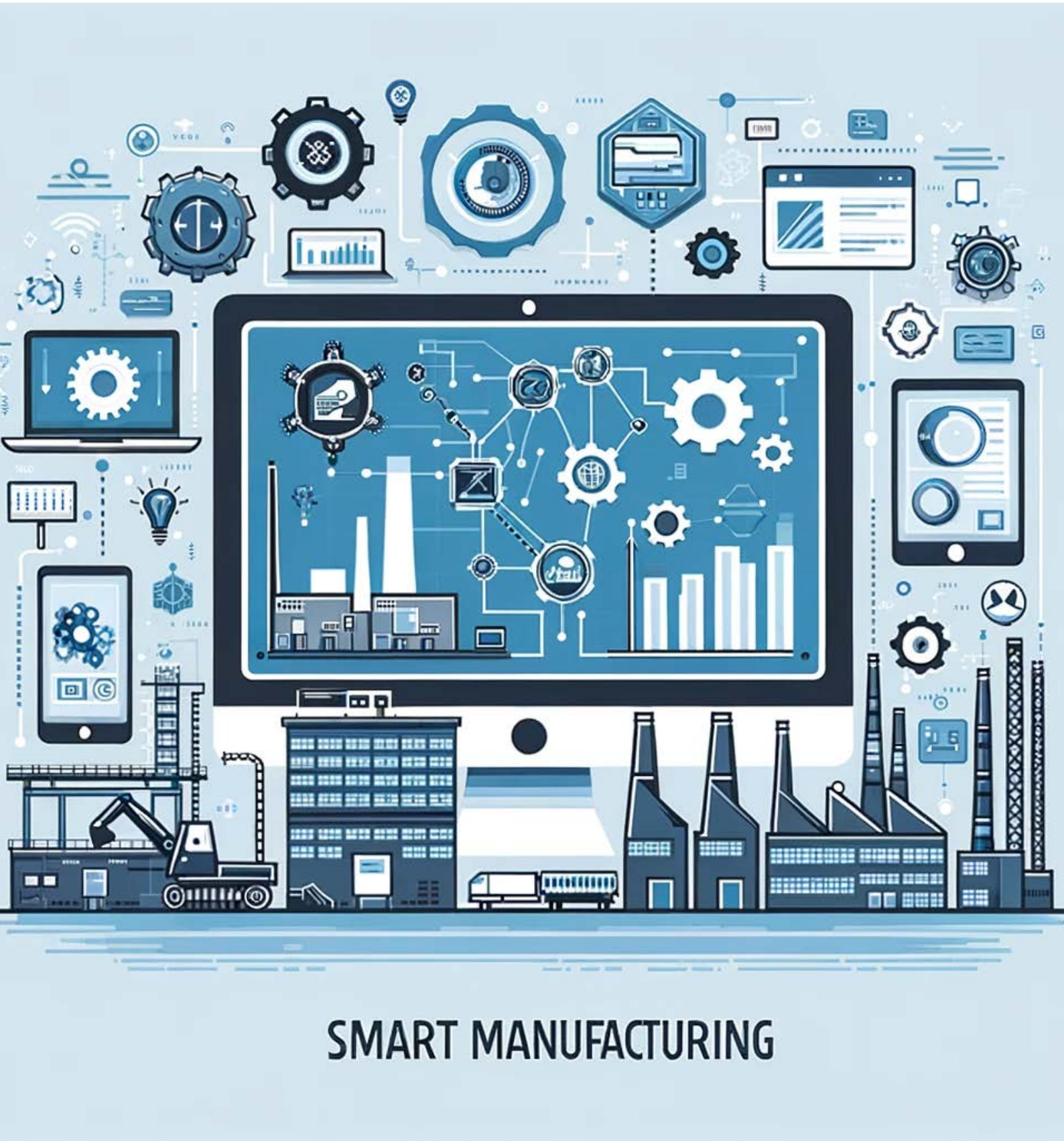
CEN-CENELEC-ETSI Coordination Group on Smart Manufacturing (SMa-CG)
Task Group Industrial Data

Recommendation Paper



Content

1 Executive Summary

This paper by the CEN-CENELEC-ETSI Coordination Group on Smart Manufacturing (SMa-CG) Task Group on Industrial Data explores the crucial role of standardization in managing industrial data, essential for industrial production and the lifecycle of goods and services. It emphasizes the need for interoperability, security, and effective data management to obtain optimal data usage.

