RFID based systems or other solutions to identify the worker and enable the access workstations or tools, only to authorized workers, allocated to the job based on their skills, see [24] – RFID/AutoID is in Scope of ISO/IEC JTC 1/SC 31, also in liaison to ISO/IEC JTC 1/SC 41.

– Sensors/cameras/kinetics to detect human position, behaviour and postures in order to prevent risks related to possible collisions with robots; wrong operations leading to quality errors; unhealthy postures not compliant with ergonomics guidelines, see [25].

– Wearable sensors to measure workload, fatigue or stress (i.e. Brain Computer Interfacing; see [26]. – "Wearables" are in the Scope of ISO/IEC JTC 1/SC 41 SG7.

  Including not only physiological things but also radiation/chemicals which are applicable to this aspect, see [27].

  - Virtual reality/augmented reality on wearable device to provide context- and situation-aware information and instruction to the operator, see [28].
  - Microphones/cameras or other devices managed by the operator to record, store and share field observations (i.e. product defects, problems with machine tools, etc.).

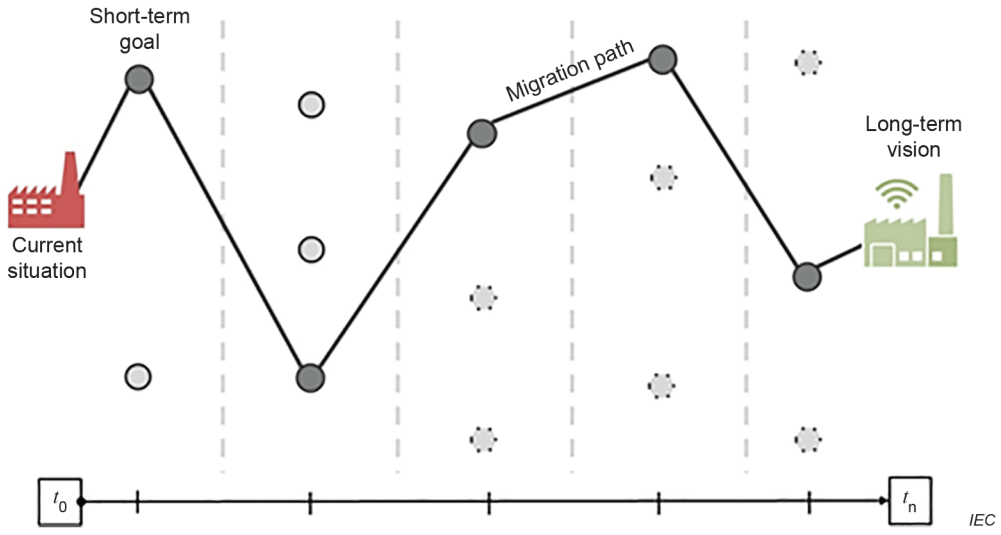
5.2.7 IIoT migration strategies, see [29]

Although automation in manufacturing is clearly changing, only few industries have adopted advanced automation solutions in their production environment. Reasons are various. Many research projects focused on solving highly specific problems while neglecting other technological issues. At the same time, manufacturers are quite conservative in adopting new technologies with their legacy systems and processes since the implementation of IIoT systems and new communication protocols has a big impact on the production systems, not only on the technical dimension of the factory but also on system's performance, work organization and business strategy. One of the key challenges is the lack of standardized holistic and smooth strategies to support manufacturers in their migration towards adoption of IIoT.

