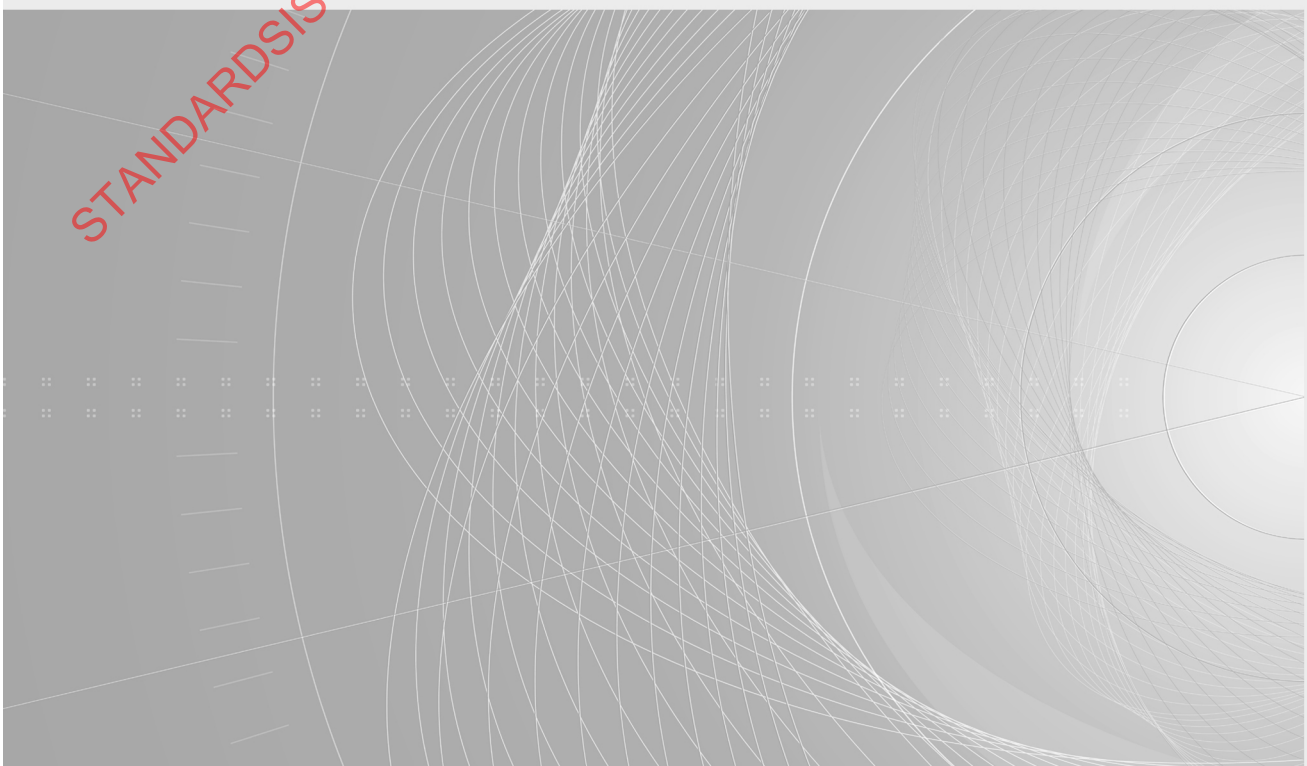
ISO/IEC TR 30166

Edition 1.0 2020-04

TECHNICAL REPORT

Internet of things (IoT) – Industrial IoT



ISO/IEC TR 30166:2020-04(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

ISO/IEC TR 30166

Edition 1.0 2020-04

TECHNICAL REPORT

Internet of things (IoT) – Industrial IoT

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25-040-40; 35.020; 35.240.50

ISBN 978-2-8322-8251-9

CONTENTS

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.

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.

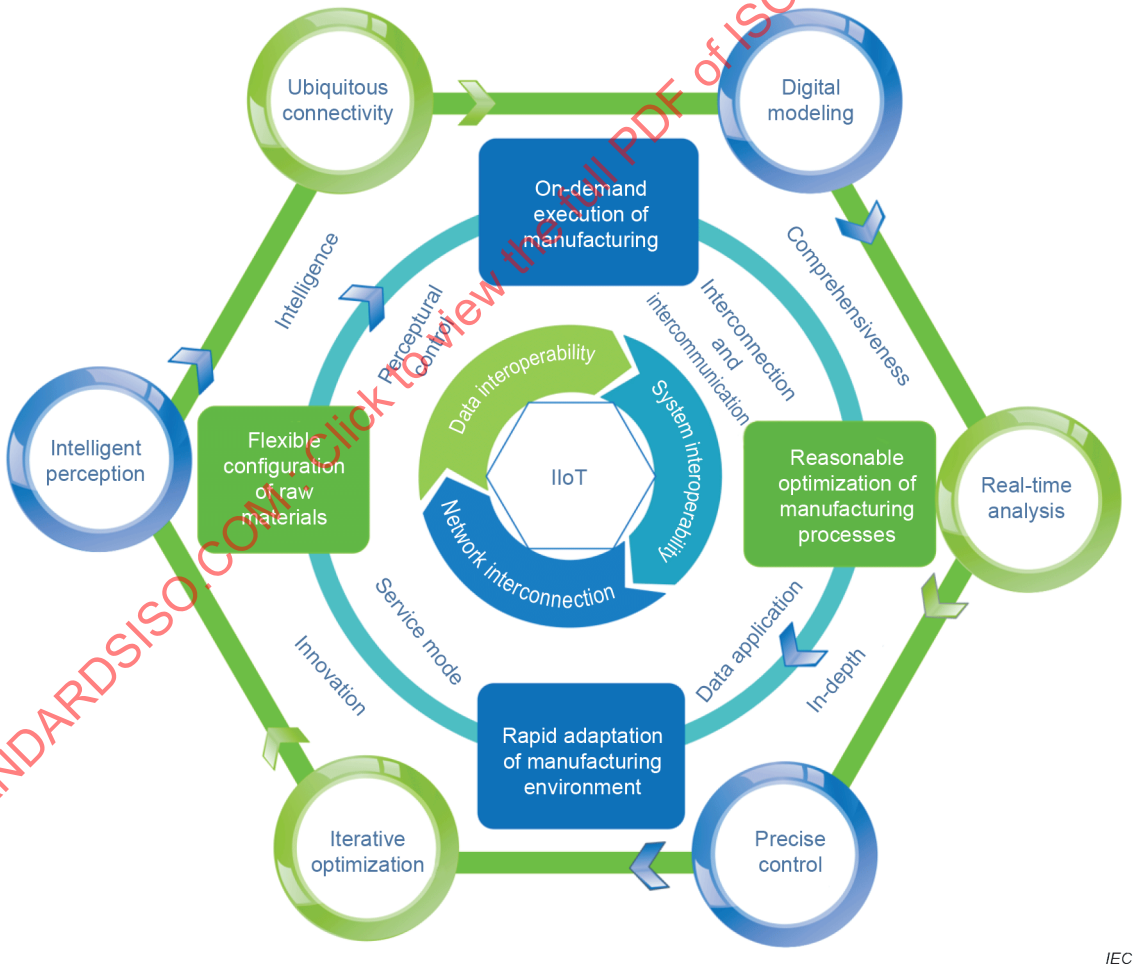
First of all, a definition is used based upon work by CESI in the whitepaper on IIoT from the China NC in 2017:

> "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.

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

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.

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

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

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.

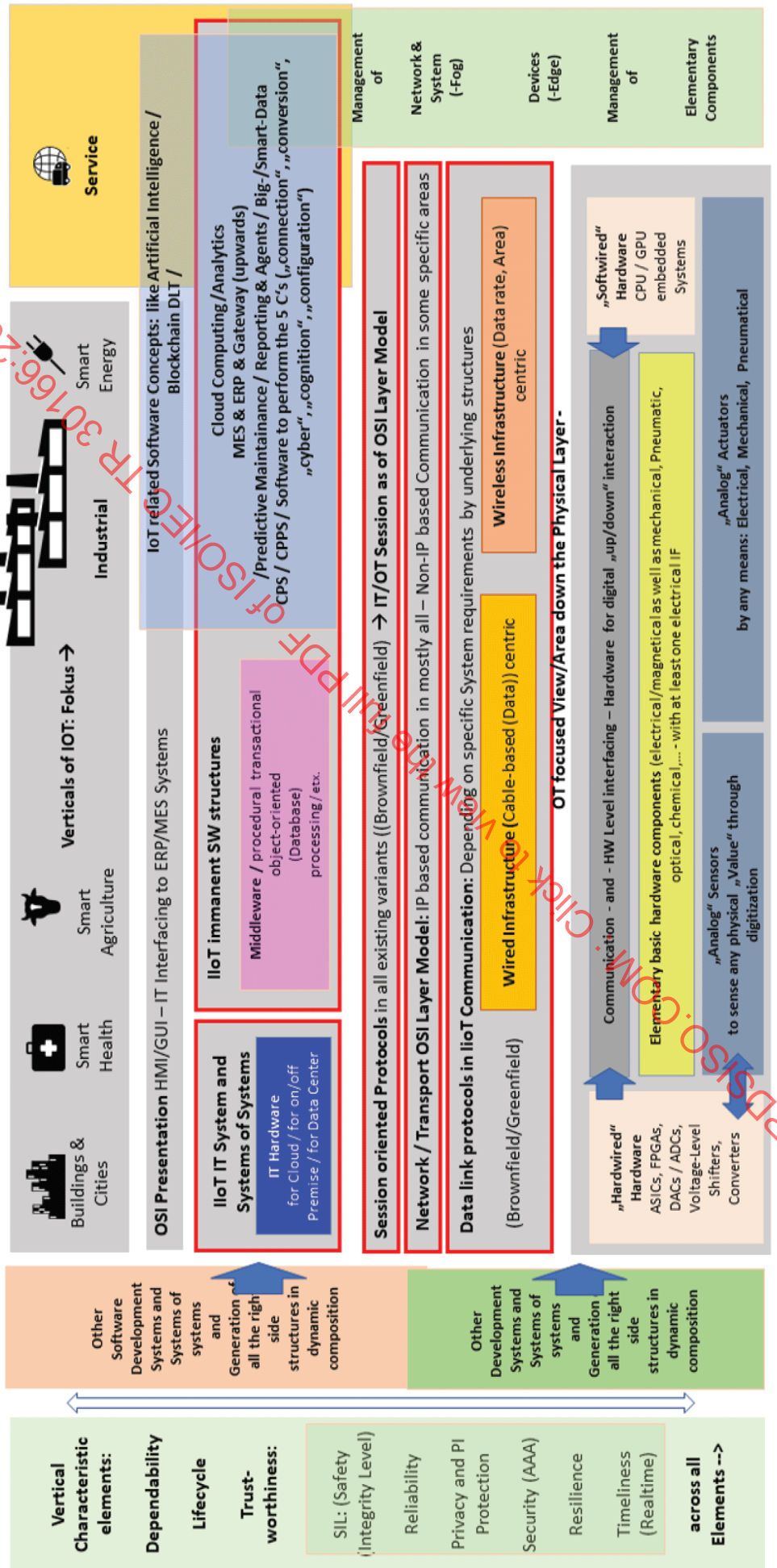
Figure 2 should give a base impression of the complexity and structural setup of IIoT, intended as a common view; all technical details and aspects shown therein are explained in the following clauses and subclauses.

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).

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.



IIoT Infographic: The Internet of Things (IIoT) - the structural static view to it as a „Big Picture"

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

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).

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).

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.

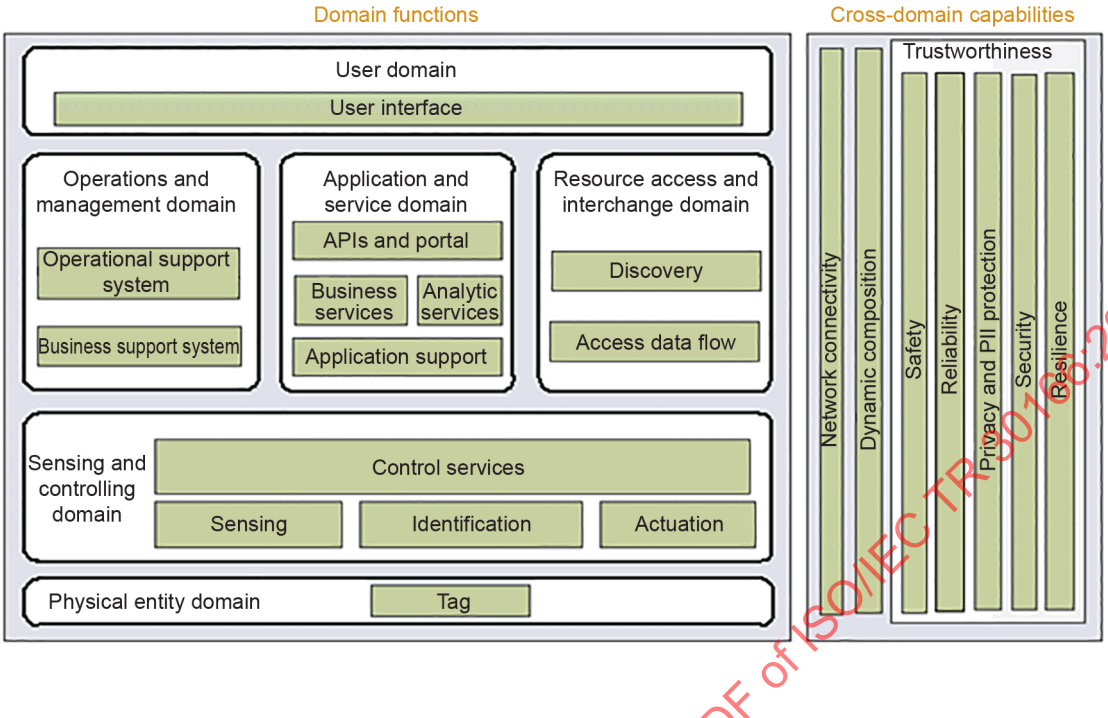
EXAMPLES: Big-Data security (e.g. NIST), edge computing security (ECC); security gateway for exchange of industry data and services (IDSA); Industrial Automation and Control Systems Security (ISA 99); secure protocols (DDS by OMG); web security (W3C).

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.



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.

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.

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;

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.

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.

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.

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.

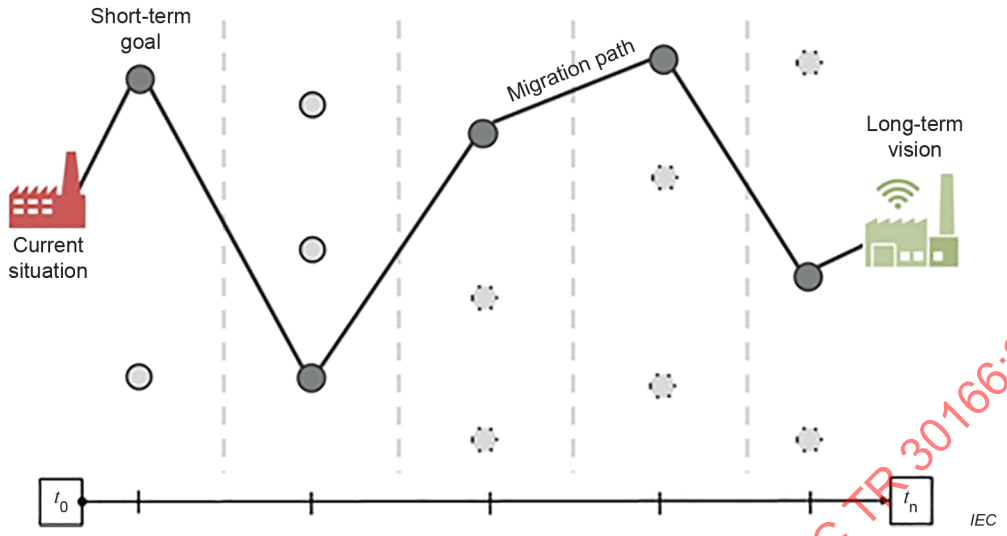
  Including not only physiological things but also radiation/chemicals which are applicable to this aspect, see [27].

  - 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.).

