Standardisation for Industry 4.0: Challenges, Opportunities and Trends in Brazil

Highlights from the First National Forum on Standardisation 4.0

GPQI
Dialogues for Innovation and Trade

Published by
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn, Germany

Global Project Quality Infrastructure
SCN Quadra 1 Bloco C Sala 1111 -11º Andar
Brasília Trade Center
70711-902 Brasília-DF
Brazil
E info@gpqi.org I www.gpqi.org

Design
Oliver Hick-Schulz

Photo credits
metamorworks / Shutterstock

On behalf of
German Federal Ministry of Economic Affairs and Climate Action (BMWK)
Berlin, Germany 2023
Brasília, Brazil 2023

Text
The content was prepared based on the discussions of experts during three technical workshops by the team from the Organisational Engineering Centre of the Federal University of Rio Grande do Sul - UFRGS.

Authors
Alejandro G. Frank, Dr
Néstor F. Ayala, Dr
Camila Costa Dutra, Dr
Laura Visintainer Lerman, MSc
Márcia Possa Forcelini

The German Federal Ministry for Economic Affairs and Climate Action (BMWK) has commissioned the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH to implement the Global Project Quality Infrastructure (GPQI). This publication was also supported by the Brazilian Chamber of Industry 4.0 (BCI4.0) and the Brazilian Ministry of Development, Industry, Commerce and Services (MDIC).

Implemented by

Federal Ministry for Economic Affairs and Climate Action

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

CÂMARA DA INDÚSTRIA 4.0

MINISTÉRIO DO DESENVOLVIMENTO INDÚSTRIA, COMÉRCIO E SERVIÇOS

GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Industry 4.0 in Brazil and the 1st National Forum on Standardisation 4.0

The core of the Industry 4.0 concept lies in seamless data flows along industrial value chains. Technical standards are hereby the main tool to enabling the necessary interoperability. In this vein, therefore, ISO and IEC are conducting a series of strategic processes aimed at fostering the development and improvement of standards towards implementing Industry 4.0 in the industrial sector worldwide. Brazil has been identified as a frontrunner that is keeping pace with discussions on the concept of Industry 4.0 and its evolution. The scale of Brazil´s industrial sector, however, is not reflected in its current role within those international processes.

In this context, the Brazilian Association of Technical Standards (ABNT) and Brazilian Chamber of Industry 4.0 (BCI4.0) organised the First National Congress for Standardisation in Industry 4.0. The event was supported by the Global Project Quality Infrastructure (GPQI), which is implemented by the Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH (GIZ) and commissioned by the German Federal Ministry for Economic Affairs and Climate Action (BMWK). Comprising three workshop groups, the congress addressed specific fields within the relevant technology, preselected prior to the event by BCI4.0.

The 170 participants jointly identified technical barriers that currently undermine the implementation of Industry 4.0 in their companies. The study groups then compiled relevant standardisation projects at ISO/IEC level which address these barriers and should therefore be considered relevant for increased engagement by Brazilian experts. Beyond these operational recommendations, the final version of the study in Portuguese[1] included thorough analysis of the current status of the discussion in each committee. Important information on regulatory aspects in Brazil and the European Union/Germany were also included, in particular, for Artificial Intelligence (AI) and cybersecurity.

In the first workshop, which focused on AI, the group of experts identified thirteen problems, including the lack of standards on data collection, information processing, tools, best practices, algorithm frameworks and security. The group also observed a lack of understanding between the fields of business and information technology, as well as between AI models and the statistical baseline.

On the issues of information security, cybersecurity and privacy, the experts identified eight problems, including a lack of knowledge of cybersecurity regulations and main concepts, as well as a lack of understanding of integration and communication standards. In sum, they highlighted the scarcity of qualified professionals active in the field of cybersecurity. They stressed the need to define minimal prerequisites for governance in cybersecurity as well as cybersecurity in IoT gadgets. Nevertheless, the experts pinpointed a window of opportunity to debate which problems

[1] Análise dos Workshops do Primeiro Congresso de Normalização Internacional no contexto da Industria 4.0 - Desafios da Normalização para Indústria 4.0 no Brasil. Available on: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivo-camara-industria/iniciativas/ci_nt_normalizacao_industria4-0_giz.pdf

will be tackled by regulations and whether further regulations or adaptations in the current set will be necessary.