The paper advocates for closer collaboration among standardization bodies and the adoption of new standardization processes aligned with modern software development practices.

Moreover, the paper calls for breaking down "data borders" to streamline standardization efforts and recommends aligning data semantics and machine-readable standards to support semantic interoperability. It also suggests incorporating industrial data spaces into the EU regulatory framework to align with existing IT and process support tools.

In essence, the paper highlights the balance between the fast pace of data technology development and the thorough integration offered by standardization processes, urging a review of current practices to prepare industries for future challenges and opportunities.

2 Aims

The primary goal of this paper is to assess the potential role of standardization in the field of industrial data. The term “industrial data” indicates the focus on industrial applications, cross-industry requirements such as interoperability, focusing on industrial data for supporting data economy, security of industrial data, cross-industry initiatives and more. This includes the use of digital twins, digital product passports, data spaces, virtual/augmented reality, industrial applications and further future technologies.

The paper focusses on general principles and potential institutional gaps in standardization work.

The paper provides a high-level analysis of existing standards and identifies gaps to promote interoperability and security of industrial data operations. This helps to assess whether a standardization roadmap will be necessary in the field of industrial data.
The aim of this paper is to provide recommendations based on the performed gap analysis to identify a list of actions supporting interoperability in the field of industrial data.

3 Introduction

In the rapidly evolving landscape of industrial data management, addressing specifically data interoperability and data quality, the intricacies of handling, securing, and utilizing data effectively are paramount. This paper, developed by the Task Group on Industrial Data of the CEN-CENELEC-ETSI Coordination Group on Smart Manufacturing (SMa-CG), delves into the multifaceted realm of industrial data, offering a limited overview with the aim of assessing whether a roadmap is going to be necessary in this field.

At the outset, "industrial data" is defined as data representing information that enables and supports the lifecycle of goods and services (see ISO 8000-2: 2022, 3.5.1.), whilst the term "industrial" refers to business-to-business relations in this document. This definition serves as the foundation for the exploration into various industrial initiatives, specifications, and standards related to industrial data.

Through this document, the aim is to shed light on some critical aspects: the semantics of digital data, the distinction between data and information, and the principles guiding data storage, exchange, and security. The significance of digital product passports, applications that leverage VR (virtual reality)/AR (augmented reality), operational (technical) data, and data aggregator/platforms, which are pivotal in industrial environment, are also explored.

Furthermore, the paper provides an overview of data security measures, outlining key principles and best practices for data storage and exchange. These principles are crucial for ensuring the integrity, availability, and confidentiality of industrial data.

In alignment with the evolving digital landscape, this paper also discusses the importance of regulatory frameworks and standardization in the context of industrial data. This includes a look at how international standards interact with industrial data management practices.

4 Overview of the ongoing (standardization) work on industrial data

Nowadays, industrial data related standardization processes might occur as an effort of international standardization bodies, such as ISO/IEC/ITU, regional standardization bodies, such as CEN/CENELEC/ETSI, national standardization bodies or by a temporary or permanent consortium of subject matter experts/members who are representing the industry and the future business adoption of the standardisation work, e.g. OPC UA, Catena-X, Manufacturing-X and more. The joint benefit from standardization initiated by different institutions is the increased quality and efficiency of the data exchange. In other words, standards which serve technological progress support the achievement of interoperability.

This chapter presents some well-known global and regional, as well as institutional and market driven initiatives on standardisation related to industrial data application. The presented list in the annex to this paper is not all encompassing, however, it represents major topics of interest and their initiators in the field.

Digitalisation is a process which is deeply integrated into industrial activities. From smart manufacturing to the logistics and transportation of the materials and components, there are highlighted concepts which initiated standardisation work around them. One of the examples is the "digital twin".

> **ISO/IEC 30173:2023** Digital twin Concepts and terminology defines as "digital twin DTw digital representation (3.1.8) of a target entity (3.1.3) with data connections that enable convergence between the physical and digital states at an appropriate rate of synchronization"
> Note 1 to entry: Digital twin has some or all of the capabilities of connection, integration, analysis, simulation, visualization, optimization, collaboration, etc.
> Note 2 to entry: Digital twin can provide an integrated view throughout the life cycle of the target entity.