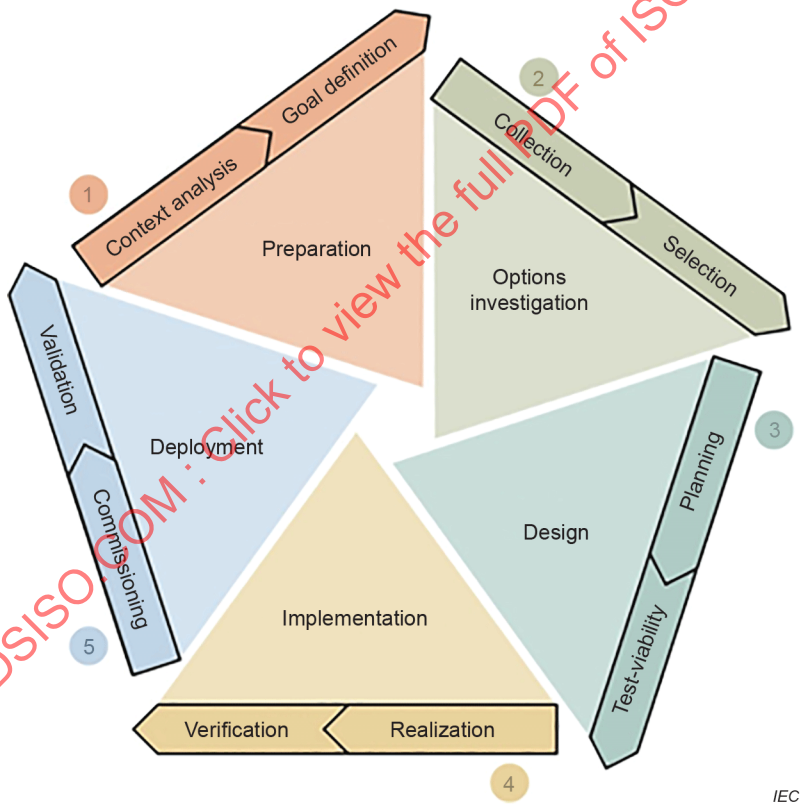
5.2.7 IIoT migration strategies, see [29]

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.



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

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.

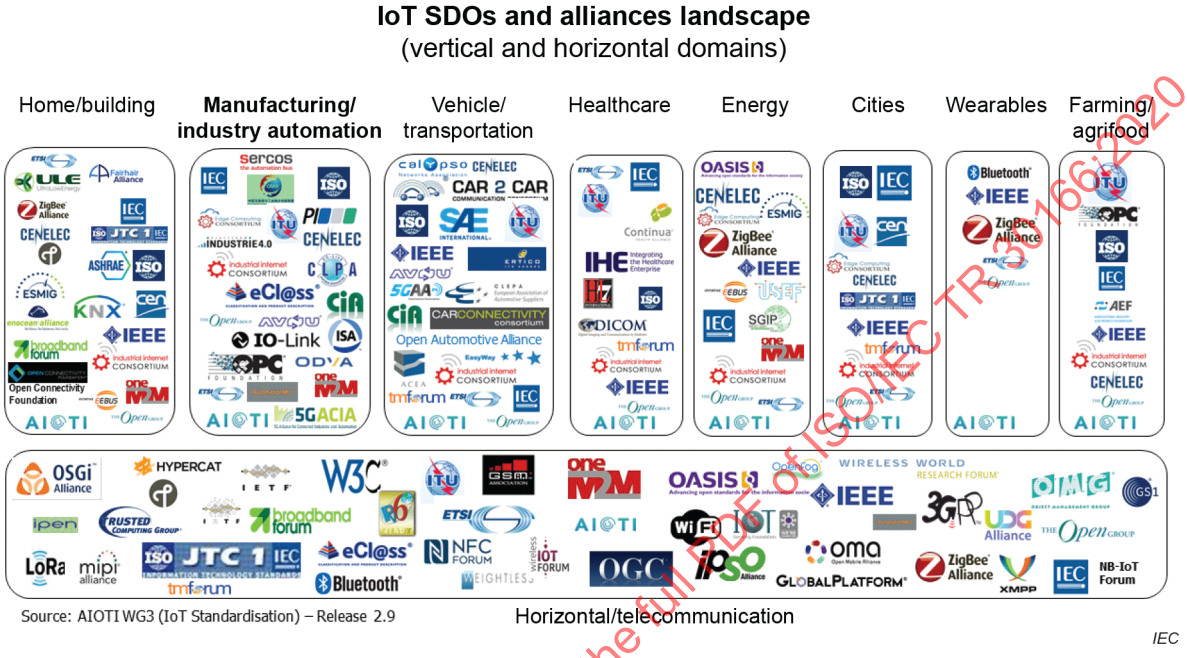
Until this clarification, we keep and recognize Smart Manufacturing as a specific application of IIoT.

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,

Manufacturing (Industrial automation), Vehicular/Transportation, (Smart) Healthcare, (Smart) Energy, (Smart) Cities, Wearables, (Smart) Farming.

Furthermore other verticals are identified in study groups of ISO/IEC JTC 1/SC 41 such as wearables (or in IEC TC 124, Wearable electronic devices and technologies), and in liaisons of ISO/IEC JTC 1/SC 41 in regard to technical standardization, e.g. IEC SyC Smart Energy.



a) Manufacturing / industrial automation as part of AIOTI standardization view, see [33]

b) Detail view of AIOTI diagram on standardization in industrial automation

Figure 5 – IoT SDOs and alliances landscape (vertical and horizontal domains)

Figure 5 b) focuses on the SDOs with work-scope on standard Smart Manufacturing and its derivatives as given in the definition above.

Additionally, this document identifies the relevant standards organizations for the underlying horizontal communication and networking infrastructure elements (telecommunications, energy, etc.).

It is noted that while out of scope of this document as it falls under national regulations, in some cases there are initiatives to allocate spectrum for industrial use, mostly based upon needs for industrial automation given the current ongoing development of IIoT.

This also causes the initiation of standards based consortia like 5G-ACIA as a driver to foster standardization in this regard (see also Annex A on this initiative).

5.4 Smart Manufacturing and IIoT

5.4.1 General

Subclause 5.4 lists elements to the ToR regarding Smart Manufacturing and IoT in a detailed view: It holds the appropriate definitions as well as in regard to vocabulary to update accordingly in collaboration with the ISO/IEC JTC 1/SC 41/WG 3 IoT Architecture and Vocabulary group work.

This document also lists and determines by name the appropriate reference architectures in view of its Scope.

5.4.2 The IIoT high-level view

Subclause 5.4.2 sets an initial "bird's eye view" of IIoT in separated contexts.

For this document, a most common definition of IIoT is agreed out of the existing ones as explained in 5.4.1 to avoid overlapping ones by diverse stakeholders in SDO/non-SDO/FOSS.

In addition, this document identifies the following aspects:

– Differientiation between IIoT and SM:
  - On communication and data centric "digital twins" as a virtual counterpart to read systems,
  - Smart Manufacturing scopes on business models and operations,
  - Migration to twin and/or of legacy manufacturing system to Smart Manufacturing.
– Uncertain targets – must be clarified between both (SM vs. IIoT).
– Separation – between both SM/IIoT (table based).
– Congruence/similarities – between both SM/IIoT (table based).

Figure 6 and Figure 7 provide 'bird's eye view' graphical representations showing there are often elements which overlap in the context of IIoT.

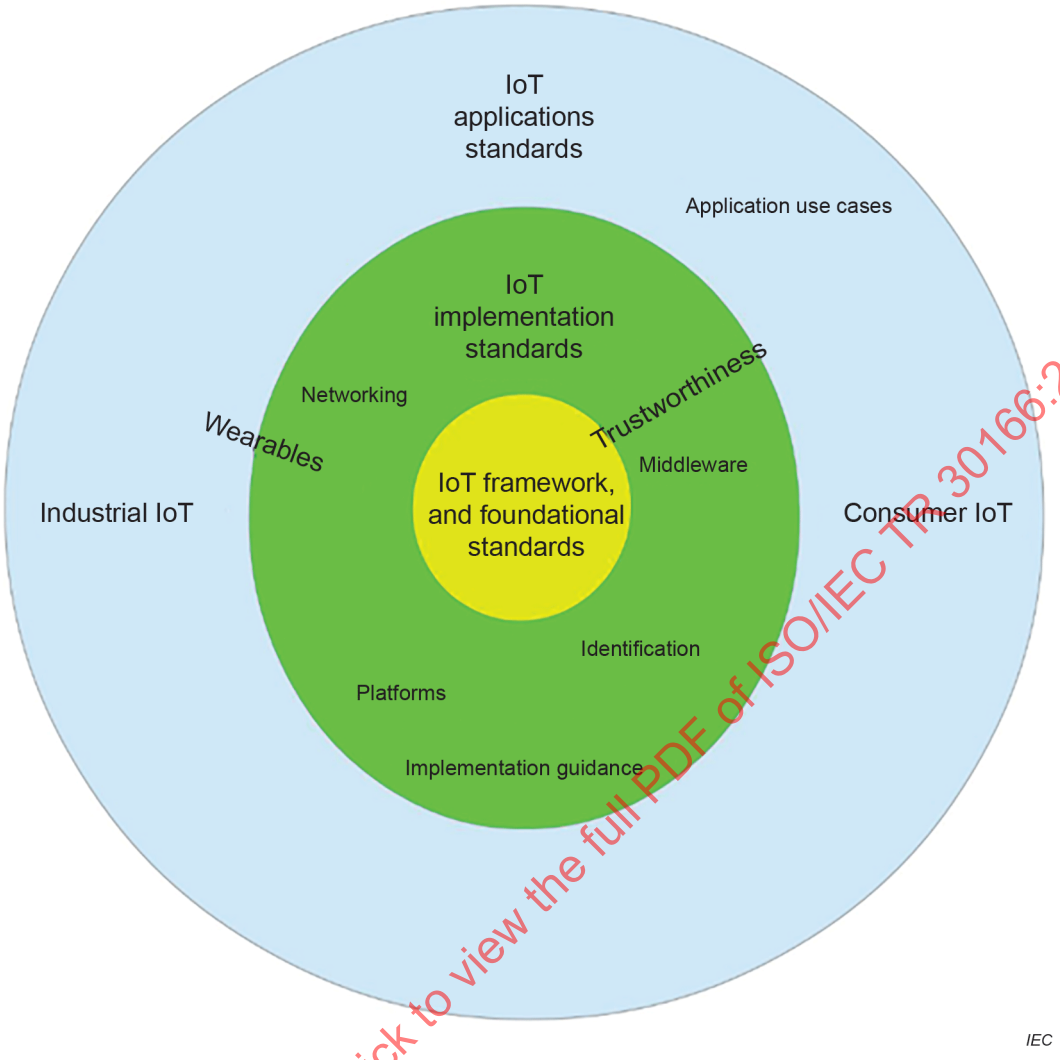


Figure 6 – Layout of the overall view on IIoT in the SC 41 context – the IoT bird's eye view in ISO/IEC JTC 1/SC 41, see [34].

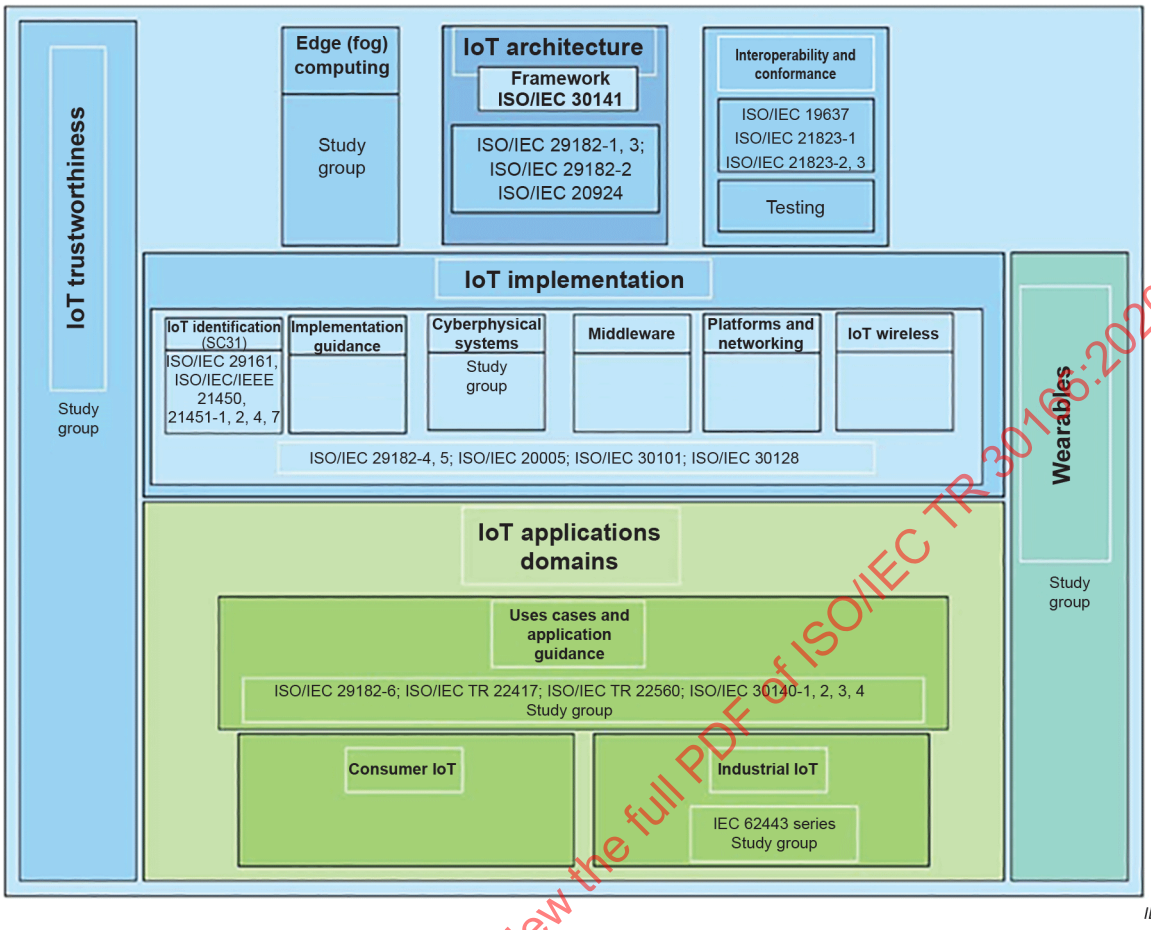


Figure 7 – Diagram showing that the IIoT is part of the IoT applications domain (bird's eye view), see [35]

5.4.3 Industrial products/services life cycle – in IIoT/Smart Manufacturing

In reference to the analysis of ISO/SAG/TMBG AHG#1, see [36], "Analysis and comparison on RA Model" – the life cycle must be separated between the different aspects:

– product;
– life cycle;
– system life cycle.

All of the analysed RA Models have a similar capability to represent a (product/system) life cycle manufactured by a factory/organization.

5.4.4 Industrial manufacturing/automation through (IT/OT) standardization – CPPS

IIoT in regards of fieldbus level: The field device level is identified as one of the most important levels for standardization in general. The fieldbus standards are developed within IEC TC 65/SC 65C:

The classical OT view does not have a strong focus on IT networking of its devices in layers. Furthermore, it is today still burdened with proprietary solutions and therefore incompatible fieldbus architectures and structures, which must be overcome by standardization, unable to operate over a single network. This is one of the main drivers for the development of TSN standardization.

Additionally, the lack of standardization in the meaning of cyber physical system coming from the Brownfield integration of legacy systems to an autonomous operating "living unit" of its classical OT devices and structures drives the requirements for IIoT. This is performed by three elements of digitization:

– Computerization: Local by gateway devices (GDs) "assisting" the OT Brownfield infrastructure.
– Connectivity: Enabling Brownfield OTs to perform "networking".
– Collaboration: Bringing autonomous operation to Brownfield OTs by AI/smart enhancements through both above solutions – especially sustained by edge- and fog-computing concepts as a further important “enabler”.

Considerations: Together with (communications) protocols by IEEE and ITU-T as identified, this is a key field for standardization which should be fostered in the future.

Knowing that there have already been many native standards defined in IEC on fieldbus level, it is clear that with the upcoming IIoT there is a need for a good "synchronization" between the IT and the OT level in the above initial mentioned meaning. This could be intended by consideration of this document as further work in ISO/IEC JTC 1/SC 41/SLG 1 IIoT together with all the above-mentioned OT level SDOs in common liaisons.

5.5 Collaboration considerations on an IIoT reference architecture for standardization (use case driven)

5.5.1 General

It is highlighted that IIoT should avoid thinking in “vertical” silos.

Taking a horizontal approach captures the necessary requirements, which leads to better results, understanding and recommendations for future standardization.

Thus, with respect to the given ToRs, this document will therefore use the term "requirements and characteristics" instead of the term "taxonomy" to improve understanding of its relevant elements.

In accordance with this rationale, the former ISO/IEC JTC 1/SC 41/SG 9 IIoT Report and this document focus on identifying characteristics rather than taxonomy by naming.

Subclause 5.5 lists the requirements in detail given they help define the scope for standardization. Furthermore, this document tries to identify potential work items by a given ToR in regard of development of technology from their “characteristics and requirements”.

Additionally this document takes ISO/IEC 30141 as the base for building an IIoT reference architecture.

5.5.2 General comparison of RAs and models on IIoT, see [37]

This document indicates on the different RAs which is based on several comparison reports from ISO/SAG/TMBG/I40, IEC/SEG7, IEC/SG8, not to be detailed therefore more inside this document.

5.5.3 IIoT systems characteristics: connectivity and communication aspects

This document recognizes that communication aspects for IIoT are defined by a broader scope of layered infrastructure.

The concept of IIC/IIRA connectivity stack does match well to the needs and outlines modern element and standards widely used in this area.