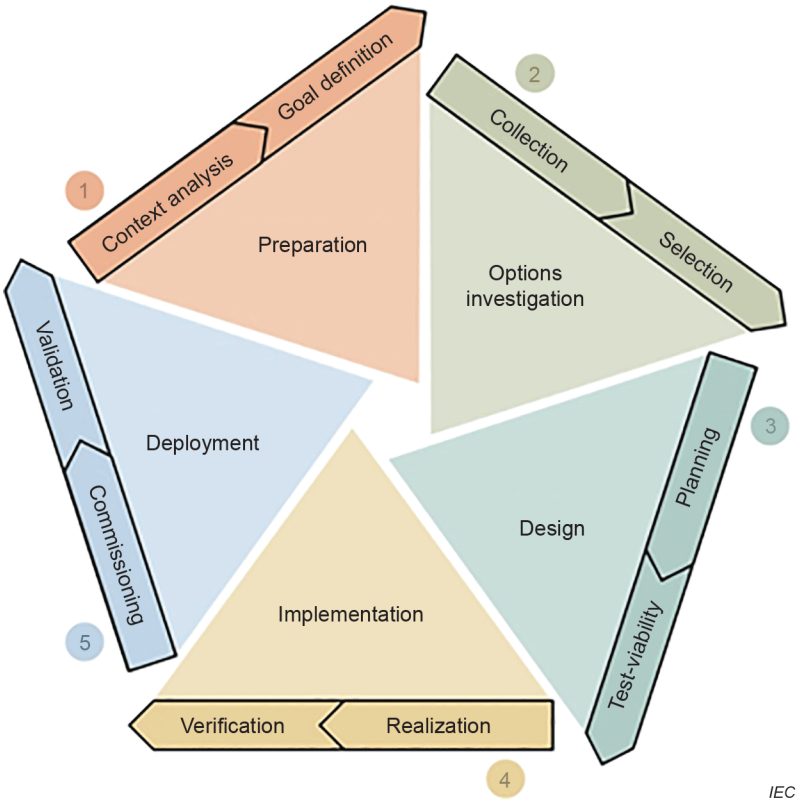
EXAMPLE: The EU PERFoRM project [7] [18][20] has developed a holistic migration approach based on a stepwise process. In fact, only a stepwise approach can mitigate the risk related to the implementation of non-well-known solutions (here: IIoT) in existing production systems, especially when the way forward and the target condition of the migration are unclear and uncertain. The approach in Figure 4 supports the continuous improvement, adaptation to changes and innovation of a system by generating a set of intermediate steps towards the long-term vision of Smart Factory, envisioned by the Industrie 4.0 paradigm, which decomposes the migration path in incremental steps (a). This approach is supported by a 5-phase migration process (b), which has been developed for the identification, design and execution of the migration steps towards the long-term goal following an iterative and incremental approach.

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020



a) Definition of the migration path



b) Migration process towards IIoT system

Figure 4 – Migration approach towards IIoT systems

5.3 General definition of IIoT and smart manufacturing (SM)

5.3.1 Definition of IIoT

The following definition is used based upon work by CESI in the whitepaper on IIoT from the China NC in 2017:

> "IIoT is a new industrial ecosystem of service driven built based on the network interconnection, data interoperability and system interoperability of industrial

AVA Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 30166:2020

resources, to realize the flexible configuration of the manufacturing materials, the on-demand execution of the manufacturing process, the rational optimization of the manufacturing process and the rapid adaptation of the manufacturing environment, and to achieve the efficient utilization of the resources."

Smart machines connected and coexisting by modern means of IIoT can serve more accurately and more consistently than a human could do permanently.

So, enhancement and achieving better efficiency and quicker problem solving and for less money without the replacement of the human being in a production scenario is key. This should therefore lead the thoughts of further standardization to this motivation in IIoT!

In addition, this document has expanded this view by seeing IIoT as a subset of IoT as defined in ISO/IEC 30141.

5.3.2 Cyber physical systems differentiation in the IIoT

IoT is about connecting "things" (objects and machines) to the Internet and eventually to each other; while cyber physical systems (CPS) are integration of computation, networking and physical process.

There is today a more or less hard defined border between these definitions and there will be related technical aspects from one side to the other which cross this border. NIST has initiated/published a "Reference Architecture for Cyber-Physical Systems" in its "Cyber Physical Systems Program", see [30].

5.3.3 Industrial Internet to CPPS and CPS definition

The industrial company GE defined the "Industrial Internet" to describe the industrial transformation context of machines, cyber-physical systems, advanced analytics, AI, people, cloud, edge computing in a connected, to fully integral (time, structure) manner, see [31].

5.3.4 Smart Manufacturing differentiation vs. IIoT

For initial discussion on comparison, this document takes the following definition of smart manufacturing by the ISO Smart Manufacturing Coordinating Committee (ISO SMCC) agreed with the IEC Systems Committee on Smart Manufacturing (IEC SyC SM):

"A domain of integrated processes and resources (cyber, physical, human) to create and deliver products and services, which also collaborates with other domains within an enterprise value chain and improves its performance aspects."

NOTE 1 Performance aspects include agility, efficiency, safety, security, sustainability or any other performance indicators identified by the enterprise.

NOTE 2 In addition to manufacturing, other enterprise domains can include engineering, logistics, marketing, procurement, sales or any other domains identified by the enterprise.

As with the initiation of IEC SyC SM, see [32], ISO/IEC JTC 1/SC 41/SLG 1 IIoT, in collaboration with IEC SyC SM, is mandated to get a better understanding about the differences in the key core components on standards between SM and IIoT.

Until this clarification, we keep and recognize Smart Manufacturing as a specific application of IIoT.

5.3.5 Verticals of IoT market

IIoT, as previously mentioned, can itself be recognized as a part of IoT. Within IOT AIOTI defines eight verticals around IoT in general, as shown in Figure 5: (Smart) Home/Building,

AVA Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 30166:2020