In other words, a digital twin is a virtual representation of a real-world object or system. It spans the lifecycle of the object or system it represents, is updated from real-time data, and uses simulation, machine learning, and reasoning to aid decision-making.

The object being studied is outfitted with various sensors related to vital areas of functionality. These sensors produce data about different aspects of the physical object's performance, such as energy output, temperature, weather conditions, and more. This data is then relayed to a processing system and applied to the digital copy.

Once informed with such data, the virtual model can be used to run simulations, study performance issues, and generate possible improvements, all with the goal of generating valuable insights — which can then be applied back to the original physical object.

While a simulation typically studies a particular process, a digital twin can itself run any number of useful simulations in order to study multiple processes. Digital twins are designed

around a two-way flow of information that first occurs when object sensors provide relevant data to the system processor and then happens again when insights created by the processor are shared back with the original source.

There are various types of digital twins depending on the level of product magnification. The biggest difference between these twins is the area of application. It is common to have different types of digital twins co-exist within a system or process.

The digital twin concept was occupying regulatory institutions and subject matter experts in order to conceptualize its purpose and functionality, as well as to define a safe way of data related operations. Examples are the Eclipse Digital Twin and the standards by ISO/IEC JTC 1/SC 41 (Internet of things and digital twin), such as ISO/IEC 30173 (Digital twin - Concepts and terminology). Digital twins rely on data that they consume and generate in order to provide the user with a digitalised (and actionable) view of the real-world assets. Digital Twins may include diverse subsystems accountable for different functionalities. These subsystems could use different data exchange technologies, which might have been developed with no interoperability consideration[1]. This is an issue within ISO 23247 - digital twin framework for manufacturing – standard, which has provided a functional reference architecture for digital twins without explicitly addressing how to support interoperability.

While the digital twin concept was the subject of multiple regional and international standardisation initiatives, the Digital Product Passport (DPP) has been a special focus of the EU Commission and might shape the future of the industrial data. It is important to mention that the development of the regulatory framework around the DPP has not been completed at the moment of writing.

Within the EU, the DPP has been conceptualized at the political level as a reporting instrument of especially green and circular economies with features of data quality and interoperability supporting the digitalisation of SMEs and decentralized data governance. The EU wants to develop an interoperable DPP system and has issued a standardization request for the European Standardisation Organisations (ESOs) with a target date at the end.

In the request, EU suggests that DPP ecosystems specify a data structure. The resulting ecosystem can be considered a central catalyst for the digital and green transformation. The DPP approach will improve transparency and quality through value chains. The ESOs decided not to produce any sector specific standards but to coordinate the standardization of the passport technologies to avoid double work.

As per the final standardization request draft for the DPP from February 28th 2024, the EU requests harmonized standards on an interoperable DPP ecosystem by 31.12.2025 on:

1. Standard(s) on unique identifiers,
2. Standard(s) on data carriers and links between physical product and digital representation,

[1] H. da Rocha et al. "An interoperable digital twin with the IEEE 1451 standards," Sensors, vol. 22, no. 19, p. 7590, 2022

3. Standard(s) on access rights management, information, system security, and business confidentiality,
4. Standard(s) on interoperability (technical, semantic, organisation),
5. Standard(s) on data processing, data exchange protocols and data formats,
6. Standard(s) on data storage, archiving, and data persistence,
7. Standard(s) on data authentication, reliability, integrity ,
8. Standards on APIs for the DPP lifecycle management and searchability.

Recommendation: as it can be derived from both examples, any concept around industrial data should consider the interoperability aspect. For instance, it should decrease the workload on the implementation level and should contribute to the value chain and the product lifecycle. ***Interoperability forces an alignment not only on a technological level, but also on an institutional level.***

Recommendation: there are plenty of organisations founded to collaboratively develop new technologies in the context of industrial data, e.g. data space or the digital twin. Their efforts initiate certain standardization work with the purpose of interoperability. Most of such organizations are relatively new or/and are initiated by SMEs. Some of the organizations might have no link to the official regulatory bodies. The recommendation is to increase the level of cooperation amongst the institutions dealing with data related standardization work, as well as to leverage the awareness of the work performed on regional and international level. Clarity and alignment amongst the standards will improve the quality of the product, the levels of compliance and will ease the international commercial activities. At the same time, it will positively impact the consumer, who will not need to compromise on quality.