Therefore, Figure 8 is the communication "big picture" on IIoT in relation to the static one shown in Figure 2 but showing more detailed concrete named/listed protocols standards by FOSS as well as SDO based developments.

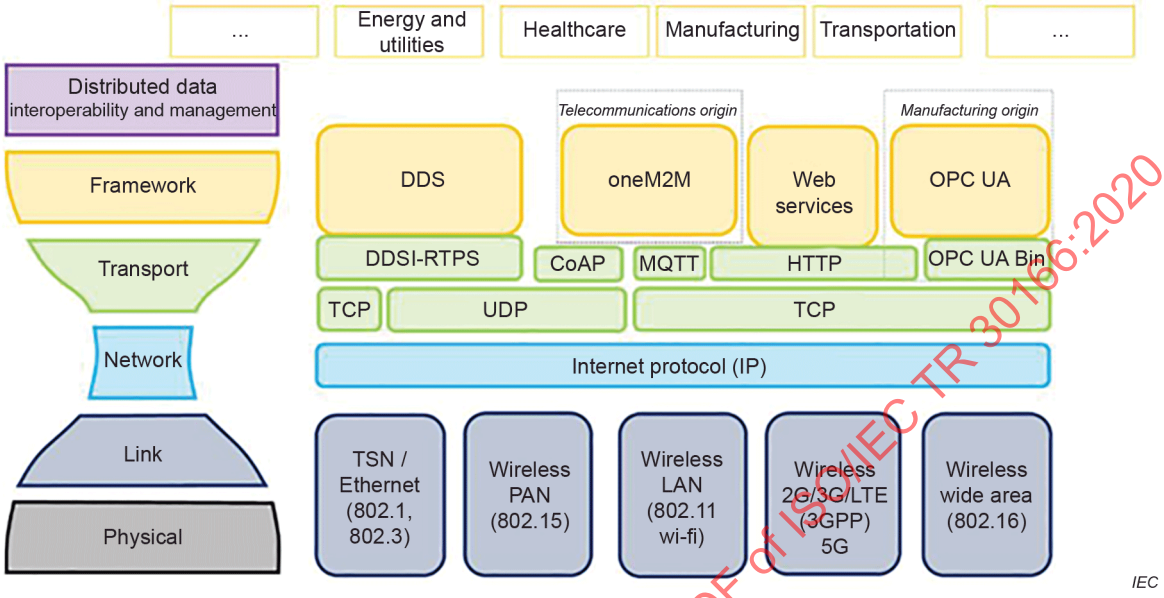


Figure 8 – IIoT connectivity stack from IICF, see [38]

5.5.4 IIoT semantic aspects: IIoT characteristics

Subclause 5.5.4 is an introduction to "semantics" in the realm of this document in ISO/IEC JTC 1/SC 41/WG 5, see [39].

Note that semantics is seen as a very important aspect in IIoT.

As defined in NRM I4.0 (Rev 3.0) White Paper: "Semantic Standards and Use Cases for Industrial Automation and Controlsystems in the Standardization Roadmap Rev.3. of 2018/01 based on Graph Manipulation Theory":

> "Semantics of, or even more vivid: a design (of a system) is sloppily said as a guideline of a set of directives – in case of designing system behavior with a Graph Manipulation Semantics – the directives give guidelines to implement a system thus indirectly on how to manipulate graphs with appropriate tools. Since Graphs comprise (System) Nodes resp. (Graph) Vertices, Edges and relationships by which a system design is modelled comprising a system architecture and its behavior. In case of behavior a graph edge represents an interface obeying two kind of formats, i.e. a mapping assigning to every edge a pair of ordered or unordered nodes called directed respectively undirected edge. A directed edge represents an event at a system interface between two nodes with an event head as the starting node and an event tail as the targeted node. An undirected edge is an event that has not yet been activated, in other words the condition to occur has not yet been enabled. Thus an undirected edge is simply a relationship between system nodes that will eventually communicate.
>
> Furthermore, nodes represent system components with variables and edges representing activities as transitions that are triggered by conditions as part of the components.
>
> Hence a design based on the graph manipulation semantics (i.e. behavior of a real system) is expressed in terms of subgraphs constructed from nodes and edges.

The nodes representing components use guards on variables, activities and events in order to model system behavior."

Compared to the definition of semantics above, this document does not contain a similar semantics definition, although conceptually semantics has been handled by many institutions and organizations and all of them have different and sometimes diverging goals. There is however a need to distinguish in IIoT and elsewhere between types of representation of ontological, semantical and cyber-physical real-world systems.

These representations are related to each other by the so-called semiotic triangle composing ontological language artifacts with semantics reasoning artifacts with cyber-physical implementation artifacts (see Figure 9).

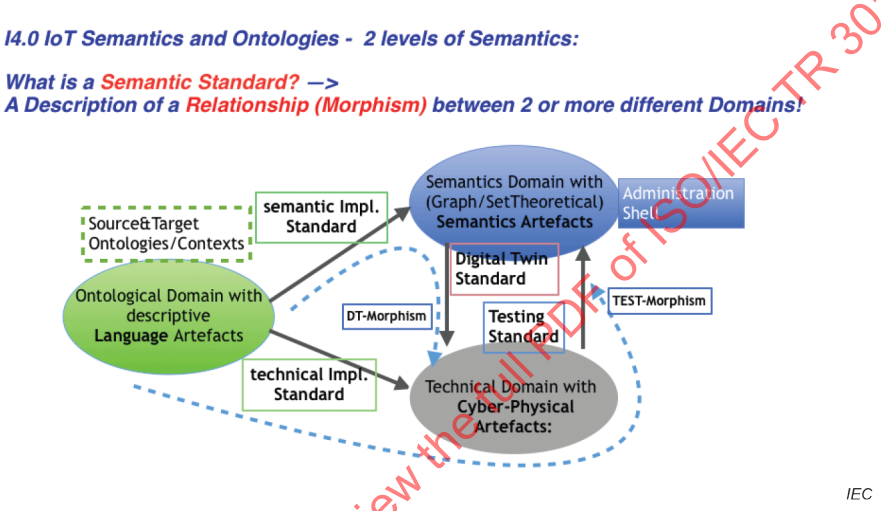


Figure 9 – The semiotic triangle

Relevant identified standardization activities of ontological semantics used in IIoT are:

– eCl@ss based on ISO 13584-42– and IEC CDD classes and properties,
– "Semanz4.0", see [40],
– "AutomationML" – based upon IEC 62714, see [41],
– "WSDL", see [42] Web Services Description Language (WSDL) by W3C,
– IEC SC3D with IEC 61360 (the semantic information model),
– IEC 62656 (the spreadsheet-based transfer of information),
– IEC CDD (the semantic and ontological repository based on IEC 61360 and IEC 62656) accessible via URL https://cdd.iec.ch,
– etc. (Appropriate: W3C listed below in Annex A on Organizations)

while mathematical semantics is based upon theories such as:

– modal logics,
– algebras,
– graph manipulations, etc.

However, both, i.e. ontological and mathematical semantics, must be related to each other, thus to be related by a homomorphism.

The Reference Model RAMI 4.0 (IEC PAS 63088:2017) is considered as an architectural representation but not as a semantical model. It comprises three dimensions, each of which

represents a type of transformation to be modelled by a kind of semantics based on graph manipulation theory of the NRM I4.0 (Normative Roadmap in RAMI 4.0), see [43].

Semantics is used in a twofold manner:

1) to provide an information model (related to a specific ontology) for querying or reasoning purposes, and
2) to provide a system dynamics model supporting checking inconsistencies during interoperation. Both possible interpretations shall be related to semantics web descriptions (such as FOAF based on RDF, see [44].)

Semantics is meaning in a formal sense and it refers not only to data as such but to a way of axiomatic interpretation of data. For example, the ontological approach by which the device description functions is part of the ontology about measurement data capturing – so, semantics is understood as an overall explanation of system-inherent properties and activities, e.g. the interpretation of temperature sensors in a certain environment.

Meta-information of data is given as part of the data model and not part of the semantics model. The semantics model is handled separately in order to provide tools for reasoning. The meta-data model describes the attributes of data in terms of rights to access, to use, to handle or to consume data.

Obviously, in IIoT there needs to be an agreement on how the data handling is stated by a set of meta-data constraints, e.g. indoor temperature measurement, etc. instead of semantics as a global (system-wide) not a “point-to-point” attitude.

Interoperability requires a semantical tool (with a GUI) that is able to perform both data and performance (processing) of Global IoT (GIoT) models.

Standardized data models are represented as “abstract data types” of an algebraic style.

Using semantics for predictive analyses requires simulation tools obeying a GUI that is able to perform GIoT system models such that it becomes possible to predict, for example, next safe states or to check whether some system invariants get violated or not under certain circumstances. In other words, system analysis requires a semantics model which allows the simulation of system properties.

Graph theory based semantics can provide powerful tools for dealing with predictive analysis, e.g. see [45]. By the discussion and explanation already achieved in ISO/IEC JTC 1/SC 41/SG 9 on IIoT, the Semantic IoT may become a meaningful term provided to separate semantics concerns from concerns of the technique of IoT. Thus, this can be seen in two levels: a semantics level of understanding related to an IoT level of understanding.

Up to some extent the relationship must be homomorphic, i.e. structure-preserving respectively almost like each other. Thus, changes at one level introduce similar changes at the other: There is a need according to this analysis to find a semantics approach that can model semantically the full ontology of the technical IIoT. For more information, compare to “WiSE worldwide interoperability for Semantics IoT” [50].

Data models and structural semantics are different descriptive elements. Whereas data models describe things, structure describes a kind of logic of things. For example, the elements of a book can be described in a unique way, such that any device or service of IoT is able to exchange descriptions of books with the same meaning.

A book data model does not tell how to understand a book, – that depends on circumstances and contexts in which the book will be used.

For the latter it requires a unique way of understanding of a book, i.e. the appropriate logic **“**to read” the book in a similar reverse way it has been written, see “Project Haystack” [46].)

As a conclusion, using the book example: data structures (e.g. a book) and data logics (to understand a book in given contexts) are different things and thus must be modelled by different methods, i.e data models or semantics models.

This document considers to take action on data modelling techniques by looking out for committees or organizations which already do standardization of semantic descriptions in order to collaborate and to consider the needs and requirements with respect to IIoT.

RAMI 4.0 (IEC PAS 63088:2017) has defined a "big picture" on semantics for the Model which already covers aspects on RAMI 4.0 implementations. A deeper look and analysis can be found in IEC SEG 8 Industrie 4.0 report, see [47].

Please note again that the RAMI 4.0 is an architectural model and not a semantical model, see [48]. Nevertheless it comprises three dimensions which are not (yet) similar (homomorphic) with the chosen semantics based on graph theory.

The relevant considerations by this document’s analysis is that this will also be investigated and enhanced for standardization by JTC 1/SC 41/AG 20(SLG1) IIoT in context of the standardization council of the national body of Germany at DIN/DKE and in regard to the new started Standardization Roadmap revision number 4.0 to IIoT, see [49]. Other example is shown for the IIoT/SM “Semantics” Standardization in Europe:

- ETSI/SmartM2M – is concerned with semantics in different working groups. As a liaison to ISO/IEC JTC 1/SC 41 it should exchange information with regard to IIoT.
- "WiSE-IoT" – Interoperability for semantics IoT: Wise-IoT is a collaboration project between Europe and Korea, see [50].
- For EU side, funded under the H2020 framework program for research of the European Commission. It aims at deepening the interoperability and interworking of IoT existing systems.

Based on a use case driven approach, the project will use the experiences available in the consortium to build a comprehensive mediation framework that can be used between various IoT systems. Wise-IoT also aims to build up federated and interoperable platforms ensuring end-to-end security and trust for reliable business environments with a multiplicity of IoT applications. Building synergies with national and international initiatives in both Europe and Korea, the project acts on the field of standardization, fostering IoT development and interoperability.

The ontological approach is shown in Figure 10 (DDD), in which the device description functions as the ontology about the measurement data. So, semantics helps understanding as an overall explanation of i.e. the usage of temperature sensor in a certain environment.

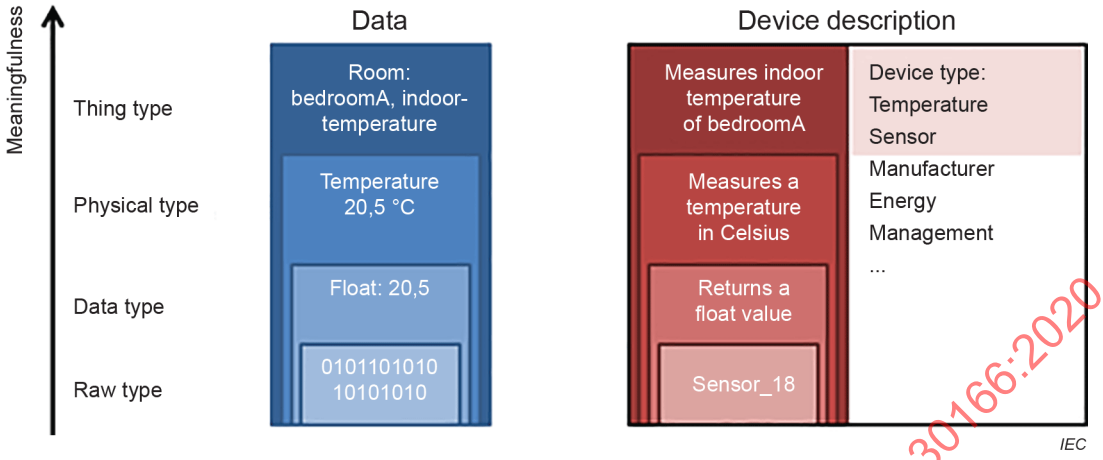


Figure 10 – Semantics in IIoT meaning context, i.e. sensing

Definition according to WiSE-IoT as reference:

> "Semantics is the study of meaning. In our context, this refers to the meaning of data, information or knowledge represented in an IoT system. If systems can *a priori* agree on the semantics of information, the semantics can be implicit, i.e. encoded in the system itself.
>
> For example, due to such an agreement, an information consuming system knows that the value 56,0 provided by an information producing system is a temperature value in Celsius that represents the internal working temperature of a particular machine.
>
> Such exchange of information is efficient but requires a very tight coupling and each change requires explicit steps to change the configuration or even to recompile the system (Notice: Re-compilation in graph semantics approach is called 'type coercion').
>
> For large-scale, dynamically changing systems as in the Internet of Things, the involved systems need to be able to self-adapt to any such changes. To be able to find the currently relevant information or the set of currently relevant sources of information, their semantics has to be explicit, i.e. provided as meta information with the data or information itself."

As discussed earlier, this document indicates the following.

– Meta-information of data should be used as part of the data model.
– The semantics model should be handled to provide tools for reasoning.
– The meta-data model should describe the attributes of data in terms of rights to access, to use or to consume data.
– For two systems to interwork succesfully – there is no such thing as general semantics of exchange because of different contexts, although there must be an agreement on how the data handling is achieved by a set of meta-data constraints, e.g. indoor temperature measurement, etc. as Figure 10 shows.
– Semantics is a global, not a point-to-point, approach.

This is referred to as semantic interoperability, which is defined as "means enabling different agents, services, and applications to exchange information, data and knowledge in a meaningful way, on and off the Web". Semantic interoperability is achieved when interacting systems attribute the same meaning to an exchanged piece of data, ensuring consistency of the data across systems regardless of individual data format.

5.5.5 Data scale in IIoT

Data scale is a relevant characteristic of sizing of data and the capability within the IIoT to handle it. Therefore, it is in scope for relevance to standardization for it. Data scale does influence the general capabilities of IIoT systems. This document identifies the following responsible committees to these aspects:

“Cloud and Cloud Infrastructures” in: JTC 1 / SC 38

“Big data and Smart data”: JTC 1/WG 9

and between both of them – edge- and fog-computing concepts, identified responsible committee: ISO/IEC JTC 1/SC 38. These are already handled by ISO/IEC SCs in detail as listed above and by NIST as mentioned for "Cloud Workgroup Mandate" by reference (see Annex A).

This document identifies the need for standardization but does not recommend putting the focus of standardization onto the "size of data" alone as an indicator for the IIoT. So, by distinguishing between the above-mentioned aspects and concepts there is no identified need for standardization with only regard to "data size". This would be more a classical question on data storage and structuring technologies.

5.5.6 Runtime integration of IIoT

The runtime integration is a conceptual part of real-time integration. IIoT standardization does need in this context the ability to seamlessly interoperate between different reference architectures with the worldwide scope.

IIoT also has needs for coexistence between different reference architectures (RA) in worldwide scope to handle this kind of runtime integration. Consequently, this should also be reflected by the work of study group ISO/IEC JTC 1/SC 41/SG 11 on “Real-Time IoT”.

5.5.7 Edge computing in IIoT

Edge computing was analysed and tracked for standardization via study group ISO/IEC JTC1/SC 41 – AhG/SG#10.

Now it has become part of ISO/IEC JTC 1/SC 41/WG 3 as an ongoing project of ISO/IEC JTC 1/SC 41, see [51].