The third workshop, which focused on Internet of Things (IoT) and digital twins, identified a total of four barriers. Here, experts highlighted the challenges involved in integrating both software and hardware systems from different manufacturers, given the diversity of protocols and communication standards. They also pinpointed issues relating to the interoperability of automised data collection within different IoT systems. They observed the lack of open documentation relating to legacy systems and proprietary protocols. Moreover, they emphasised the need to modernise the equipment necessary for the digital transformation, to standardise Retrofitting 4.0 procedures and to establish the basic requirements for gateways. Since industries operate in various technology cycles, they have to create mechanisms to modernise their equipment and lines of production on a regular basis.

Notwithstanding the challenges highlighted, the subsequent study managed to identify standardisation projects that are currently addressing those barriers. It also highlights trends and opportunities concerning both the development and improvement of existing regulations. The study underlines the fact that such discussions pave the way towards new solutions, as well as the country's insertion in the international debate regarding regulations and Industry 4.0. Within all three workshops, there was genuine interest in participating in the discussions via ABNT. A key outcome, for instance, was the preparation of a list of more than 80 professionals who volunteered to join ABNT committees. The study also outlines the need to improve the linkage between cybersecurity and both AI and IoT regulations, which should enable priority stakeholders and committees to design regulations in line with the current and future needs of the industry.

Industry 4.0 requires new cyber security strategies
© Michael Traitov / AdobeStock

In sum, the workshops contributed to strengthening ABNT's capacity to play an industry-driven role in international standardisation processes on Industry 4.0. Based on the experience of the three workshops and the ongoing projects identified, ABNT is currently elaborating a strategic agenda for national standardisation activities and the participation of experts in international committees.

Topic	Analysed committees	Industry demand	Suggested standardisation projects	Description
Artificial Intelligence	ISO/IEC JTC 1/SC 42	Lack of standardised procedures for data collection	ISO/IEC AWI 5259-1	Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 1: Overview, terminology and examples
Artificial Intelligence	ISO/IEC JTC 1/SC 42	Lack of standardised procedures for data collection	ISO/IEC AWI 5259-2	Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 2: Data quality measures
Artificial Intelligence	ISO/IEC JTC 1/SC 42	Lack of standardised procedures for data collection	ISO/IEC AWI 5259-3	Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 3: Data quality management requirements and guidelines
Artificial Intelligence	ISO/IEC JTC 1/S C42	Lack of standardised procedures for data collection	ISO/IEC AWI 5259-4	Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 4: Data quality process framework
Artificial Intelligence	ISO/IEC JTC 1/SC 42	Lack of integration and communication for data exchange	ISO/IEC FDIS 23053	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
Artificial Intelligence	ISO/IEC JTC 1/SC 42	Lack of integration and communication for data exchange	ISO/IEC 20547-3:2020	Information technology — Big data reference architecture — Part 3: Reference architecture
Artificial Intelligence	ISO/IEC JTC 1/SC 42	Lack of integration and communication for data exchange	ISO/IEC 38507	Information technology — Governance of IT — Governance implications for the use of artificial intelligence by organisations
Artificial Intelligence	ISO/IEC JTC 1/SC 42	Lack of understanding between the business and information technology areas	ISO/IEC FDIS 23053	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)

Topic	Analysed committees	Industry demand	Suggested standardisation projects	Description
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of understanding between the business and information technology areas**	**ISO/IEC 20547-3:2020**	**Information technology** — Big data reference architecture — Part 3: Reference architecture
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of understanding between the business and information technology areas**	**ISO/IEC 38507**	**Information technology** — Governance of IT — Governance implications for the use of artificial intelligence by organisations
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of a clear standard on information processing**	**ISO/IEC DTR 27563**	**Impact of security and privacy in artificial intelligence**
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of a clear standard on information processing**	**ISO/IEC AWI 5259-3**	**Artificial intelligence** — Data quality for analytics and machine learning (ML) — Part 3: Data quality management requirements and guidelines
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Need for definition of minimum requirements of AI projects**	**ISO/IEC T 24030:2021**	**Information technology** — Artificial intelligence (AI) — Use cases
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Need for definition of minimum requirements of AI projects**	**ISO/IEC AWI 5339**	**Information Technology** — Artificial Intelligence — Guidelines for AI applications
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Need for definition of minimum requirements of AI projects**	**ISO/IEC TR 24028:2020**	**Information technology** — Artificial intelligence — Overview of trustworthiness in artificial intelligence
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Need for minimum requirements for the quality of AI algorithms**	**ISO/IEC DIS 23053**	**Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)**