5 Basics of Data

5.1 Semantics of data

5.1.1 Data versus Information versus Knowledge

"Data" and "Information" are two related concepts that are sometimes used interchangeably even by experts in the industry, but they have distinct meaning when viewed in the context of knowledge.

Data refers to the facts and figures (or statistics), i.e. the "raw" form of knowledge. This means that data does not carry, on its own, any meaning, significance, or purpose. Put simply, data must be "interpreted" to have a meaning and it seems useless when viewed without context until it is formatted, analysed, and interpreted. In the context of this report, only machine-readable data is considered.

Information, on the other hand, is processed/interpreted data within a context to give it meaning, purpose, and relevance. The process of producing information entails the analysis, interpretation, and transformation of data into an "understandable" format that can, in turn, be used to construct knowledge (or message) that can be actionable.

Metadata is data associated to data that is typically necessary to interpret and use data, for example for the purpose of retrieving, using, or sharing them.

A ***data feature*** is a measurable property of the object we are trying to analyse. Features appear typically as columns in datasets. Each industrial segment defines the minimal set up of data features necessary for required information flow. This definition is based on use cases and data applications planned for a related process.

When used correctly, data (and the resulting information obtained from it) can drive smarter and faster business decisions. However, many organisations face barriers when trying to create a "data-driven" culture internally. Using inaccurate or outdated information is one of these main barriers.

Standardization is of utmost importance to ensure that data and related metadata are correctly interpreted as information. Lack of standardisation leads to the impossibility to interpret data consistently in different contexts and to the fragmentation of information.

In the context of Industry 4.0, machines, systems and products are increasingly connected to each other and are producing ever-growing volumes of data. This data can be transformed into meaningful insights using various analytical technologies. With modern techniques, such as artificial intelligence (especially machine learning), organizations gain valuable information about their business processes, products and production systems and establish an important basis for optimisation measures as well as new data-driven business models.

Knowledge is the *capability* of understanding the relationship between pieces of information and what to actually ***do*** with that information. In other words, knowledge involves understanding and expertise, i.e. understanding the rules needed to *interpret* the information. Knowledge therefore equals information + rules.

5.1.2 Semantics of Data

Semantics of data can be defined as the "meaning" and "use" of data, i.e. the reflection of the real world. In the information systems context, semantics represent a mapping between an object modelled in the information system (represented or stored, such as an "object" in a database) and the real-world object(s) it represents [2]. This mapping constitutes the semantics of the modelled object by describing the meaning and the use perspectives.

- There should be a differentiation between the "semantics of data" and the "semantics of the data within the context of the application". Existing applications might not exploit the data uses fully. In other words, more future uses/applications can be enabled if the data semantics were to capture the ***meaning***, whether in the current application context or other future ones.
- Semantics exist only when a form of an agreement between the parties observing the "real" situation is established. This agreement can be either formal or informal.
- Semantics have always existed, but what we need in any application/domain is the "interpretation" of the semantics, i.e. the interpretation *agent* derives the "meaning" behind an object.
- Semantics depends on humans and their interpretation of the world. Hence, it is difficult to address it in the context of machines.

5.1.2.1 Implicit vs. Explicit Semantics

In general usage, "explicit" means clearly expressed or readily observable whilst "implicit" means implied or expressed indirectly. Within the context of industrial data, M2M communication is designed in a way that the communicating parties exchange symbols and characters patterns between each other. The "meaning" of the exchanged pattern is derived/ensured via the "implicit" understanding of what the sequence/pattern is by the machine software developers, who have the same understanding of exchanged characters between the data sender and the data receiver. This exchange is often called information exchange with implicit or hidden semantics, where the meaning of the data (i.e. Information) is known by both communicating parties (Figure 1).

[2] Sheth, A. (1997). "Data semantics: what, where and how?" In Database Applications Semantics: Proceedings of the IFIP WG 2.6 Working Conference on Database Applications Semantics (DS-6) Stone Mountain, Atlanta, Georgia USA, May 30–June 2, 1995 (pp. 601-610). Springer US.