Outside of ISO/IEC the newly founded ECCE (Edge Computing Consortium Europe), see [52], has started an initiative to build a Reference Architecture on Edge Computing (RAMEC4) comparable to or based on RAMI 4.0.

While edge computing is taking place proxied near to the endpoints (devices) and cloud computing moves data and calculation (as virtual processes) into a data space, fog computing can be recognized as the overlapping view between both paradigms. As listed below, the Open Fog Consortium (now part of IIC), see [53], deals with standardization in this regard.

5.5.8 The endpoint – considerations on IIoT

Endpoints are by definition not only located in the outer connectivity area nor are they located purely in the low-Level OT Areas like Device Level or Work Station Level.The most important aspects on endpoints is not only their integration for OT layers but also their security concepts, which are one of the most recognized "entry points" for potential attacks!

IIC considers an endpoint to be a component that has an interface for network communication and it can be of various types including device endpoint or an endpoint that provides cloud connectivity.

Further aspects relevant to IIoT standardization work program are identified within the following SCs:

– (Unique) Identification of Endpoints in IIoT (JTC 1/SC 31 and JTC 1/SC 27)
– "Endpoint Security in IIoT" (JTC 1/SC 27)
– "Endpoint vs. Edge-Computing" (Collaboration with JTC 1 / SC 38)

5.5.9 "Dependability" for IIoT systems (IEC TC 56)

Characteristics are determined by the industrial area operation needs for:

– Trustworthiness (performed work by JTC 1/SC 41/AHG 8), and
– Dependability (performed work by IEC TC 56),

and should be tracked within the scope of these committees.

As in the existing liaison from ISO/IEC JTC 1/SC 41 to IEC TC 56 to foster standardization, especially for example on the IEC 60300-3-10/Ed2 development.

6 Considerations for future standardization of IIoT

6.1 Main findings by this document on IIoT standardization

This document identifies that there is a current and (fast) increasing number of organizations, collaborations, industrial consortia, and academia initiatives which claim to standardize the industrial IoT each from their own perspective. It is therefore absolutely necessary to maintain communication and coordination with these organizations to be able to identify standards on IIoT regarding the corresponding IEC and ISO work scopes.

This document indicates there is the potential of duplication of standards which could be avoided by intense collaboration through liaison performed potentially within ISO/IEC JTC 1/SC41 by the advisory group ISO/IEC JTC 1/SC 41/AG 20/SLG 1 IIoT.

Clearly semantics will play a key role for standardization within IIoT. As described in previous sections, semantics are becoming more and more important and therefore should be fostered by standardization.

The recommendations of PI40/NRM I4.0 Rev. 3.0, (becoming NRM I4.0 Rev. 4.0 as new revision expected to be released by mid-2020), already cover many aspects identified by comparison of the different reference architecture models described earlier.

Privacy and privacy impact assessment as well as "ownership of data" are some of the key challenges to be solved through a standardized process. Therefore, it is of prime importance to take these aspects also into account for further analysis by ISO/IEC JTC 1/SC 41/AG 20/SLG 1 IIoT.

However, the generation of standards creating data and/or communication "silos" should be avoided in all cases.

Consequently, there is a need to develop a common architecture element of these verticals into a base layer. Standards within this base layer should therefore focus on the horizontal elements of industrial IoT to enable a standardized interchange on information models between all participants across the verticals. This is particularly relevant in technologies such

as AI, microservices, blockchain, etc. which are already being implemented across many industries.

This document proposes standardization collaboration supported by ISO/IEC JTC 1/SC 41/AG 20/SLG 1 IIoT and its referenced SDO. All parties should reflect on all of these new technologies and give directions to generate standards in close liaison and exchange to the technical experts of all impacted SDOs.

General "interoperability" and coexistence within IIoT is another main challenge and therefore should be kept under close analysis and review:

To this end, the first new work item proposals have been submitted to cover these aspects for the first time: on “compatibility requirements for devices within IIoT systems”, see [54].

6.2 Risk for standards development on IIoT

6.2.1 General

Subclause 6.2 explains in detail the different identified aspects or risks for standards developments as of our given term of reference, also based upon the discussions and results of the JTC 1/SC 41 SG 9 Report on IIoT. Consequently, all IIoT standards should be certified to a risk assessment, i.e. based upon the 31000 family of International Standards.

6.2.2 Avoiding work duplication on IIoT standards development – across SDOs

There is a constant risk in standardization engagement of similar or comparable topics being duplicated across SDOs.

This document recommends therefore to intensify communication and coordination across related SDOs via liaisons, etc. Further consideration to this aspect by this document:

– missing synchronization on complementary elements in SDOs to IIoT standards;
– missing synchronization between platforms by noncomplementary standards;
– correct and valuable identification of gaps on IIoT standards and coordinated effort on filling those identified gaps;
– keeping the intention on a generic life cycle on standards as mentioned by JTC 1/SC 41 SG 9 Report on IIoT.

This is seen as a key area of work for ISO/IEC JTC 1/SC 41/AG 20/SLG 1 IIoT.

6.2.3 Important to IIoT: "semantics above syntax", see [55]

As semantics and in its context the semantic Web becomes more and more important to any Smart Manufacturing / IIoT implementation, and in addition to this the ongoing development of Artificial Intelligence in the context of semantics for IIoT may also get more dominant recognition, it is highly recommended to intensify the exchange between all the SDOs and consortia which handle these developments for further standardization. See also detailed explanation on semantics in 5.5.4.

Further findings by this document highlight the ongoing developments on semantics in IoT in general where requirements may be applied to IIoT which have not been standardized yet.

6.2.4 Standards for handling the “ownership of data” in IIoT, see [56]

There are many (legal) considerations for IIoT which are out of standardization scope. The following is an excerpt from the official World Economic Forum report in 2015 which shows the need for further discussion on the ownership of data:

"For public policy-makers Clarify and simplify data policies: To realize the promise of the Industrial Internet (IIoT), global companies need clear legal guidelines over data ownership, transfer and usage:

- Who owns the data generated by equipment?
- What information can be shared or sold, and under what circumstance?
- How will responsibilities among parties be handled when the data originates in one jurisdiction and is used in a different one?
- In complex global organizations, it is often more difficult to segregate Industrial Internet data than that of consumer Internet based on national boundaries. Until the full impact is better understood, it would be prudent to introduce temporary policies to guide the market and spur innovation.
- Governments need to collaborate with each other and industry to harmonize compliance requirements in data and liability laws, as the European Commission and the United States are doing on message standards.
- This will streamline data flow within a jurisdiction and across national boundaries – an issue critical to large, global organizations."

A general concept to solve issues in an automatic way may be supported by the blockchain technology, see [57].

This document indicates that the work of ISO/TC 307 on distributed ledger and it's use case: smart contracts may also be of use.

As of today, there are no known standardization activities around ownership of data, but there may be a need to define such rules or standards which tackle this issue.

6.2.5 Vocabulary definitions – issues to IIoT

In the past there have been situations in which common names and expressions have taken other or different meanings in OT than in IT – and vice versa. This document also indicates on the coordination of standardization activities together between ISO/IEC JTC 1/SC 41/WG 3 and ISO/IEC JTC 1/SC 41/AG 20/SLG 1 IIoT due to the particular wordings and syntactical identifiers within the area of IIoT.

6.3 Perspective to development of standards for IIoT

6.3.1 "Digital twins" – as a generic concept in IIoT

The following definition provides a view of the digital twin within the concept of Smart Manufacturing and IIoT.

A digital twin (DigTwin) in IIoT and Smart Manufacturing is a replicated virtual instance of a physical entity – with all of its (object) properties (Content, representing data, …) and (functional and structural) behaviour as well as its capabilities (Communicating, Processing, …). The DigTwin "shadows" the entity completely by simulation and including its future behaviour (prediction).

The DigTwin can be (optionally) supported by sensing of the real entity (instance) during its entire life cycle which feeds back into the DigTwin model.

Through this concept, a DigTwin can be used to predict and control real-world status of elements as well as also potentially predict its future behaviour. Therefore the DigTwin approach is capable of being used in different conceptional IIoT models and reference architectures to enhance IIoT/SM. Typical use cases for DigTwins include detection of potential issues with CAE based design, reducing R&D costs dramatically, and simulation of entire future value chains in production series as well as processing plants again reducing

costs in finding the best possible solution virtually before investing in physical deployment, see [1].

The DMDII – The Digital Manufacturing and Design Innovation Institute identifies other examples, whilst further sources on digital twin concepts can be found within both ISO and IEC, for example:

ISO/TC 184/SC 4 – ISO 10303-242, *Industrial automation systems and integration – Product data representation and exchange – Part 242: Application protocol: Managed model-based 3D engineering*

ISO/TC 184/SC 4 – ISO 10303-238, *Industrial automation systems and integration – Product data representation and exchange – Part 238: Application protocol: Application interpreted model for computerized numerical controllers*

ISO/TC 184/SC 4 – ISO 23247-1, *Digital Twin manufacturing framework – Part 1: Overview and general principles*

ISO/TC 184/SC 4 – ISO 23247-2, *Digital Twin manufacturing framework – Part 2: Reference architecture*

ISO/TC 184/SC 4 – ISO 23247-3, *Digital Twin manufacturing framework – Part 3: Digital representation of physical manufacturing elements*

ISO/TC 184/SC 4 – ISO 23247-4, *Digital Twin manufacturing framework – Part 4: Information exchange*

A further development in DigTwin definition comes from MT-Connect: This standard enables manufacturing equipment to provide data in structured XML rather than proprietary formats using its Quality Interoperability Framework (QIF), which defines it as a Unified XML framework standard for computer-aided quality measurement systems.

6.3.2 (AI) Artificial Intelligence to be used by IIoT (ISO/IEC JTC 1/SC 42)

6.3.2.1 General

This document uses Wikipedia as a starting point to define the Meaning of AI: see [58].

> "Artificial intelligence (AI, also machine intelligence, MI) is intelligence demonstrated by machines, in contrast to the natural intelligence (NI) displayed by humans and other animals. In computer science AI research is defined as the study of "intelligent agents": any device that perceives its environment and takes actions that maximize its chance of successfully achieving its goals.
>
> Colloquially, the term "artificial intelligence" is applied when a machine mimics "cognitive" functions that humans associate with other human minds, such as "learning" and "problem solving."

AI is seens as highly relevant for IIoT and Smart Manufacturing:

- AI can and will increase the Smart Industrial Evolution beyond the narrow tasks that robots perform today for automation.
- AI can enable and sustain autonomous operations and systems in Smart Manufacturing and IIoT Domains.
- AI can be implemented in IIoT Solutions to solve challenges of the handling and processing in the key field of big data in manufacturing as well as in Process Industrial applications.

– AI can – based upon the already mentioned semantical aspects – perform and enhance industrial applications in general and thereby enable new solutions in the industrial field.

AI aspects are being investigated and developed in many SDOs. Within ISO/IEC JTC 1, a subcommittee (SC 42) has been established to develop standardization in the area of Artificial Intelligence.

Relevant standardization on AI is done in ISO/IEC JTC 1/SC 42 « Artificial Intelligence »

The scope of JTC 1/SC 42, Artificial Intelligence, is as follows.

“Standardization in the area of Artificial Intelligence

– Serve as the focus and proponent for JTC 1’s standardization program on Artificial Intelligence
– Provide guidance to JTC 1, IEC, and ISO committees developing Artificial Intelligence applications”

6.3.2.2 “Cognitive intelligence” in IIoT

Cognitive intelligence in IIoT covers machine learning and predictive analytics and maintenance in IIoT. This is still in its infancy and unclear if this will be included as a definite task to ISO/IEC JTC 1/SC 42.

Potential organization to work on this further in collaboration with Open Group and W3C is being addressed by JTC 1/SC 41/SLG 1 IIoT.

6.3.3 Federation of cloud in/between IIoT systems (DIN SPEC 92222)

Work is currently ongoing regarding the interaction of IIoT and cloud-based solutions. For example the German national body DIN is now working on a reference architecture model (RA) for “Industrial Cloud Federation” (ICF).

See also DIN SPEC 92222 “RA Model for Industrial Cloud Federation”.

There is other work on this topic, including work from University of Amsterdam, see [59].

6.3.4 Future standardization on: “microservices and micro-applications in IIoT” see [40]

Both terms microservices and micro-applications have brought recognition in the IT field of distributed system and therefore within the scope of ISO/IEC JTC 1/SC 38 which is already now working on this.

As with other envelope standards, the central core technology development is kept in ISO/IEC JTC 1/SC 38 although integration within IIoT will likely be required, via collaboration.

6.3.5 “Blockchain technology” – future standardization in IIoT

It is envisaged that blockchain technology will be used extensively in IIoT.

To this extent, there are identified reported new built initiatives by SDOs as well as non-SDO and Open Source (FOSS) around the world.

The SDChain Initiative is also engaged on blockchain for IIoT and is therefore mentioned within this document referentially by the following abstract and citation.

"Since the birth of Bitcoin, blockchain and cryptocurrencies have been flourishing vigorously. However, most current blockchain projects are still on the basic level of token issuance and exchange of virtual information – there are very few digital assets which have real value to be widely used to establish a practical business ecosystem. In other words, there lacks an effective symbiotic mechanism between the physical world and the digital world. Future development of the blockchain ecosystem inevitably requires mutually beneficial situations of symbiosis between the physical and digital economy.

IoT (Internet of Things) will be a major connection of both the physical world and also the digital world. On one hand, IoT can establish an efficient coordination mechanism between users and objects in the physical world, thus promoting efficiency and bringing benefits to various industries, in addition to a new "Wisdom Revolution". On the other hand, with a potential size of tens of billion possibilities and a high concurrency for transactions; IoT has the potential to create huge, high-value and steady streams of digital asset resources for blockchain. Meanwhile, this connection need of both physical and digital worlds will promote the establishment of a value system of digital assets and network credit, in order to achieve multilateral prosperity of both digital and physical ecosystems.

The SixDomainChain Platform is a decentralized public blockchain ecosystem for data exchange that integrates International Standards of IoT Six-Domain Model (ISO/IEC 30141) and reference architecture standards for distributed blockchain (SDChain Platform), which would operate on its own native blockchain (SDChain).

The design of SDChain gives full consideration to IoT characteristics and requirements of business ecosystem construction. In specific fields like issuance of digital assets, management of users' credits and identities, P2P communication, encryption algorithm, consensus algorithm, smart contracts, cross-chain smart contract model, market consensus incentives, decentralized Dapp (Distributed Applications) and fast access to new businesses, SDChain optimizes current blockchain infrastructure in depth. By seamlessly implementing the underlying SDChain blockchain infrastructure and IoT Application ecosystem, the SDChain Platform will create a business ecosystem with benign, rapid and sustainable development, enabling SDChain Platform to have a coexistence of tokens, blockchain and industrial IoT. A reliable blockchain ecosystem based on IoT digital assets will be established, and an efficient way to realise the circulation and value transformation of reliable digital assets will be formed as well. In this manner, SDChain will become a global benchmark for the integration of IoT and blockchain ecosystem."

6.3.6 "Wearables" (in IIoT)

This document makes reference to the Study Report on Wearables, see [60], by ISO/IEC JTC 1/SC 41/AHG 7 and highlights that there is a need to optimize standards on wearables to be developed especially in the context of IIoT solutions and services and to be integrated natively by means of communication and data.

Where wearables will remain active especially for IIoT human interaction to: cobots, robotics, logistics, aided operations, augmented reality, virtual reality and many other fields.

IEC TC 124, Wearable electronic devices and technologies, is developing standards in wearable devices although this report highlights the need that IIoT should work in close collaboration with a potentially also being established working group on wearables within or in liaison with ISO/IEC JTC 1/SC 41.

6.3.7 Compatibility requirements and model – for devices – within IIoT systems

This clause describes the development of the draft standard that was led by PJSC "Rostelecom", involving the specialists from The Bonch-Bruevich Saint Petersburg State University of Telecommunications and Kaspersky Lab, see [61].

"This ISO/IEC 30162 developed by JTC 1/SC41 describes the requirements and interaction models for Industrial IoT (IIoT) devices. The draft standard describes the IIoT devices compatibility issues, as well as the requirements for interoperability and co-existence.

The compatibility of IIoT equipment is defined as the degree with which the Industrial system, information resource or other entity of Industrial Internet of Things can exchange the information with other IIoT entities through special IIoT services or without it, and/or can provide the required functions in common software/hardware environment or network.

Based on this term, the following functional and non-functional compatibility aspects are defined, according to which the requirements of the IIoT systems can be established.

Functional requirements:

- Compatibility at the physical level (Physical aspect).
- Compatibility at the MAC level (Media Access Control (MAC) aspect).
- Compatibility at LLC level (Logical Link Control (LLC) aspect).
- Compatibility at the network level (Network aspect).
- Compatibility at the transport level (Transport aspect).
- Compatibility at the session level (Session aspect).
- Compatibility at the level of data presentation (Data Presentation aspect).
- Compatibility at the application level (Application aspect).
- Compatibility at the level of measuring and actuating devices. (Measuring and automation aspect)
- Compatibility at the semantic level (Semantic aspect).