Topic	Analysed committees	Industry demand	Suggested standardisation projects	Description
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Need for minimum requirements for the quality of AI algorithms**	**ISO/IEC AWI TS 5471**	**Artificial intelligence** — Quality evaluation guidelines for AI systems
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Need for minimum requirements for the quality of AI algorithms**	**ISO/IEC AWI 5339**	**Information Technology** — Artificial Intelligence — Guidelines for AI applications
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of standardisation of tools, best practices and frameworks for algorithms**	**ISO/IEC AWI TS 5471**	**Artificial intelligence** — Quality evaluation guidelines for AI systems
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of standardisation of tools, best practices and frameworks for algorithms**	**ISO/IEC AWI 5259-1**	**Artificial intelligence** — Data quality for analytics and machine learning (ML)
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of clarity on how algorithms can be used by different subjects**	**ISO/IEC TR 24030:2021**	**Information technology** — Artificial intelligence (AI) — Use cases
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of clarity on how algorithms can be used by different subjects**	**ISO/IEC TR 24372:2021**	**Artificial intelligence (AI)** — Overview of computational approaches for AI systems
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of clarity on how algorithms can be used by different subjects**	**ISO/IEC AWI 5339**	**Information Technology** — Artificial intelligence (AI) — Guidelines for AI applications
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of an understanding of AI models and the statistical basis**	**ISO/IEC TR 24029-1:2021**	**Artificial Intelligence (AI)** — Assessment of the robustness of neural networks — Part 1: Overview
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of an understanding of AI models and the statistical basis**	**ISO/IEC AWI TS 5471**	**Artificial intelligence** — Quality evaluation guidelines for AI systems
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of understanding of how to use AI algorithms to create research aligned with the needs of academia and business**	**ISO/IEC AWI 5339**	**Information Technology** — Artificial intelligence (AI) — Guidelines for AI applications

Topic	Analysed committees	Industry demand	Suggested standardisation projects	Description
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of a minimum safety standard in AI**	**ISO/IEC AWI TR 5469**	**Artificial intelligence** — Functional safety and AI systems
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of a minimum safety standard in AI**	**ISO/IEC DIS 23894**	**Information technology** — Artificial intelligence (AI) — Risk management
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of a minimum safety standard in AI**	**ISO/IEC DTR 27563**	**Impact of security and privacy in artificial intelligence**
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of understanding of the ethical aspects of using AI algorithms and using the data**	**ISO/IEC AWI 5259-3**	**Artificial intelligence** — Data quality for analytics and machine learning (ML) — Part 3: Data quality management requirements and guidelines
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of understanding of the ethical aspects of using AI algorithms and using the data**	**ISO/IEC DTR 24368**	**Information technology** — Artificial intelligence (AI) — Overview of ethical and societal concerns
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of minimum knowledge and training on AI solutions**	**ISO/IEC DIS 22989**	**Information technology** — Artificial intelligence — Artificial intelligence concepts and terminology
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of minimum knowledge and training on AI solutions**	**ISO/IEC 20546:2019**	**Information technology** — Big data — Overview and vocabulary
Artificial Intelligence	**ISO/IEC JTC 1/SC 42**	**Lack of minimum knowledge and training on AI solutions**	**ISO/IEC TR 24030:2021**	**Information technology** — Artificial intelligence (AI) — Use cases
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of knowledge about cybersecurity standards**	**ISO/IEC 27013:2021**	**Information security, cybersecurity and privacy protection** — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