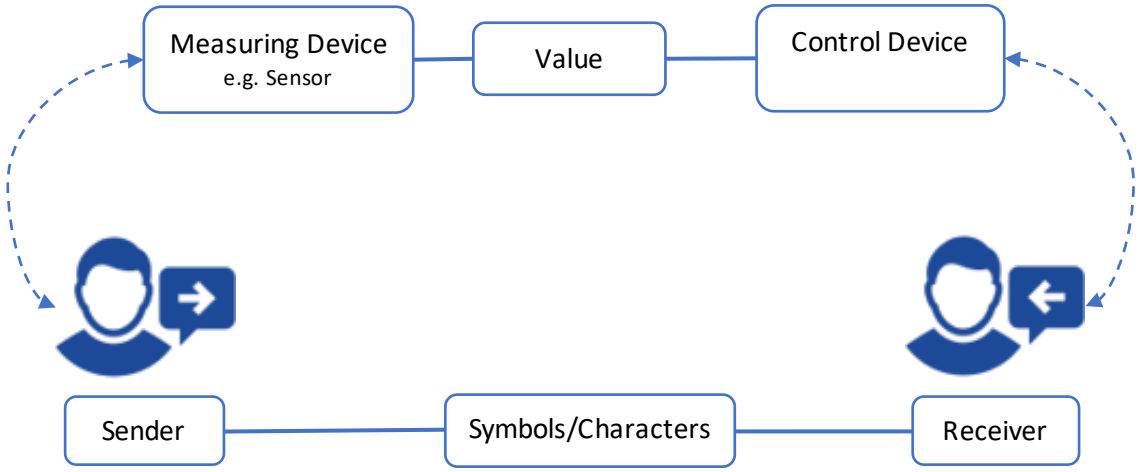


Figure 1: Information exchange

On the other hand, if an ID and value of data feature/property are exchanged between the interacting parties with an explicit reference to the "semantic model" that contains a definition of the feature/property, then a "data context" is provided in addition to the data communicated. Hence, an information exchange with explicit semantics has been established. This is only possible if both the data sender and data receiver use the same semantic data model. The unique ID references a concept/object within the semantic model, which contains the description of the semantic concept/object. The description of the concept contains various attributes, such as the name/title, data format, and unit. The description, therefore, provides the minimum "context" necessary to understand the value's meaning and turns it into information (Figure 2).

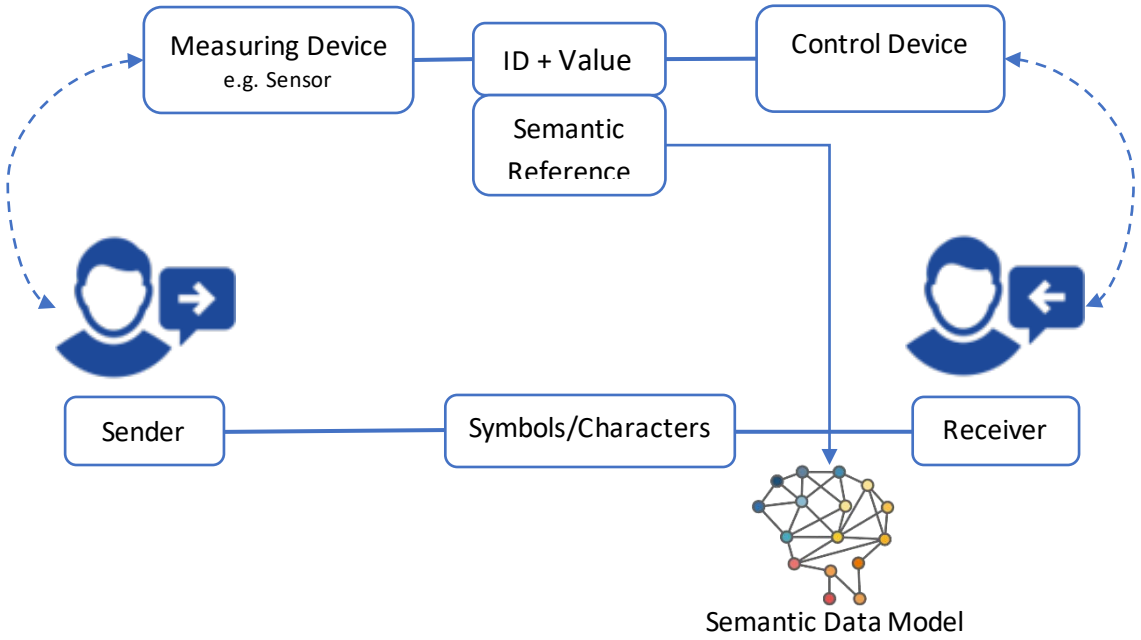


Figure 2: Sematic data model for information exchange

Standardization allows to express explicit semantics in a cross-sector context and is a key aspect of interoperability. Different technical standards exist in different sectors and

domains, standardization of semantics play a key role to ensure interoperability within and among common data spaces.