Non-functional requirements:

- Version compatibility of the IIoT entity (Version aspect).
- Compatibility at the Quality of Service provisioning level (QoS management aspect).
- Compatibility at the security level (Security aspect).
- Compatibility at the legislative level (Compliance aspect).

In addition, the draft describes IIoT entities compatibility levels for various aspects. The following compatibility levels have been defined:

- Fully compatible.
- Compatible.
- Partially compatible.
- Incompatible.

It describes possible models and interoperability ensuring methods for various IIoT entities. In particular, there were defined models for different industrial equipment connection to a remote IIoT cloud service:

- direct industrial equipment connection to a cloud service through a dedicated IIoT controller;
- connection to the cloud through special IIoT gateways;
- connection of special industrial monitoring systems of industrial equipment operation to a cloud platform via the IIoT gateway.

The models of semantic and heterogeneous gateways of IIoT are given, which can be used for various application systems and protocols transformation and the semantic data interchange.

Thus, in the content part of the document this standard defines the requirements, by execution of which the developed IIoT entity can be considered as fully or partially compatible with other IIoT entities. The Appendix describes a possible solution for ensuring the interoperation of various IIoT entities in a shared environment."

6.4 Roadmap perspective analysis for future standardization work for IIoT

6.4.1 Future standardization work for IIoT as a vertical domain of the IoT

6.4.1.1 General – An "IIoT standardization roadmap"

A roadmap of intended IIoT standards could lead the way to generate the big picture on how to proceed with standardization. To this end, the following considerations should be taken into account.

– While the initiative may come from classical manufacturing and process industries adapting themselves to the industrial IoT, it should be clear that these initiatives should go for a close collaboration with the experts within the SDOs already in liaison to ISO/IEC JTC 1/SC 41 to this regard.

– To this conceptual idea, the base-work of classical standards should remain within those SDOs dealing with them as of today. Therefore, the initiative should be led by ISO, IEC, IEEE, OMG, IETF, etc. – and the ISO/IEC JTC 1/SC 41/AG 20/SLG 1 IIoT participates as of its mandate about getting these initiatives and synchronizing them to initiate the generation of appropriate useful IIoT standards within the counterpart SDOs and vice versa.

– Technically capable, i.e. ISO/IEC JTC 1/SC 38 on "big data" as needed by, for example, IEC SC 65 or ISO/TC 184 or ISO/IEC JTC 1/SC 42 on AI to the same motivation.

– The timespan to start this roadmap in light of the paradigm shift to this intention is short, but it will take a long time (maybe decades) to finally achieve a 100 % execution: But this should not inhibit these organizations from getting started soon and now.

– This is especially the case for the integration of IT/OT standardization concepts and for a seamless data flow between all these instances.

– More to this all stakeholders like machine manufacturers, system builders, ICT specialists, system integration companies, IT and OT OEM companies, should work together in all these old as well as new SDOs, non-SDOs and FOSS initiatives.

It is highly recommended to define an IIoT reference architecture model within ISO/IEC JTC 1/SC 41 maybe within AG 20/SLG 1, see [62].

6.4.1.2 Standards for Industrial IoT- "ecosystems"

This document identifies that especially in regard of "ecosystems" between different implemented reference architecture models (RAM) and the appropriate standards, it would be meaningful to standardize ecosystems (i.e. cloud-, fog-, edge-, etc. "ecosystems"). Some national initiatives (i.e. by DIN, NC of Germnay) are leading the way.

This also in special regard of necessary customer needs and requirements to ensure a proper interoperability by domains through their internal representative existing protocols and standards – already defined by SDOs and non-SDOs as well as with open source and other industrial collaboration and consortia. This in common especially to the future development.

6.4.1.3 Standards for "integration of legacy systems" into IIoT

This document identifies further that the integration of existing legacy systems only by standard gateways may not be an appropriate solution in regard to avoiding "double standardization".

This document identifies to build "Brownfield/Greenfield integration standards" which indicates the appropriate way to operate:

One of these standards is as a positive example already initiated by the new work item proposal by Russian Federation ISO/IEC NP 30162 on "Compatibility requirements and model for devices within industrial IoT systems"

6.4.1.4 "Upgradeability" of IIoT systems

This document indicates the ongoing and very fast expanding activities worldwide with respect to Industrial IoT standardization efforts, also along the life cycle of IIoT systems. Plus, there would be a need for "upward" and "downward" compatibility between different maturity grades / stages of implementations along that timeline to become "compatible". This is surely one of the strongest challenges this document has identified for standards as being at risk of "non-interoperability", or "non-coexistence".

6.4.1.5 "Interoperability" of IIoT standards

This document identifies also that the same risks as with "upgradeability" apply also to "interoperability" between existing and new IIoT standards. Therefore, it should be noted that further work on this is already done within new revisions of the already mentioned NRM I4.0 Rev. 4.0 by NC of Germany to IEC (DKE), together with DIN.

6.4.1.6 "Integral safety and security" of IIoT systems

As an identified IT and OT "common perspective" for the IIoT, this document identifies (data-) security standards along ISO/IEC JTC 1/SC 27 work to be one of the most appropriate and well-known, and also with a wide degree of acceptance around the IT industry.

Also becoming more necessary to the OT World (as championed in IEC TC 65) and therefore there is direct collaboration between ISO/IEC JTC 1/SC 41/AG 20/SLG 1 IIoT and ISO/IEC JTC 1/SC 27 in their liaison to IEC TC 65 and ISO/TC 184 – including JWGs between the two organizations.

Safety standards on the other side are in the primary scope of the OT World – i.e. IEC 61508 by IEC TC 65/SC 65A.

With the advent of OT near edge "fog" device and the more IT-centric cloud infrastructure, it becomes obvious that a federation across these standards should become a driving point for future standardization.

Therefore, current projects, e.g. on "Cloud Federation" as ongoing by DIN, NB of Germany (i.e. DIN SPEC 92222), should go also for a deeper look and work on security and safety aspects in their work especially in internationalization by global SDO ISO/IEC in close collaboration also with non-SDO and FOSS initiatives afterwards.

The detailed aspects of trustworthiness within this document have been listed by the work in ISO/IEC JTC 1/SC 41/SG 8, Trustworthiness.

6.4.1.7 Consideration on a unified IIoT master data management

6.4.1.7.1 General

By this document it is identified that: "unifying the master data management" will become mandatory for the success of IIoT.

6.4.1.7.2 "Sync" standards for "Common Data Dictionaries" on IIoT

ISO/IEC JTC 1/SC 41/AG 20/SLG 1 IIoT holds the mandate to interact and communicate between the different SDO entities in liaison also about the synchronization on "data handling" in IIoT in syntax (procedural) and semantics (more important as analysed above).

6.4.1.7.3 "DDS" (Data Distribution Services) vs. OPC-UA – data exchange

There are some discussions ongoing today between different use case / IIoT application stakeholders on setting standards for data processing concepts:

One of the regarded initial statements by the OMG is the following:

From definition of DDS by OMG, see [63]:

> "Many real systems include devices, servers, mobile nodes, and more. They have diverse communication needs, but it's better – and easier – to use a single communication paradigm when possible.
>
> System designers should determine which of the protocols meets the primary challenge of their intended applications. Then, if possible, extend that primary choice to all aspects of the system.
>
> For example, inter-device data use is a different use case from device data collection. Requirements for turning on your light switch (best with CoAP) are much different than the requirements for managing the generation of that power (best with DDS), monitoring the transmission lines (best with MQTT), or communicating power usage within the data center (best with AMQP).
>
> …
>
> DDS: It can manage tiny devices, connect large, high-performance sensor networks and close time-critical control loops. It can also serve and receive data from the cloud.
>
> DDS communication is peer-to-peer. Elimination of message brokers and servers simplifies deployment, minimizes latency, maximizes scalability, increases reliability, and reduces cost and complexity. Using DDS does require building a data model and understanding data-centric principles. It is ideal for IoT applications that require a lasting, reliable, high-performance architecture."

6.4.1.7.4 Open repositories for "systems of systems" in IIoT

With an open repository of "systems of systems" the development of IIoT standards could lead to a more efficient way of Data Science based processing between different implementations and will lead to a better implementation by means of standard based interoperability and co-existence.

This document therefore recommends to keep this task in an IIoT WG to track and report between future plenary meetings.

6.4.2 ISO/IEC collaboration in relation to IIoT

6.4.2.1 General

Identified work and exchange for IIoT by JTC1 / AG 20 is planned for further development on IIoT standardization together with the following listed entities:

- ISO/IEC JTC 1/SC 7 ("Software and systems engineering")
- ISO/IEC JTC 1/SC 27 ("IT Security techniques")
- ISO/IEC JTC 1/SC 37 ("Biometrics")
- ISO/IEC JTC 1/SC 40 ("IT Service Management and IT Governance")
- ISO/TC 10 ("Technical product documentation")
- ISO/TC 39 ("Machine tools")
- ISO/TC 39/ SC 10 ("Safety")
- ISO/TC 184 ("Automation systems and integration")
- ISO/TC 184/ SC 1 ("Physical device control")
- ISO/TC 184/ SC 4 ("Industrial data")
- ISO/TC 184/ SC 5 ("Interoperability, integration, and architectures for enterprise, systems and automation applications")
- ISO/TC 211 ("Geographic information/Geomatics")

- ISO/TC 261 (“Additive manufacturing”)
- ISO/TC 292 (“Security and resilience”)
- ISO/TC 299 (“Robotics”)
- ISO/TMBG/SMCC “ISO Smart Manufacturing Coordinating Committee”
- IEC TC 65, including
  - TC 65/WG 23,
  - IEC TC 65/SC 65A,
  - IEC TC 65/SC 65B,
  - IEC TC 65/SC 65C
  - IEC TC 65/SC 65E
- IEC SyC SM (“Smart Manufacturing”)
- IEC TC 3/SC 3D “Product properties and classes and their identification”
- IEC TC 3 “Information structures and elements, identification and marking principles, documentation and graphical symbols”
- IEC TC22 “Power electronic systems and equipment”

6.4.2.2 IEC ACSEC advisory committee on information security and data privacy

Scope: ACSEC deals with information security and data privacy matters which are not specific to one single technical committee of the IEC. It coordinates activities related to information security and data privacy and provides advice to the SMB on those subjects. ACSEC provides guidance to IEC TCs and SCs for implementation of information security and data privacy in a general perspective and for specific sectors. ACSEC also provides a venue for exchanging information between the IEC and other SDOs relevant to ACSEC’s scope. ACSEC follows closely research activities and trends in Academia.

6.4.2.3 ISO/TC 307 Blockchain and distributed ledger technologies

As the blockchain technology has become highly recognized in the entire field besides standard payment and finance transactions – a liaison should be taken into regard by 3rd Plenary Decision.

This document indicates further also to taking the reference of work in use of ISO/IEC 30141 as being the base of SDChain Initiative as recommended.

- ISO/TC 307 Blockchain and distributed ledger technologies
- ISO/TC 307/SG 2 Use cases
- ISO/TC 307/SG 6 Governance of blockchain and distributed ledger technology systems
- ISO/TC 307/SG 7 Interoperability of blockchain and distributed ledger technology systems
- ISO/TC 307/WG 1 Foundations
- ISO/TC 307/WG 2 Security, privacy and identity
- ISO/TC 307/WG 3 Smart contracts and their applications

Currently there are diverse PoC (proofs-of-concept) running in IIoT related SDO, Consortia, FOSS and other initiatives on blockchain for different use cases in IIoT [like Security, AAA (Authentication, Access, Authorization)] which shows the immense significance of the horizontal technology – therefore this document indicates the necessity to foster the standardization in this key field for IIoT.

This document indicates further that there is still a big challenge to identify the real capabilities and use cases on blockchain in IIoT because of unsolved problems on

– scalabililty,
– performance,
– optimization

in light of the open-book like nature of a distributed ledger (blockchain).

6.4.2.4 "Data management" and exchange of data – in IIoT

Data management and interchange is a key field of IIoT operation and therefore standards should be kept in strong and sustained development.

Identified relevant standardization is done within:

ISO/IEC JTC 1/SC 32 – Data management and interchange

Scope: Standards for data management within and among local and distributed information systems environments. SC 32 provides enabling technologies to promote harmonization of data management facilities across sector-specific areas.

Specifically, ISO/IEC JTC 1/SC 32 standards include:

– reference models and frameworks for the coordination of existing and emerging standards;
– definition of data domains, data types, and data structures, and their associated semantics;
– languages, services, and protocols for persistent storage, concurrent access, concurrent update, and interchange of data;
– methods, languages, services, and protocols to structure, organize, and register metadata and other information resources associated with sharing and interoperability, including electronic commerce.

6.4.2.5 ISO/IEC JTC 1/SC 38, Cloud computing and distributed platforms

Cloud computing is also identified as a key field of IIoT technology operations and therefore standards should be kept in strong and sustained development.

Especially in regard to the conceptual "companions" of cloud computing and its federation, (especially edge- and fog- computing across and between (horizontal) as well in the vertical infrastructure of the IIoT) – focus should be on very good optimization and synchronization between the open source on the IT-related and the adjunct OT side (mostly IEC and ISO TC related SDO initiatives) under an umbrella of the conceptual idea in IIoT.

6.4.2.6 ISO/IEC JTC 1/SC 42, Artificial Intelligence

AI is a further key field of IIoT technology operations and therefore standards should be kept in strong and sustained development.

Ref.: Scope: Standardization in the area of Artificial Intelligence

– ISO/IEC JTC 1/SC 42/WG 1 Foundational standards
– ISO/IEC JTC 1/SC 42/WG 2 Big data
– ISO/IEC JTC 1/SC 42/WG 3 Trustworthiness
– ISO/IEC JTC 1/SC 42/WG 4 Use cases and applications
– ISO/IEC JTC 1/SC 42/WG 5 Computational approaches and characteristics of AI systems

Serve as the focus and proponent for JTC 1's standardization program on Artificial Intelligence.

Provide guidance to JTC 1, IEC, and ISO committees developing Artificial Intelligence applications.

Annex A
(informative)

Listing of all SDOs, non-SDOs, consortia, FOSS (free open source systems) in context of the IIoT mentioned in this document

A.1 SDOs recognized/identified as of interest to IIoT and also in relation to Clause 5 on standardization landscape in IIoT

A.1.1 General

Many standards are being developed or at least the requirements from different scopes are being defined and recommended in this wide field of industrialization applying the enabling IoT technologies and services.

The standards and projects in Clause A.1 are listed with the best information available at the time of the development of this document.

A.1.2 3GPP 3rd Generation Partnership Project

By own description: The 3rd Generation Partnership Project (3GPP) on: http://www.3gpp.org/ unites the seven telecommunications standards development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as “Organizational Partners,” and provides their members with a stable environment to produce the reports and specifications that define 3GPP technologies.

Relevance to IIoT: Regarding IIoT, the 3GPP covers the appropriate technical standards for the next generation 5G network which has special attention to factory automation.

The portfolio of technologies that 3GPP operators can now use to address their different market requirements includes the following:

1) eMTC (enhanced machine-type-communication)

   Further LTE enhancements for machine type communications is building on the work started in Release-12 (UE Cat) – all this enabling new and better IIoT related communication abilities (M2M, Smart Manufacturing).

2) NB-IoT

   New radio added to the LTE platform optimized for the low end of the market

   Stand-alone: Utilizing stand-alone carrier, e.g. spectrum currently used by GERAN systems as a replacement of one or more GSM carriers.

   Guard band: Utilizing the unused resource blocks within an LTE carrier’s guard-band. This may apply especially in areas of factory automation and therefore touches future IIoT developments for communication layer purposes.

   In-band: Utilizing resource blocks within a normal LTE carrier. This may also be of interest for future intervention and analysis for IIoT communication applications.

3) EC-GSM-IoT

   EGPRS enhancements in combination with PSM make GSM/EDGE markets prepared for IoT applications.

A.1.3 ETSI (European Telecommunication Standards Institute)

Name: **ETSI (European Telecommunication Standards Institute)**

Ref.: www.etsi.org
Ref.: 3gpp.org

Description: ETSI produces globally-applicable standards for information and communications technologies (ICT), including fixed, mobile, radio, broadcast and Internet technologies. Its standards enable the technologies on which business and society rely. For example, its standards for GSM™, DECT™, Smart Cards and electronic signatures have helped to revolutionize modern life all over the world.[2]

Areas of interest for IoT in ETSI include, but are not limited to:

– standards updates on IoT services enabling technologies (oneM2M and ETSI TC SmartM2M, ISG CIM, etc.);
– standards updates on IoT enabling communication technologies (e.g. 3GPP NB-IoT and 5G, LoRa, Sigfox, etc.);
– standards updates on IoT security and privacy;
– standards and research activity in the area of semantic and ontology-based interoperability; and
– FOSS open source (I)IoT projects.

Relevance to IIoT: the Wireless Industrial Real Time Communication in collaboration with 3GPP/5G and AIOTI/WG3 (WG11).

A.1.4 IEEE (Institute of Electrical and Electronics Engineers)

A.1.4.1 General

Ref.: www.ieee.org

Relevance to IIoT: IEEE does cover many technical/physical standard developments with high relevance for both wired and wireless communication systems.