Topic	Analysed committees	Industry demand	Suggested standardisation projects	Description
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of knowledge about cybersecurity standards**	**ISO/IEC 27021:2017**	**Information technology** — Security techniques — Competence requirements for information security management systems professionals (ISO/IEC 27021)
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of knowledge about cybersecurity standards**	**ISO / IEC 19896: 2018**	**IT security techniques** — Competence requirements for information security testers and evaluators (ISO/IEC 19896)
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of knowledge about cybersecurity standards**	**ISO/IEC TS 23532-1:2021**	**Information security, cybersecurity, and privacy protection** — Requirements for the competence of IT security testing and evaluation laboratories — Part 1: Evaluation for ISO/IEC 15408
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of knowledge about cybersecurity standards**	**ISO/IEC TS 23532-2:2021**	**Information security, cybersecurity, and privacy protection** — Requirements for the competence of IT security testing and evaluation laboratories — Part 2: Testing for ISO/IEC 19790
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of knowledge about the main cybersecurity concepts**	**ISO/IEC AWI TR 27109**	**Cybersecurity education and training**
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of knowledge about the main cybersecurity concepts**	**ISO/IEC TS 27100:2020**	**Information technology** — Cybersecurity — Overview and concepts

Topic	Analysed committees	Industry demand	Suggested standardisation projects	Description
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of knowledge about the main cybersecurity concepts**	**ISO/IEC TR 15443-1:2012**	**Information technology** — Security techniques — Security assurance framework — Part 1: Introduction and concepts
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of knowledge about the main cybersecurity concepts**	**ISO/IEC 19896-1:2018**	**IT security techniques** — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of knowledge about the main cybersecurity concepts**	**ISO/IEC 24760-1:2019**	**IT Security and Privacy** — A framework for identity management — Part 1: Terminology and concepts (ISO/IEC 24760)
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of knowledge about the main cybersecurity concepts**	**ISO/IEC 27033-1:2015**	**Information technology** — Security techniques — Network security — Part 1: Overview and concepts
Information security, cybersecurity and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of knowledge about the main cybersecurity concepts**	**ISO/IEC 27034-1:2011**	**Information technology** — Security techniques — Application security — Part 1: Overview and concepts
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of knowledge about minimum communication and integration standards**	**ISO/IEC DIS 27400**	**Cybersecurity** — IoT security and privacy – Guidelines
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of knowledge about minimum communication and integration standards**	**ISO/IEC 27036-1:2021**	**Cybersecurity** — Supplier relationships — Part 1: Overview and concepts

Topic	Analysed committees	Industry demand	Suggested standardisation projects	Description
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of knowledge about minimum communication and integration standards**	**ISO/IEC DIS 27036-2**	**Cybersecurity** — Supplier relationships — Part 2: Requirements
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of knowledge about minimum communication and integration standards**	**ISO/IEC CD 27036-3**	**Cybersecurity** — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of qualified professionals in cybersecurity**	**ISO/IEC AWI TR 27109**	**Cybersecurity education and training**
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Information security, cybersecurity and privacy protection**	**ISO/IEC JTC 1/SC 27**	**Information security, cybersecurity and privacy protection**
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of qualified professionals in cybersecurity**	**ISO/IEC TS 23532-1:2021**	**Information security, cybersecurity, and privacy protection** — Requirements for the competence of IT security testing and evaluation laboratories — Part 1: Evaluation for ISO/IEC 15408
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of qualified professionals in cybersecurity**	**ISO/IEC DTR 24368**	**Information technology** — Artificial intelligence — Overview of ethical and societal concerns
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of understanding of key benefits of cybersecurity and standards for outsourcing cybersecurity**	**ISO/IEC 15408–1**	**ISO / IEC 15408 Information technology** — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