5.1.2.2 Examples

Monitoring includes periodic and trigger-based measurements of an event based on defined threshold. Any measurement outside of a threshold defines a trigger event. Measurements within a threshold are periodic.

Many manufacturing companies rely on critical and expensive goods that should be transported under special precautions guarantee (or they could be otherwise damaged). For example, components for the automotive sector (such as windshield wiper control systems that include sensors), the electronics industry, the machinery industry, or the chemical industries. Unfavourable environmental conditions such as temperature (high or low), humidity, light and air pressure pose various degrees of risks to these goods and components. These conditions are usually monitored during transportation and storage using sensors, and the respective industrial data generated are then transmitted via communication technologies. Therewith, potential risks can be detected early, and suitable necessary measures for risk mitigation can be taken.

As discussed previously, the measurement data on its own does not have a "meaning" and requires some "application" context and processing to turn into information. For instance, in the beforementioned example of transporting and storing sensitive goods, the sequence "21.1, 22.0, 21.5" is just data. However, if you put it into context: "The temperature of the warehouse in the last three minutes is 21.1° C, 22.0° C, and 21.5° C", it becomes information because it provides meaning and context. In order to make this information "actionable", it can be then compared to a pre-set threshold, which can trigger an action.

The number tuple "48.740528, 9.099550" has no meaning on its own, but in the context of a coordinate system (location measurement), it represents coordinates (Latitude, Longitude). Taking this a step further, these coordinates can be translated using "transformation" into an address on a map (contains the city and country), which is Nobelstrasse 12, 70569 Stuttgart, Germany. This in turn can then be cross-referenced with other information regarding buildings/organisations, which will result in the name of the institute "Fraunhofer IPA", whose coordinates are "48.740528, 9.099550".

Principles of message structure:

1. Based on pre-defined criteria;
2. Interoperability - a common information model and an agreed approach for data exchange (e.g. standardized API) guarantee secure and seamless data exchange amongst platforms or data aggregators;

   There are different layers to interoperability: In principle, data can be technically interoperable using open data format (e.g. CSV) and an easily parsable structure (e.g. JSON). However, an external system needs "meaning" to perform more operations on a particular dataset. This "meaning" has to be explicit through semantic interoperability.

   An "open" data format is one where the published specification describing the data is in the public domain and places no restrictions upon its use.

An open data format is important because it allows anyone to build the software tools required to work with that data.

Recommendation: the main criterion to the data structure is open data format to enable its implementation in various applications;

3. Minimum required to avoid fraud and overload;
4. Ability to include the context information, in order for the receiver (processing node) to determine how to process the message.;
5. Compatible with the security principles;
6. Verification that data was not tampered (optional).

5.1.3 Data interoperability

The concept of interoperability goes back to the early computer networks era (1960s-1980s). Before computer networks, the systems were isolated and lacked any standardized protocols to communicate. The ARPANET (precursor of the Internet) development marked an important step towards enabling data exchange and communication amongst different systems and networks.
Interoperability can be defined as the ability of different systems and services (or their components) to work together seamlessly, i.e. to have clear and shared expectations for the data contents, context, and meaning. Interoperable data is data held in different formats and locations, but can be used together smoothly, without having to go through a lengthy (expensive) consolidation process.
Different sectors and domains achieved internal interoperability with specific standardization. This was a market driven key aspect of the evolution of industry, but this led to fragmentation and creation of data silos. This paper does not address sectorial standardization, but it aims to identify standardization activities on top of existing standards to face this fragmentation and allow data sharing and use outside their original purpose.

5.2 Data security and efficiency in data exchange

Data security and efficiency are crucial aspects when dealing with industrial data for various reasons, and they play integral roles in the functioning and success of organizations, businesses, and even individuals.

On the international, regional and domestic levels, there is evidence of successful standardization efforts, supporting businesses to handle data in a secure and trusted manner. Data related business activities have no geographical boundaries, yet data security principles and regulations differ from one region to the other, having geography specific elements in its legislation. For example, the General Data Protection Regulation (GDPR) is an EU regulation that defines the standards for acquiring, managing and processing the personal data of EU citizens as well as EU residents. GDPR protects and regulates various sectors of information that can be tied to data subjects, such as IP information and location, unlike similar US data protection regulation that only limits this to a particular area, such as healthcare-related data.