Regarding IoT, IEEE described in its working paper, “Towards the Internet of Things (IoT),” its many intentions to further IoT-related work within IEEE. (Pub. 2015)

IEEE Standards focus mainly on horizontal technologies – primary physical layer-communication:

– IEEE 802.11 Series
– IEEE 802.1 Series
– IEEE 802.3 Series (Time-Sensitive Network, TSN)

Especially in regard to OPC UA, most of the physical layer is defined by IEEE standards:

Recommendation for further collaboration or exchange of information regarding future developments of IIoT.

---

2 GSM and DECT are trademarks of the GSM Association and ETSI, respectively. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC.

Today there is already a very long list of identified projects by IEEE relevant to IIoT, and its reference architecture models have already been summarized by the German national body (DIN) in RAMI 4.0 reference model.

The projects listed below are of interest to the IIoT, yet it is not a complete list in the context of SM/IIoT:

– IEEE Standard Ontologies for Robotics and Automation;
– IEEE Standard for System and Software Verification and Validation;
– IEEE Standard Adoption of ISO/IEC 15026-1;
– Systems and Software Engineering;
– Systems and Software Assurance – Part 1: Concepts and Vocabulary;
– ISO/IEC/IEEE 15288: Systems and software engineering – System life cycle processes;
– IEEE Guide for the Use of Artificial Intelligence Exchange and Service Tie to All Test Environments; and
– Project: (AI-ESTATE).

A.1.4.2 IEEE P2413 – Standard for an Architectural Framework for the Internet of Things (IoT)

The Internet of Things (IoT) is predicted to become one of the most significant drivers of growth in various technology markets. Most current standardization activities are confined to very specific verticals and represent islands of disjointed and often redundant development. The architectural framework defined in this standard will promote cross-domain interaction, aid system interoperability and functional compatibility, and further fuel the growth of the IoT market. The adoption of a unified approach to the development of IoT systems will reduce industry fragmentation and create a critical mass of multi-stakeholder activities around the world.

A.1.5 ISO/IEC

A.1.5.1 General

International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC).

Ref.:

http://www.iso.org
http://www.iec.ch

These two organizations are the parent organization of JTC 1. The JTC 1 Subcommittee 41 (SC 41) is the JTC 1's main SC standardizing the IoT technologies and related fields.

The committees listed in A.1.5 have generated different reports in relation to Smart Manufacturing, global advanced industrial systems (GAIS), and further analysis which influences future industrial IoT systems' standard development.

Subclauses A.1.5.2 to A.1.5.9 detail the result of the work of ISO and IEC committees and joint cooperation between IEC and ISO.

A.1.5.2 ISO/GAIS

Reconstitution of the JAG Group on Global Advanced Industrial Systems (GAIS)

This document is the result of an input and discussion process initiated by the first and second meetings of participating members of the reconstituted JAG 60 Recommendation #14 from the JAG Meeting in March 2017, convened by DIN, NB of Germany.

This document also contains material gathered from reports on Smart Manufacturing, industrial IoT research projects, ICT projects and group output from the ISO/IEC JTC 1/WG 10 meetings regarding Smart Manufacturing and industrial IoT relevant findings and materials as well as contributions by national bodies within ISO/IEC JTC 1/WG 10 as one of predecessors of ISO/IEC JTC 1/SC 41 IoT.

Standardization for Advanced Industrial Systems Tools and Services is found in, but is not limited to, the following documents:

– ICT aspects of Advanced Industrial Systems and Smart Machines;
– Digital Manufacturing and Machinery;
– Cloud Manufacturing, Intelligent Manufacturing; and
– Agile Manufacturing and Lean Manufacturing.

The ICT aspects of Advanced Industrial Systems and Smart Machines principles can be found in:

– the reports of IEC/SG 8 “Industrie 4.0 – Smart Manufacturing;”
– ISO/SAG “Industrie 4.0/Smart Manufacturing;”
– the final report of GAIS on Global Advanced Industrial Systems (GaIS);
– looking for opportunities for Advanced Industrial Manufacturing AIM; and
– “Smart Machines” within JTC 1.

A.1.5.3 ISO/IEC JTC 1/SC 41/SLG 1 Sectorial Liaison Group (SLG) on IIoT – (AG20)

Definition: JTC 1/SC 41/SLG 1 on IIoT is a Sectorial Liaison Group with the following mandate, having its scope on IoT for Smart Manufacturing, industrial facilities and related areas, in order to exchange the information on IIoT related standardization across all identified SDOs of this document.

– Coordinate liaison activities between all SDOs, internal and external, in the IIoT sector and JTC 1/SC 41.
– Proactively solicit requirements and use cases, when applicable, from the SDOs under its responsibility.
– Promote the use of JTC 1/SC 41 foundational and core standards by these SDOs.
– If required, assist in the socializing of NWIPs that appear to be relevant to the scope of one or more SDOs within their sector.
– If required, facilitate the set-up of joint projects between these SDOs and JTC 1/SC 41.
– Responsible committees in Scope of AG 20 SLG 1 IIoT are:

• IEC TC 65	Industrial-process measurement, control and automation
• ISO TC 184/IEC TC 65 JWG 21	Smart Manufacturing Reference Model(s)
• ISO TC 184/ SC 1	Physical device control
• ISO TC 184/ SC 4	Industrial data
• ISO TC 184/ SC 5	Interoperability, integration, and architectures for enterprise systems and automation applications
• ISO TC 39	Machine tools
• ISO TC 261	Additive manufacturing
• ISO TC 299	Robotics

- ISO TC 261 Additive manufacturing
- ISO TC 10 Technical product documentation
- IEC SyC SM Smart Manufacturing

The initial work of AG 20 SLG1 covers many findings of the analysis and work performed in the former JTC 1/SG 9 Report on IIoT in this document summarized by the following listed aspects:

– re-configurability and pluggability of IIoT systems;
– future standardization on: “microservices and micro-applications in IIoT”;
– IIoT connectivity and Interoperability;
– standards for Industrial IoT “ecosystems”; and
– edge- fog- together and in context with cloud-computing aspects of IIoT.

Therefore, JTC 1/SC 41/AG 20 SLG1 acts as the primary focus group related to all the liaisons of JTC 1/SC 41, with the primary intention to synchronize all standardization work across those JTC 1/SC 41 Category A to C liaisons in the context of vertical as well as horizontal aspects of the Industrial IoT.

A.1.5.4 IEC systems committee on Smart Manufacturing

Definition: Systems committee on Smart Manufacturing

Mandate: To provide coordination and advice in the domain of Smart Manufacturing to harmonize and advance Smart Manufacturing activities in the IEC, other SDOs, and consortia according to Clause 2 in AC/22/2017 (Transparency of SyC work to TCs and other groups).

As a priority since the IEC Strategic Group 8 formation in 2014, the resulting Standardization Evaluation Group 7 (SEG 7) – Smart Manufacturing, has continued to be focused on an IEC strategy addressing manufacturing enterprise operations to ensure that the real-time data needs of the manufacturing enterprise are sustained to achieve safe, secure, energy efficient and productive operations within the context of a connected Smart Manufacturing enterprise.

In its work, SEG 7 studied many architectures for Smart Manufacturing that will enable it to function as a smart application within a broad IoT environment; and to leverage the adoption of current and next generation technologies to achieve safe and secure factory operations.

To understand the future requirements of Smart Manufacturing, SEG 7 sought to:

– analyse market and industry developments,
– identify gaps and overlaps in the standards portfolios of IEC and ISO and other SDOs,
– make sure that appropriate standards are delivered in a timely manner,
– define a structure for collaboration between standardization organizations (notably ISO and IEC), and
– monitor the practical application of collaborations already in place.

Smart Manufacturing ecosystems use multiple value chains to support their goal of delivering productivity and efficiency to meet their specific manufacturing enterprise business goals.

Smart Manufacturing enterprises comprise one or more organizations which operate in various industry sectors, e.g., automotive, aerospace, chemical, energy, semiconductor, oil and gas.

These enterprises may utilize management system standards which are the domain of ISO, in addition to many other business functions and processes which are the domain of other SDOs and which support the manufacturing automation function which is largely in IEC domains.

The ICT infrastructure for the “office management” of the enterprise is supported by standards produced within ISO/IEC JTC 1.

The manufacturing execution function is the domain of ISO/TC 184 and IEC TC 65, while the control and automation centre is largely standardized within IEC TC 65.

The machinery and process equipment are the domain of ISO committees, while the sensors and actuators on the equipment are the domain of IEC standards.

The whole enterprise needs to have a seamless set of standards to ensure that safety, security, environment, energy and EMC are not compromised, which are in the standards domain of both ISO and IEC.

Coordinated access to critical data (as defined by ISO 8000 data quality standard) at every key point of decision making within the system, whether it be by machine or person, will lead to improved decisions and resulting actions that should optimize the performance of the enterprise according to the desired business operation strategy.

Most of the standards that exist today have been developed in the traditional “silos” of product or business functions, and there has been little focus on the connected value streams and interdependent data needs of the devices or functions within these value streams.

The bi-directional flow of data will necessitate interfaces to be developed within the existing standards portfolios of many IEC and ISO TCs that make up a manufacturing enterprise and consequently, increased collaboration and partnership is anticipated in the future to facilitate the reality of a smart enterprise.

The ultimate goal of Smart Manufacturing is to interconnect every step of the manufacturing business processes and integrate the manufacturing function with the other business functions that make up a manufacturing enterprise.

For the purposes of harmonizing and advancing Smart Manufacturing activities in the IEC, SEG 7 (now disbanded) proposed to the SMB in its report, SMB/6235/R to establish a new systems committee on Smart Manufacturing as justified by the market overview, business case and national initiatives. IEC SyC SM on Smart Manufacturing was established in 2018/11.

A.1.5.5 ISO SMCC

ISO “Smart Manufacturing Coordinating Committee” (ISO SMCC), see [64]

Definition – From normative roadmap NRM I4.0 Rev. 3.0 of Standardization Council Industrie 4.0 (SCI 4.0) – 2018-04-27 Release / Section 2.3.1:

> "In September 2016, the ISO Strategy Group Industrie 4.0 successfully completed its work. In order to continue its international activities, the ISO SMCC was set up as its successor body. In the first instance, it will remain in existence for two years and will comprise representatives from the relevant technical committees. Representatives were nominated from a total of 21 ISO committees, in addition to one representative each from the IEC and the ITU, to take part in the collaboration.
>
> Under German leadership, the ISO SMCC has since been the driving force behind the work being carried out on an international level on Industrie 4.0. The aim is to ensure the overarching coordination in that area and to draw up implementation recommendations, especially with regard to a joint international approach. At the same time, a national mirror committee was set up as a means of offering interested parties a national platform that would enable them to take part in the shaping of the work being undertaken on an international level."

Workplan of ISO SMCC and IEC SEG is to work on the definition of Smart Manufacturing. Here is the current definition from ISO/IEC:

“Manufacturing that improves its performance aspects with integrated and intelligent use of processes and resources in cyber, physical and human spheres to create and deliver products and services, which also collaborates with other domains within enterprises’ value chains.

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.”

Focus is on the result of the work of ISO/IEC Smart Manufacturing Standards Map – Joint Working Group

A.1.5.6 ISO/TC 184

Scope: Standardization in the field of automation systems and their integration for design, sourcing, manufacturing, production and delivery, support, maintenance and disposal of products and their associated services. Areas of standardization include information systems, automation and control systems and integration technologies.

ISO/TC 184 ToR Proposal in the context of IIoT:

The JWG21 is tasked to prepare a standardized unified Reference Model to support ISO and IEC activities in Smart Manufacturing, which shall comprise either:

– a single model with multiple consistent views/projections, or
– a set of consistent and coherent models in order to support the requirements of stakeholder groups, including:
– industrial users,
– systems suppliers and integrators, and
– standardizers.

The JWG21 shall take account of available standardized reference models for industrial automation

A.1.5.7 IEC TC 65, see [65]

Scope: To prepare International Standards for systems and elements used for industrial-process measurement and control concerning continuous and batch processes. To coordinate the standardization of those features of related elements which affect suitability for integration into such systems. The work of standardization outlined above is to be carried out in the international fields for equipment and systems operating with electrical, pneumatic, hydraulic, mechanical or other systems of measurement and/or control.

IEC TC 65(A-E) Work analysed in context of IIoT:

Much of the work of IEC TC 65 and its subcommitees is found and reflected heavily by referencing of its standards in the reference architecture in IIoT around the world.

Scope of IEC TC 65 for JWG 21:

“Development of Smart Manufacturing Reference Model(s) that shows technical objects (assets), different aspects related to their life cycle and their technical and/or organizational hierarchies and development of a basic architecture of Smart Manufacturing components as essential parts of the virtual representation of objects (assets).”

See also Figure A.1.

Also, to be recognized: Work of WG 16 in IEC TC 65 on the "Digital Factory":

IEC 62832 is a reference model for representation of production facilities (Digital Factory):

– Part 1 is a general introduction to the model and principles of the DF framework;
– Part 2 is a detailed data model for all the concepts of the DF framework;
– Part 3 provides an application description of how the DF Framework is used to manage the life cycle of a production system;
– Part 4 provides an information exchange model description of how data is migrated into the DF framework.

A.1.5.8 ISO/IEC joint initiatives/commitees (ISO/TC 184 and IEC TC 65) JWG 21 in Smart Manufacturing – IIoT Scope

The scope of Smart Manufacturing is wider than those of ISO/TC 184 and IEC TC 65, and it also contains scopes of other TCs. It is proposed that ISO/TC 184 / IEC TC 65 JWG 21 uses the mechanisms of ISO SMCC and IEC SEG 7 (or its successor) to interact with the other affected TCs.

Most of the organizations dealing with digitizing industry need to clarify the relevance and the mutual positioning of the related standards because:

– there are numerous (thousands of) standards,
– they are published by several bodies that have their specific terminology, so the scope and purpose of the standards might be unclear for others,
– they may be overlapping or lacking coverage,
– SDOs do not provide catalogues with features like any other product catalogue has.

The FR contribution to the call IEC TC 65 – 65/650/DC is the basis for the project "Smart Manufacturing Standards Landscape".

This contribution is already a proposal that aggregates important previous existing publications:

– "Big Picture" from ISO/TC 184;
– "RAMI 4.0" from the Industrie 4.0 German initiative (IEC TC 65: IEC PAS 63088);
– "Standards Landscape for Smart Manufacturing" from NIST;
– the report from ISO/SAG Smart Manufacturing;
– the report from IEC SG 8 Industrie 4.0/Smart Manufacturing.

There are already an analysis and requests to amend the FR contribution coming from Japan.

Joint Scope ISO TC 184/IEC TC 65 JWG 21: To develop standards for Smart Manufacturing reference model(s), either consistent models or equivalently a unified model with consistent views/projections, as demanded by the variety of Smart Manufacturing phases, the intersecting and often concurrent design, resources availability/appropriation, deployment and business life cycles, the end products life cycles, the requirements by end users, and the connectivity between all the above entities. (IEC TC 65 – 65/650/DC)

ISO TC 184/IEC TC 65 JWG 21 works on the differentiation or changes from manufacturing to Smart Manufacturing with following key points:

– Service orientation.
– Product as a part of the automation solution.

- Vertical interoperability (integration, federation, etc.) – New aspects are passive objects/assets, the product itself speaks with the equipment, Internet and cloud technologies).
- Horizontal interoperability (integration, federation, etc.): logistics, conceptualization, design, procurement, construction, commission production, development, etc.
- Elimination of offline processing in favour of inline processing by technologically advanced devices capable of computational work at point of value creation.
- Interaction and cooperation across and between all whole life cycles – from internal value chains to value network partners.
- Data, information and knowledge exchange inside and outside of organizations (companies) including more OT/IT exchange.
- New communication – Each object/asset can talk with each other object/asset.
- New business models available out of data.
- Self-improvement adaptive system including human in a loop.
- Cyber physical systems (CPS) approach.
- New IT "driving" Smart Manufacturing.
- Coexistence of real things and their digital twin.
- Cultural change of the organization resulting from the refined role of humans in the manufacturing process.
- Technical solution for legal issues, e.g. negotiations between two machines, data privacy, etc.
- Interoperability facilitated by system(s) characterized by their standardized capabilities.