Topic	Analysed committees	Industry demand	Suggested standardisation projects	Description
Information security, cybersecurity, and privacy protection	ISO/IEC JTC 1/SC 27	Lack of understanding of key benefits of cybersecurity and standards for outsourcing cybersecurity	ISO/IEC DIS 15408-4	**Information security, cybersecurity and privacy protection** — Evaluation criteria for IT security — Framework for the specification of evaluation methods and activities
Information security, cybersecurity, and privacy protection	ISO/IEC JTC 1/SC 27	Lack of understanding of key benefits of cybersecurity and standards for outsourcing cybersecurity	ISO/IEC 27036-1:2021	**Cybersecurity** — Supplier relationships — Part 1: Overview and concepts
Information security, cybersecurity, and privacy protection	ISO/IEC JTC 1/SC 27	Lack of understanding of key benefits of cybersecurity and standards for outsourcing cybersecurity	ISO/IEC DIS 27036-2	**Cybersecurity** — Supplier relationships — Part 2: Requirements
Information security, cybersecurity, and privacy protection	ISO/IEC JTC 1/SC 27	Lack of understanding of key benefits of cybersecurity and standards for outsourcing cybersecurity	ISO/IEC CD 27036-3	**Cybersecurity** — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security
Information security, cybersecurity, and privacy protection	ISO/IEC JTC 1/SC 27	Lack of understanding to promote integration in a safe way	ISO/IEC 27036-1:2021	**Cybersecurity** — Supplier relationships — Part 1: Overview and concepts
Information security, cybersecurity, and privacy protection	ISO/IEC JTC 1/SC 27	Lack of understanding to promote integration in a safe way	ISO/IEC DIS 27036-2	**Cybersecurity** — Supplier relationships — Part 2: Requirements
Information security, cybersecurity, and privacy protection	ISO/IEC JTC 1/SC 27	Lack of understanding to promote integration in a safe way	ISO/IEC CD 27036-3	**Cybersecurity** — Supplier relationships — Part 3: Guidelines for hardware, software, and services supply chain security

Topic	Analysed committees	Industry demand	Suggested standardisation projects	Description
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of understanding to promote integration in a safe way**	**ISO/IEC FDIS 15408-4**	**Information security, cybersecurity, and privacy protection** — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Lack of understanding to promote integration in a safe way**	**ISO/IEC FDIS 15408-5**	**Information security, cybersecurity, and privacy protection** — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Need for definition of minimum cybersecurity governance requirements**	**ISO/IEC 27014:2020**	**Information security, cybersecurity, and privacy protection** — Governance of information security
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Cybersecurity in IoT devices**	**ISO/IEC DIS 27400**	**Cybersecurity** — IoT security and privacy — Guidelines
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Cybersecurity in IoT devices**	**ISO/IEC CD 27402.2**	**Cybersecurity** — IoT security and privacy — Device baseline requirements
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Cybersecurity in IoT devices**	**ISO/IEC WD 27403.6**	**Cybersecurity** – IoT security and privacy – Guidelines for IoT-domotics
Information security, cybersecurity and privacy protection	**ISO/IEC JTC 1/SC 27**	**Cybersecurity in IoT devices**	**ISO/IEC CD 27032.3**	**Information technology** — Security techniques — Guidelines for cybersecurity

Topic	Analysed committees	Industry demand	Suggested standardisation projects	Description
Internet of Things and digital twin	ISO/IEC JTC 1/SC 41	Difficulty in integrating software and hardware from different suppliers	ISO / IEC 29182-1: 2013	Internet of Things (IoT) — Interoperability for IoT systems — Part 1: Framework
Internet of Things and digital twin	ISO/IEC JTC 1/SC 41	Difficulty in integrating software and hardware from different suppliers	ISO / IEC 21823-2: 2020	Internet of Things (IoT) — Interoperability for IoT systems — Part 2: Transport interoperability
Internet of Things and digital twin	ISO/IEC JTC 1/SC 41	Difficulty in integrating software and hardware from different suppliers	ISO/IEC 21823-3:2021 -	Internet of Things (IoT) — Interoperability for IoT systems — Part 3: Semantic interoperability
Internet of Things and digital twin	ISO/IEC JTC 1/SC 41	Difficulty in integrating software and hardware from different suppliers	ISO/IEC 29182-7:2015	Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) — Part 7: Interoperability guidelines
Internet of Things and digital twin	ISO/IEC JTC 1/SC 41	Diversity of communication protocols and standards	ISO/IEC 21823	Internet of Things (IoT) — Interoperability for IoT systems
Internet of Things and digital twin	ISO/IEC JTC 1/SC 41	Diversity of communication protocols and standards	ISO / IEC 29182-1: 2013	Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) — Part 1: General overview and requirements
Information security, cybersecurity, and privacy protection	ISO/IEC JTC 1/SC 27	Cybersecurity in IoT devices for interoperability	ISO/IEC 27005:2018	Information technology — Security techniques — Information security risk management
Information security, cybersecurity, and privacy protection	ISO/IEC JTC 1/SC 27	Cybersecurity in IoT devices for interoperability	ISO/IEC 27004:2016	Information technology — Security techniques — Information security management — Monitoring, measure ment, analysis, and evaluation