Figure A.1 shows the structure of IEC TC 65 and ISO/TC 184, from ISO TC 184/IEC TC 65 JWG 21 Initial Report:

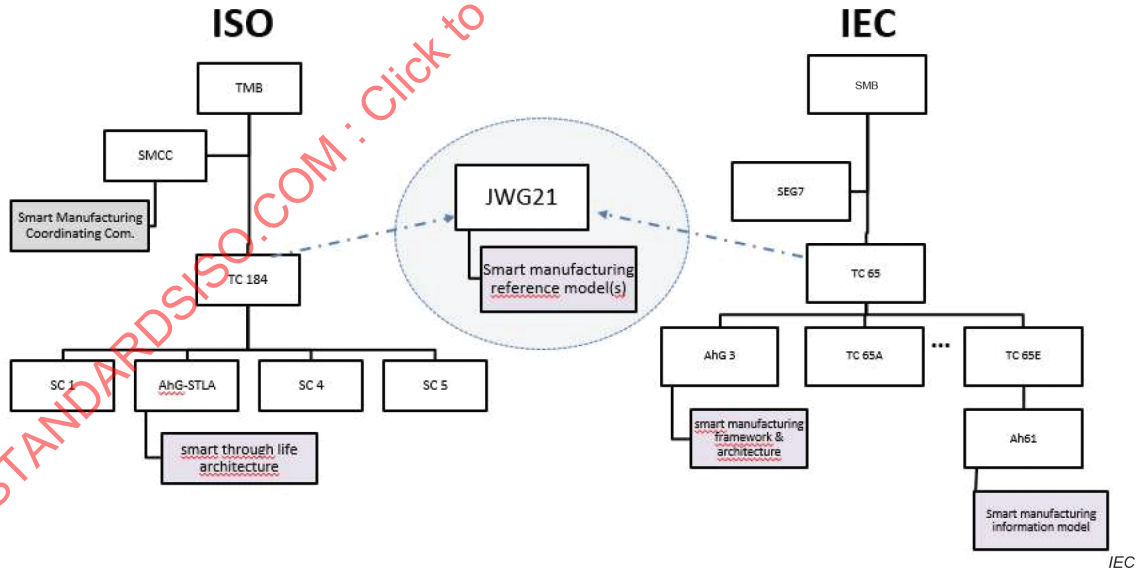


Figure A.1 – Structure of IEC TC 65 and ISO/TC 184 JWG 21

Another new 2018/11 Joint Initiative between ISO SMCC and IEC SyC SM in regard to the synchronization and harmonization on standardization relevant to Smart Manufacturing – also in relation to Industrial IoT related concepts – on a Board and steering level is the newly (2019) formed Task Force ISO/IEC SM2TF, see [66]. See Figure A.2.

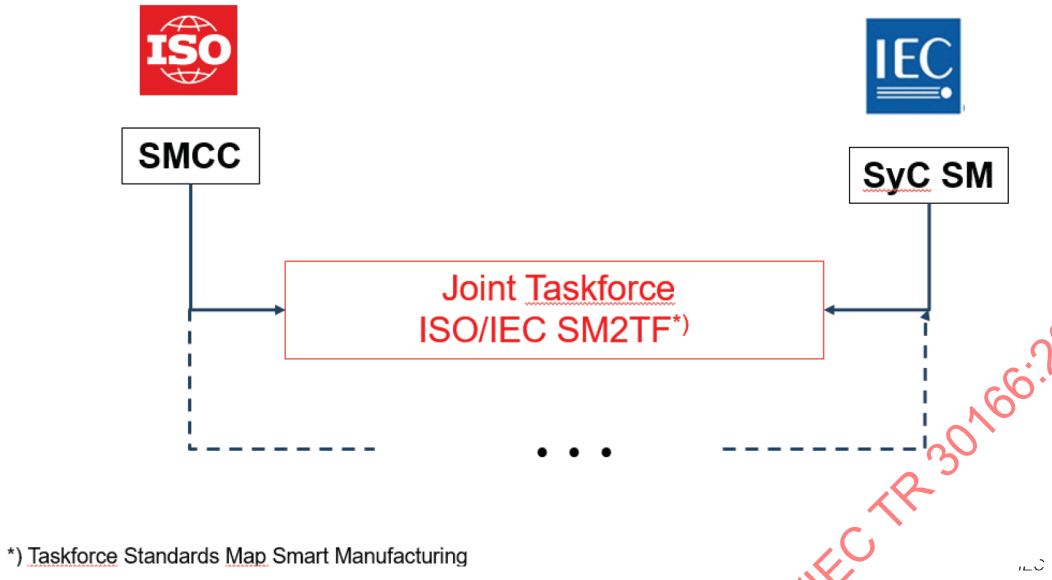


Figure A.2 – ISO/IEC Taskforce Standards Map Smart Manufacturing

Founded with the following terms and references:

To build a standards map on Smart Manufacturing in three phases of work steps.

Phase 1:

– Generate and organize a definitive list of Smart Manufacturing-relevant standards from committees participating in SMCC and IEC, taking into consideration the work done to date (e.g. ISO SAG on Industrie 4.0/Smart Manufacturing output, ISO/TC 184 "Big Picture", IEC TC 65 AhG3; IEC SEG 7).
– Identify additional relevant Smart Manufacturing standards from other SDOs, including consortia and national initiatives.
– Provide an initial classification to facilitate navigation and understanding of the content.
– Publish the output of Phase 1 as an ISO/IEC Technical Report, and issue periodic updates.

Phase 2:

– Classify the contents of the standards map according to existing reference models and the unified reference model resulting from ISO TC 184/IEC TC 65 JWG 21.
– Republish the resulting output in a maintained database format.

Phase 3:

– In collaboration with the IEC SRG work to maintain the smart energy standards map, and with bodies developing other standards mapping tools (for example the standard mapping tool referred to in ISO/TC 184 resolution 563), develop a concept to represent the content of the standards map in a smart, graphically supported way to meet the needs of market users and standards developers.
– Define a business case to publish the content of the standards map according to this concept.
– Provide a recommendation to ISO/TMB and IEC SMB to support the realization and maintenance of the standards map project.

A.1.5.9 IEC SEG 8 – followed by SyC SM (Smart Manufacturing)

The key objectives of IEC SEG 8, which has been disbanded, included:

- Monitor new or emerging communication technologies and architectures that are specified or standardized outside the IEC (e.g. 5G, Low Power Wide Area Networking, Deterministic Networking, Edge Computing/Intelligence, Management and Orchestration, and others).
- Monitor new market trends (e.g. IT/OT convergence) and analyse new business and development models (e.g. Open Source, DevOps) related to communication technologies and assess their impact on IEC activities.
- Take into account additional essential aspects of communication technologies such as security, reliability, safety, privacy, energy efficiency, and others.
- Evaluate the impact of these technologies, architectures and trends on current and foreseen IEC work, in particular on systems related activities, and engage with the concerned IEC committees by raising awareness and making technical recommendations.
- Be the IEC focal point for spectrum management related issues and coordinate with ITU-R and regional spectrum policy organizations. (see also A.1.5.11 on ITU Organization / Subsections)
- Evaluate gaps in standardization of communication technologies based on requirements provided by selected IEC use cases and take appropriate actions within the IEC or through collaboration with external bodies.

SEG 8 was organized into three active working groups to focus and accelerate the progress of specific deliverables:

- WG 1: Trend monitoring – which addresses market, business and technology trends and their impacts on IEC activities.
- WG 2: Collaboration – which addresses the collaboration within the IEC and with external bodies, as well as the evaluation of standardization gaps of communication technologies.
- WG 3: Spectrum policy – which addresses spectrum management related issues and coordinates with ITU-R and regional spectrum policy organizations.

A.1.5.10 IEC CDD (“Common Data Dictionary”)

Ref.: https://cdd.iec.ch

Description: IEC CDD is the only ISO/IEC-compliant semantic data dictionary (based on IEC 61360 and IEC 62656) with a free-of-charge offering for classification and unambiguous description of products and services for all industries.

IEC CDD is also providing unambiguous description and identification of UNITS (based on IEC 62720).

IEC CDD is provided by IEC and maintained by IEC SC 3D.

IEC SC 3D has a liaison with eCl@ss to avoid conflicting definitions of products and services.

A.1.5.11 ITU (ITU-T and ITU-R (Spectrum))

Name: International Telecommunication Union

Ref.: https://www.itu.int/en/Pages/default.aspx

Description: ITU (International Telecommunication Union) is the United Nations specialized agency for information and communication technologies (ICTs).

ITU allocates global radio spectrum and satellite orbits and develops the technical standards that ensure networks and technologies seamlessly interconnect.

Relevance to IIoT: ITU-T SG20 (IoT and Smart Cities and Communities) defined the IoT reference model in ITU-T Y.2060, which is also in relation to a Work Project by "WiSE-IoT" in regard to Network layer and service support and application support layer:

See also: http://wise-iot.eu/en/deliverables/

This is to ensure to gain recognition and information on relevant changes especially in regard to spectrum allocation by modern means for industrial automation scenarios focused on network-based wireless indoor use cases.

It is expected that spectrum allocation will become more and more important for factory automation aspects as well as for licensed bands and also unlicensed band use.

Developments in this regard by collaborations with national and local authorities in coordination with FCC and ETSI / 3GPP are ongoing.

A.2 IIoT related initiatives/engagements by national standardization bodies

A.2.1 General

Clause A.2 identifies the standardization activitivies of national bodies (NBs) from the publicly available materials.

In the past years with the advent of recognized Smart Manufacturing initiatives on the global market scale, there were many national bodies and governmental institutions engaging themselves together with local organizations, industrial consortia and associations to foster standardization in this new important field of activities beside the normal standardization progress.

The NBs often initiate study and report groups inside the NBs and/or their governmental institutions to start harmonization activities in industrial IoT, and these efforts are being recognized and mentioned herein as part of this report.

Clause A.2 is organized by the scope of the NBs' initiatives and also by taking a deeper look into these initiatives and linking them to the appropriate international standardization, and they are documented in Clause A.2. Each subclause lists the national initiatives which drives current development on Smart Manufacturing or Industrial IoT in their countries. The subclause title shows the country name and its initiative name.

A.2.2 Sweden – LISA

LISA – Line Information System Architecture (LISA)

Link: https://www.chalmers.se/en/projects/Pages/Line-Information-System-Architecture.aspx

The aim of this project is to develop a Line Information System Architecture (LISA) that can be used in industrial production systems in general and in automotive discrete manufacturing specifically. This architecture aims at capturing raw data from the plant of a production system and transforming these data into understandable and coherent information in order to ease production management decisions.

This document identifies the narrowed scope in IIoT related to Smart Manufacturing with respect to the sub-aspect Production in LISA.

Chalmers Production focuses on connected and sustainable production. This includes new resource and energy-efficient processes for manufacturing and development of new products and production systems. The research generates knowledge and tools in modelling,

simulation and optimization, combined with support for decision-making in close collaboration with industry.

It is a platform for research in manufacturing, production systems and product development with sustainability and future smart factories as common challenges. The philosophy is to influence early in the development process where many small improvements make great benefits in the end.

The Production Area of Advance congregates more than half of all Chalmers departments, five research centres and three other closely linked research environments, 25 research groups and a network of collaborating industries. The research is fundamentally based on science in mathematics, physics and/or chemistry.

Vision and Mission

Its vision is sustainable and innovative production, with respect to economical, ecological and social aspects – where industries, environment and members of society all benefit.

Its mission is to achieve excellence in scientific research and development – supporting sustainable and innovative production through knowledge, methods and tools.

This is realized by creating:

– development processes for innovative and competitive product and production systems, based on a life-cycle perspective;
– optimized production systems and manufacturing processes;
– minimized environmental impact through reduced waste of energy and natural resources;
– safe, healthy, and rewarding work environments; and
– world-class education in sustainable production.

Future sustainable competitive production systems need to be productive and flexible, as well as environmentally friendly and safe for the personnel. There are today few system solutions that assist production management with a coherent information model and a modular system architecture that facilitates data gathering regarding products and processes throughout the entire plant. To solve this problem the aim of this project is to develop a line information system architecture (LISA) that can be used in industrial production systems in general and in automotive discrete manufacturing specifically.

This document identifies the work of LISA as being of interest for future development and Industrial IoT; but due to its scope, the existing materials available today by LISA do not have an influence on a reference architecture – because an RA on IIoT is not identified therein.

A.2.3 France – “Usine du Futur”, see [67]

Definition of "Usine du Futur" – The concept of factory of the future "en France"

The Factory of the Future is a generic concept that is part of a general awareness of the importance of the manufacturing industry in the national wealth. This reflection is intended to conserve and develop in France and therefore in Europe, a strong, innovative industrial activity, an exporter, a generator of wealth and a creator of jobs.

The Factory of the Future is a response to several simultaneous transitions: energetic, ecological, digital, organizational and societal. Each of these transitions involves many new technologies or modes maturing, developing or designing. It is a question of continuing the modernization of the production tool and accompanying companies in the transformation of their business models, their organizations, their methods of design and marketing, in a world where digital tools are breaking down the industry divide and services.

Consideration by this document: A collaboration is today primarily focused in regard to reference architecture only by the direct agreement to join work in collaboration with the future development and adaptation of the RAMI 4.0 model by liaison:

Purpose of Liaison "Industrie 4.0" (Germany) and "Usine du Futur" (France)

In the Shared Action Plan of Plattform Industrie 4.0 and Alliance Industrie du Futur, published on April 26th, 2016, the work on common comprehensive scenarios describing the future of manufacturing addressing the customer needs was announced. Scenarios are defined as top down archetypical stories made possible by new manufacturing and digital technology.

A.2.4 Germany – Industrie 4.0, see [68]

German Initiative "Industrie 4.0 Standardization Roadmap" current version: 3

Link-Ref.: https://sci40.com/files/assets_sci40.com/img/sci40/german-standardization-roadmap-industry-4-0-version-3.pdf

National body DIN (ISO) in collaboration with DKE (IEC):

The aim of the future-oriented initiative Industrie 4.0 is to exploit the potential resulting from

– the extensive use of the Internet,
– the integration of technical processes and business processes,
– the digital mapping and virtualization of the real world, and
– the opportunity to create “smart” products and means of production.

This requires the development of a host of new concepts and technologies. It will, however, only be possible to implement these new concepts and technologies in industrial practice if they are backed up by standards based on consensus, as only such standards are able to create the necessary security for investments and confidence among manufacturers and users.

In order to address the standardization issues at an early stage, the Standardization Council Industrie 4.0 (SCI 4.0) was established with support of DIN and DKE.

In addition, the Labs network Industrie 4.0 (LNI 4.0) – is intended to set testbeds according to the standards and recommendations by SCI 4.0 in collaboration and exchange together with all participating parties (liaisons, standardization organizations, companies, corporations, alliances, by membership).

The fundamental task of SCI 4.0 is to develop the strategic, conceptual and organizational aspects of the topic of Industrie 4.0 from the point of view of standardization.

SCI 4.0 identifies concrete needs for standardization, coordinates their implementation and advances the development of fundamental concepts.

The Working Group “Standardization Roadmap” was established by SCI 4.0 to develop and update the first version of the standardization roadmap on Industrie 4.0.

This standardization roadmap is the central medium of SCI 4.0 for communication with standardization committees, industry, associations, research institutions and ministries.

A.2.5 Korea – “Korea – Manufacturing Industry Innovation 3.0 strategy”,

“National initiative in Korea about Manufacturing Industry Innovation 3.0 strategy”

Logo: see Figure A.3.

Figure A.3 – KOSF logo

KOSF is the foundation consisting of private companies and government established to successfully lead smart factory projects in Korea.

It is aimed at enhancing competitiveness of SMEs and to bring advanced smart features to overall manufacturing industry.

– Provision and Propagation

  Provide and propagate Smart factory for SMEs of manufacturing industry.

– Research and Development Planning

  Promote innovation and technological development and secure advanced smart solutions.

– Build Infrastructure

  Establish a testbed centre that tests interoperability of solutions and offers technological support for solution developers.

– Standardization and Education

  Promote standardization, certification, security and manpower training.

A.2.6 China – Industrial Initiatives (Standards Development)

Activities are synchronized and initiated by governmental decision through NB organizations to ISO and IEC.

National organizations and programs are involved in standard developments for IIoT are:

National IoT fundamental Standard Working Group takes the charge of IoT related standards coordination as well as fundamental and key application standards developing in China; CESI takes the responsibility of the Secretariat. Since it was founded in 2010, 150 IoT related standards projects have been coordinated through its mechanism, nearly 180 IoT standard proposals were approved including 55 published until July 2019. Within these, five IIoT proposals were approved since 2015 and four of them are already published (see Table A.1). SAC/TC 28/SC 41 – Information Technology Technical Committee/Internet of Things Subcommittee – is about to be established; it will be the mirror committee of ISO/IEC JTC 1/SC 41 in China, and further IIoT standards will be involved in that SC 41.

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

No.	Name	Status
1	Industrial Internet of Things – Specification of structured description for data acquisition	Committee stage
2	Application attribute protocol for instrument of Industrial Internet of Things	Published
3	Service protocol for instrument of Industrial Internet of Things	Published
4	Interoperating protocol for instrument of Industrial Internet of Things	Published
5	Identifier protocol for instrument of Industrial Internet of Things	Published

National organizations and programs involved in standard developments for IIoT are:

– AII
– CCSA-UG
– CESI

China has officially declared its collaboration in the OPC-UA Standard (IEC 62541) as by the announcement in 2018-03-04. See Figure A.4.

共8条记录
Search Result

每页显示 20 个记录
Number of Every Page Shows

序号	标准号 Standard No.	中文标准名称 Standard Title in Chinese	英文标准名称 Standard Title in English	状态 State	备注 Remark
1	GB/T 33863.4-2017	OPC统一架构 第4部分：服务	OPC unified architecture—Part 4: Services	现行	
2	GB/T 33863.3-2017	OPC统一架构 第3部分：地址空间模型	OPC unified architecture—Part 3:Address space model	现行	
3	GB/T 33863.6-2017	OPC统一架构 第6部分：映射	OPC unified architecture—Part 6: Mapping	现行	
4	GB/T 33863.8-2017	OPC统一架构 第8部分：数据访问	OPC unified architecture—Part 8: Data access	现行	
5	GB/T 33863.7-2017	OPC统一架构 第7部分：行规	OPC unified architecture—Part 7: Profiles	现行	
6	GB/T 33863.2-2017	OPC统一架构 第2部分：安全模型	OPC unified architecture—Part 2: Security model	现行	
7	GB/T 33863.1-2017	OPC统一架构 第1部分：概述和概念	OPC unified architecture—Part 1: Overview and concepts	现行	
8	GB/T 33863.5-2017	OPC统一架构 第5部分：信息模型	OPC unified architecture—Part 5: Information model	现行	

IEC

Figure A.4 – Link reference on Chinese GB/T standards vs. OPC/UA

So this step also leads to better interoperability across communication layers in existing and to be developed future Smart Manufacturing architecture and models especially between different companies and organizations.

A.2.7 Japan (RRI and IVI)

Name: Robot Revolution & Industrial IoT Initiative (RRI), see [69]

RRI was established in 2015 as a part of Japan's robot strategy. In the same year, Japan drew the future image "Society 5.0" that solves social issues. In 2017, the figure of the next-generation industry that supports the Society 5.0 was defined as "Connected Industries". RRI plays a key role in Connected Industries, responsible for leading "Manufacturing and Robotics".

In 2016, Japan concluded the collaboration agreement with Germany about manufacturing revolution, which has achieved various results including publishing joint papers with Plattform Industrie 4.0. Currently RRI has joint collaboration relationships with various international consortia such as IIC. See Figure A.5 for cooperative relationship.

RRI is also in charge of secretariat of Japan National Committee of IEC SyC SM.

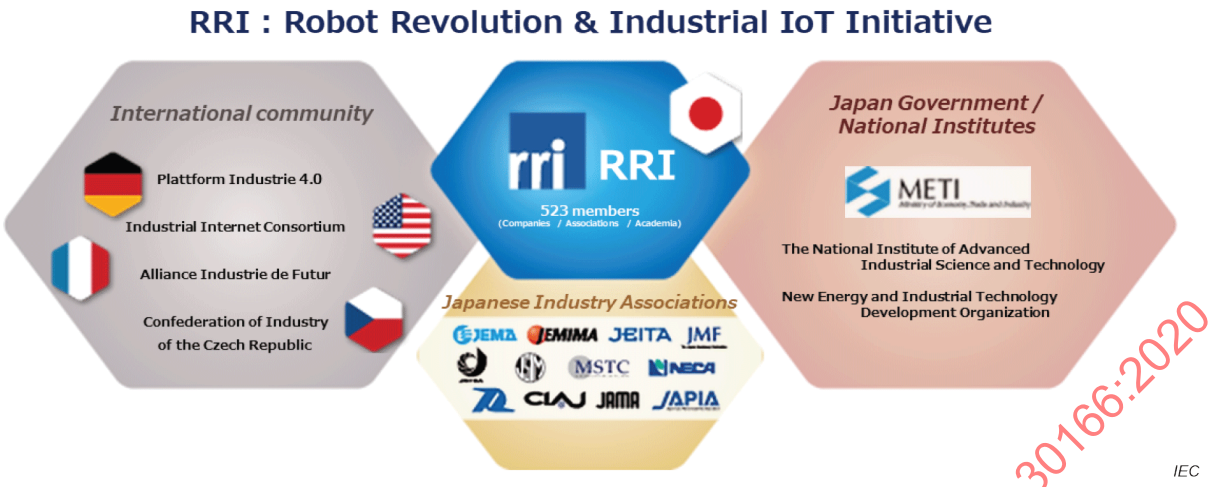


Figure A.5 – Robot Revolution & Industrial IoT Initiative

Figure A.6 – RRI and cooperative relationship

The goals of RRI are the following:

1) Matching parties that will contribute to the solving of problems in robot innovation and the promoting of robot utilization and promoting the sharing and spreading of best practices.
2) Sharing information to promote international standardization activities, organizing common issues, and planning measures for those issues.
3) Planning measures to assure information security.
4) Planning international projects, etc.
5) Preparing an environment for verification testing.
6) Planning the development of human resources.
7) Promoting Research and Development, regulatory reform and other matters with cooperating organizations.
8) Collecting and outputting related information, including that involving international cooperation, and promoting expansion and enlightenment projects.

Ref.: https://www.jmfrri.gr.jp/english/

Name: Industrial Value Chain Initiative (IVI)

IVI was established in 2015 to support to build business scenario and use cases of connected manufacturing among different enterprises referring to loosely defined standard and provide

and manage a repository of the loosely defined standard models that can be continuously changed in accordance with the future requirements, see following links;

Ref.: https://www.iv-i.org/en/index.html

Ref.: https://www.iv-i.org/en/docs/IVI_Flyer_English.pdf

Ref.: https://iv-i.org/en/docs/doc_160428_hannover.pdf

IVI has two key concepts:

– connected manufacturing;
– loosely defined standard (LDS).

See Figure A.7.

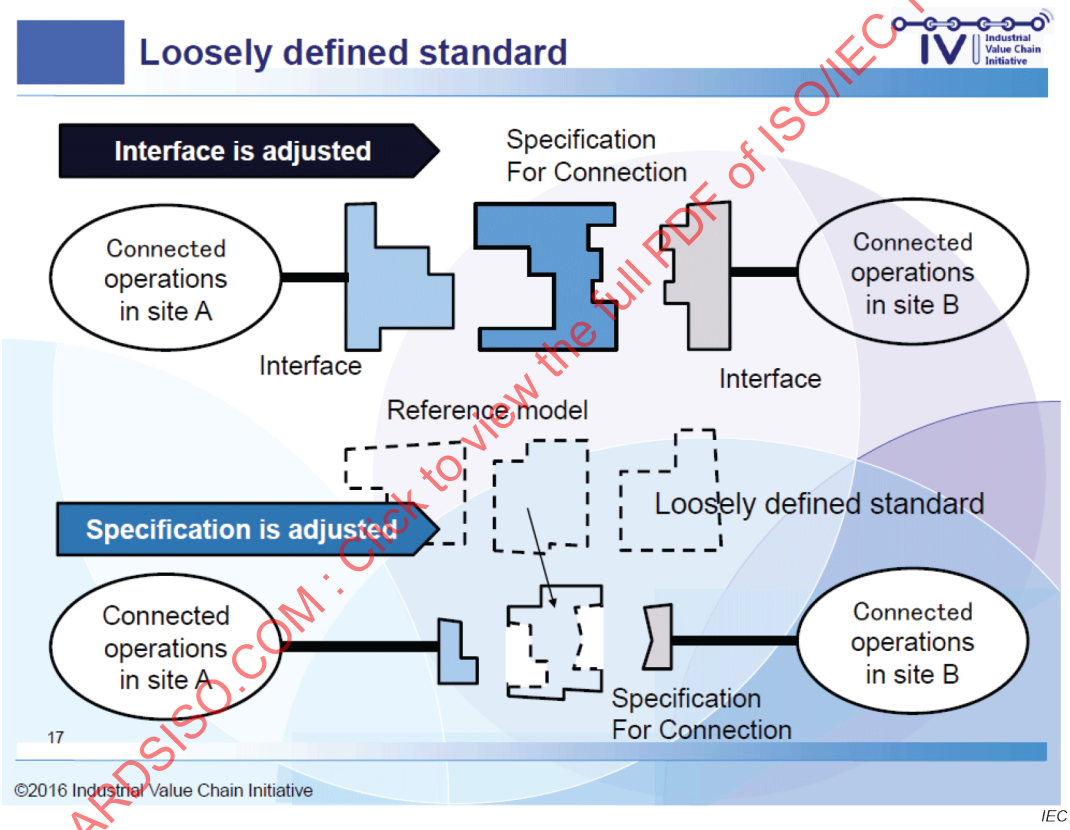


Figure A.7 – Industrial Value Chain Initiative (IVI)

A.2.8 USA – CPS/CPPS/IIoT Standards Initiatives

NIST (National Institute of Standards and Technology)

Logo: see Figure A.8.

Figure A.8 – NIST logo

Ref.: https://www.nist.gov/

Description: Founded in 1901 and now part of the U.S. Department of Commerce, NIST is one of the nation's oldest physical science laboratories. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

The relevance of NIST Engagements to IIoT Standardization is identified to be of very high importance.

NIST's CPS/IoT Program develops and demonstrates new measurement science and promotes the emergence of consensus standards and protocols for advanced cyber-physical systems and IoT that are scalable, effective, measurable, interoperable, trustworthy, and assured. In collaboration with stakeholders, NIST has developed and published its Framework for Cyber-Physical Systems (https://doi.org/10.6028/NIST.SP.1500-201) which provides an analysis methodology for CPS and IoT based on core concepts of facets (modes of the system engineering process: conceptualization, realization and assurance) and aspects (clusters of concerns: functional, business, human, trustworthiness, timing, data, composition, boundaries, and life cycle).

NIST's Cybersecurity for the Internet of Things (IoT) program (https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program) supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed and includes IoT Cybersecurity-Related Initiatives such as the NIST Guide to Industrial Control Systems (ICS) Security (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf)

Working closely with government, industry and academia NIST has published Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (https://csrc.nist.gov/News/2019/nist-publishes-nistir-8228) which provides guidance to better understand and manage the risks associated with IoT devices usage throughout the life cycles of those devices. NIST has also published a draft Core Cybersecurity Feature Baseline for Securable IoT Devices aimed at manufacturers that provides guidance for identifying security features for IoT devices and identifies a core set of common security features IoT devices should support when more specific requirements are not known (NIST IR 8259).

NIST supports the next generation of Smart Manufacturing processes and equipment such as automation, distributed sensing, and advanced control systems, which need to be optimized to enable cost-effective and agile manufacturing of high-tech products and systems.

NIST supports Smart Manufacturing through many programs such as robotics in manufacturing, to support the closer integration of robotics and humans in industrial settings, and a digital thread testbed to evaluate the performance of automated in-process quality monitoring and control systems that are critical to the efficient operation of modern factories.

NIST has provided leadership through its Global City Teams Challenge to coordinate and advance IoT use in smart cities, and has supported cities to employ interoperable, scalable and replicable smart city solutions through its IoT-Enabled Smart Cities Framework.

Work in “big data” in relation to IIoT as of the ToRs by NIST:

Ref.: https://bigdatawg.nist.gov/_uploadfiles/M0055_v1_7606723276.pdf

It is important to track NIST developments on this in future for further standardization developments. A liaison exists already in ISO/IEC JTC 1/SC 41 to NIST as well as members of NIST working in ISO/IEC JTC 1/SC 41.

The intense and broad range of analysis reports and work of NIST is of high value for any standardization activities of manufacturing.

As RAMI and NIST model elements rely on ISA-95 and ISA-88 standards development, this is a common denominator for enhancement of standardization.

As a consideration by this document: Especially work done by NIST in regard to security, cloud and big data, which all will become very important aspects for further IIoT standardization.

A.2.9 IIoT activities by EC EU

Name: The Alliance for Internet of Things Innovation

Ref.: https://aioti.eu/

The Alliance for Internet of Things Innovation (AIOTI) was initiated as a result of the European and global IoT technology and market developments.

AIOTI aims to create and master sustainable innovative European IoT ecosystems in the global context to address the challenges of IoT technology and applications deployment including standardization, interoperability and policy issues, in order to accelerate sustainable economic development and growth in the new emerging European and global digital markets.

AIOTI/WG 11 "Smart Manufacturing" and in internal correlation with AIOTI/WG 3 "IoT Standardization".

A.3 Industrial consortia recognized/identified as being of interest on working about the IIoT

A.3.1 General

During the generation of this document, a large number of non-SDO groups has been identified and these non-SDO groups have their scopes potentially related to the IIoT. Thus, these groups are kept in this document because their activities could impact on the future development of IIoT.

During the following analysis in this document, it became obvious that many of these organizations and initiatives are "unequal" in terms of their work in regard to aspects/themes on IIoT. Therefore, in this document, they are out-of-scope if they are not recommended to be followed by the ISO/IEC JTC 1/SC 41/SLG 1. In other cases, they are in-scope to indicate the recommendation that they be followed by ISO/IEC JTC 1/SC 41/SLG 1, which means that these organizations should be examined for their activities in the following ways:

– Standards relevant to IIoT by the organizations summarized in Clause A.3 to be appropriately analysed later (analysed also relevant by future reports) or in scope of JTC 1/SC 41/SLG 1 IIoT work; and

– Industrial consortia which work in direction of IIoT – but not for standardization – should also be kept under analysis for future recognition.

A.3.2 Alliance of Industrial Internet: “Chinese Model of Smart Manufacturing in context of program China Manufacturing 2025” [70]

Ref.: http://en.aii-alliance.org/

Description: As an important part and a key instrument in the transformation and upgrading of advanced manufacturing industry in China and abroad, industrial Internet is a major component in the strategic layout for “China Manufacturing 2025” and “Internet + Collaborative Manufacturing” Initiatives.

A.3.3 5G-ACIA in IIoT, and Smart Manufacturing

Name: 5G-ACIA – “Alliance for the Connected Industry and Automation”

Link-Src.: https://www.5g-acia.org/

5G-ACIA (“Alliance for the Connected Industry and Automation”) was formed with the following mission, objectives, targets and goals:

– Mission: Ensure the best possible applicability of 5G technology and 5G networks for the manufacturing and process industry by addressing, discussing and evaluating relevant technical, regulatory and business aspects.
– Objectives: Identify special spectrum needs and evaluate suitable spectrum usage models (e.g. for enabling private 5G networks in a factory).
– Use Cases, Requirements and Terminology: Define and analyse use cases, consolidate requirements and establish a common terminology with the telecommunications world, with a strong focus on industrial automation, Smart Manufacturing, advanced global industrial systems.
– Ecosystem and Operator Models: Partner with relevant stakeholders (e.g. vendors, operators), develop possible operator models and identify required technical enablers: This includes especially a strong focus on future business models for mobile network operators inside factories as well Smart Manufacturing and process automation

Standardization and Regulation by 5G-ACIA:

To foster standardization activities (3GPP, ITU, ETSI, etc.) to ensure that the needs and requirements of the automation industry are adequately considered.

To ensure a global interoperability scope on all of these standardization efforts.

Certification, Interoperability Tests and Validation:

In regard to 5G, especially for use cases within IIoT, coexistence and stability is mandatory. Thus, by identifing the relevant needs, develop a suitable framework and trigger potential interoperability tests and validation activities.

Further targets in legislation, participation to international and national standards bodies as well as technology providers, collaboration and exchange with industry associations as well as with academia.

A.3.4 China Edge Computing Consortium ECC

Description: As the focus of an emerging industry, edge computing has broad application prospects.

It covers multiple fields including Operation Technology (OT), Information Technology (IT), and Communications Technology (CT).

Further, edge computing involves many industry chain roles such as network connection, data aggregation, chip design and fabrication, sensing, and applications for a variety of purposes.

A.3.5 DMG (Data Mining Group)

Ref.: http://dmg.org/

Description: The Data Mining Group (DMG) is an independent, vendor-led consortium that develops data mining standards.

The DMG hosts the working groups that develop the Predictive Model Markup Language (PMML) and the Portable Format for Analytics (PFA), two complementary standards that simplify the deployment of analytic models.

A.3.6 eCl@ss

Ref.: https://www.eclass.eu/

eCl@ss has won international acceptance as the only ISO/IEC-compliant (IEC 61360-1 and ISO 13584) global industry reference standard for the classification and unambiguous specification of products and services.

With over 40 000 groups and more than 17 000 characteristics, the eCl@ss standard provides companies with a means of product data communication that is internationally recognized and free of media discontinuity. Already more than 3 500 companies worldwide are convinced of the advantages and are using the eCl@ss standard.

Cooperation with IEC:

The cooperation between IEC and eCl@ss e.V. centres on the requirements of international and digital information exchange based on globally implemented IEC Standards. In the framework of the project “d-m@p,” experts from IEC and eCl@ss e.V. are developing a mapping system that makes product data characteristics and attributes reciprocally readable. As digitization proceeds, companies are increasingly faced with the challenge of electronic data exchange.

C-Liaisions with several IEC TC/SC committees are established.

Source: https://www.eclass.eu/fileadmin/downloads/ecl-Whitepaper_2018_EN.pdf

https://iecetech.org/issue/2016-08/Digital-data-exchange-to-be-streamlined

Activities in the digitalization domain:

Experts of Plattform Industrie 4.0, ZVEI and eCl@ss work together to enable eCl@ss users to quickly standardize Asset Administration Shell elements in eCl@ss and apply eCl@ss mechanisms to their use. See also Figure A.9.