Topic	Analysed committees	Industry demand	Suggested standardisation projects	Description
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Cybersecurity in IoT devices for interoperability**	**ISO/IEC DIS 27400**	**Cybersecurity** — IoT security and privacy — Guidelines
Information security, cybersecurity, and privacy	**ISO/IEC JTC 1/SC 27**	**Cybersecurity in IoT devices for interoperability**	**ISO/IEC CD 27402.2**	**Cybersecurity** — IoT security and privacy — Device baseline requirements
Internet of Things and digital twin	**ISO/IEC JTC 1/SC 41**	**Cybersecurity in IoT devices for interoperability**	**ISO/IEC TR 30176:2021**	**Internet of Things (IoT)** — Integration of IoT and DLT/blockchain: Use cases
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Cybersecurity in IoT devices for interoperability**	**ISO/IEC DIS 27400**	**Cybersecurity** — IoT security and privacy — Guidelines
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Cybersecurity in IoT devices for interoperability**	**ISO/IEC CD 27402.2**	**Cybersecurity** — IoT security and privacy — Device baseline requirements
Information security, cybersecurity, and privacy protection	**ISO/IEC JTC 1/SC 27**	**Cybersecurity in IoT devices for interoperability**	**ISO/IEC WD 27403.6**	**Cybersecurity** – IoT security and privacy – Guidelines for IoT-domotics
Internet of Things and digital twin	**ISO/IEC JTC 1/SC 41**	**Data difficulties for interoperability**	**ISO/IEC 30161:2020**	**Internet of Things (IoT)** — Requirements of IoT data exchange platform for various IoT services (ISO/IEC 30161)
Industrial data	**ISO/TC 184/SC 4**	**Data difficulties for interoperability**	**ISO 23247-1:2021**	**Automation systems and integration** — Digital twin framework for manufacturing — Part 1: Overview and general principles

Topic	Analysed committees	Industry demand	Suggested standardisation projects	Description
Industrial data	ISO/TC 184/SC 4	Data difficulties for interoperability	ISO 23247-2	Reference architecture with functional views
Industrial data	ISO/TC 184/SC 4	Data difficulties for interoperability	ISO 23247-3	List of basic information attributes for observable manufacture elements
Industrial data	ISO/TC 184/SC 4	Data difficulties for interoperability	ISO 23247-4	Technical requirements for exchanging information between entities within the reference
Internet of Things and digital twin	ISO/IEC JTC 1/SC 41	Difficulty in understanding IoT concept	ISO/IEC 20924:2021	Information technology — Internet of Things (IoT) — Vocabulary
Internet of Things and digital twin	ISO/IEC JTC 1/SC 41	Difficulty in understanding IoT concept	ISO/IEC TR 22417:2017	Information technology — Internet of Things (IoT) use cases
Internet of Things and digital twin	ISO/IEC JTC 1/SC 41	Difficulty in understanding IoT concept	ISO/IEC 29182-2:2013	Information technology — Sensor networks: Sensor Network Reference Architecture (SNRA) — Part 2: Vocabulary and terminology
Information security, cybersecurity and privacy protection	ISO/IEC JTC 1/SC 27	Lack of documentation of legacy systems and proprietary protocols	ISO/IEC 27001:2013 -	Information technology — Security techniques — Information security management systems — Requirements
Information security, cybersecurity, and privacy protection	ISO/IEC JTC 1/SC 27	Need to modernise equipment for digital transformation	ISO/IEC 27050-1:2019	Information technology — Electronic discovery — Part 1: Overview and concepts
Information security, cybersecurity, and privacy protection	ISO/IEC JTC 1/SC 27	Need to modernise equipment for digital transformation	ISO/IEC 27050-4	Information technology — Electronic discovery — Part 4: Technical readiness