Industrial data exchange can be performed within one industry segment or among diverse sectors of the industry, e.g. manufacturing, supply chain and more. In this case, the data handling amongst the interested parties is not always aligned due to non-aligned data related standards. It can be rightfully assumed that the gap is small, yet significant due to its potential impact on business activity. There is a limited number of standards that can be related as global and fit all types of industrial data-related operations worldwide and enable data-driven service to go beyond national or regional levels. Internationally respected standards of the ISO 27000 and IEC 62443 series are not covering all the business cases as well as operational needs. Domestic legislation, e.g. NIST SP 1800 in the US, ES in the UK as well as compliance frameworks/series (Control Objectives for Information and related Technology - COBIT, General Data Protection Regulation - GDPR) should also be taken into consideration. Data-related technology is however not necessarily a domestic or regional product, but potentially cross-national.

This chapter and the related appendix refer to the concept of data security and exchange as well as the basic principles for secure data storage and data operations. Moreover, it is concluded with the set of recommendations for increasing the efficiency in data related activities.

5.2.1 Data Security

Data security is essential in today's digital age to protect sensitive information from theft, data breaches, cyberattacks, and other forms of unauthorized access. It is a critical component of overall cybersecurity efforts and is crucial for maintaining the trust of customers, clients, and partners who entrust their data to organizations.
Data security refers to the practice of protecting digital data from unauthorized access, disclosure, alteration, or destruction. It involves implementing a range of measures, policies, and procedures to ensure that data remains confidential, integral, and available.

These principles are a summary of common considerations, they are critical for safe and secure data handling and transactions. However, those principles (see glossary) are not limiting. It is recommended to consider industrial, segmental, regional as well as international regulations and standards related to concrete business area for full compliance. For instance, even within the EU, the national data protection acts establish specific/additional requirements for the records of data-processing activities compared with GDPR regulation. The German Conference of Data Protection officers, for example, has published a blacklist of processing activities, for which a Data Protection Impact Assessment (DPIA) is mandatory, such as the use of artificial intelligence to process personal data to control the interaction with the data subject or to evaluate personal aspects of the data subject.

In addition, there are many different data security standards to choose from, each designed to address specific risks and protect different types of information. For instance, the ISO 27000 family of standards cover a wide range of information security topics, including risk management, security controls, and security management systems. The IEC 62443 series provides guidelines, requirements and recommendations for various stakeholders including product suppliers, system integrators and asset owners, covering the entire lifecycle of IACS from design and development, through deployment and maintenance, to decommissioning.

It encompasses aspects such as risk assessment, system security, network security, and security management practices. These standards aim to establish a framework to secure industrial communication networks and systems, addressing both cybersecurity risks and vulnerabilities within industrial sectors such as manufacturing, energy, chemical plants, and others.

In the US, The National Institute of Standards and Technology (NIST)'s SP 1800 standards series covers various aspects of information security, including risk management, incident response, and supply chain security.

It is a common practice to go through the standardization process in data related initiatives using web-based platforms to facilitate version control and collaboration for software development projects, e.g. GitHub.

Recommendation: standardization bodies to align amongst themselves and across various organizations on adoption of new standardization process related to data and cyber security, which are adapted to the common practices found in software development. This includes configurations integrated into a platform enabling automated testing and development capabilities.

Recommendation: in defining data security and exchange policy to consider the nature of the business: structure of the organisation, risk profile, budget, and resources on data security.

5.2.2 Data storage & locality

Data storage is indirectly connected to data security, since it plays a critical role in service provider's validation. The current technology development allows data harvesting using technology with different geographic origin. Location of the data indicates its regulatory framework for security and handling. The way data is stored shows the level of efficiency of its usage.

Data storage principles serve as guidelines for effectively managing stored data to ensure its availability, reliability, security, and performance. These principles are applicable to various types of data storage solutions, including databases, file systems, cloud storage, and more. These key data storage principles (see glossary) help organisations to effectively manage their stored data, reduce risks associated with data loss or breaches, and optimize storage resources for better performance and cost efficiency.

5.2.3 Data Exchange

A secure and efficient data exchange is crucial for protecting sensitive information as it moves between different systems, organisations, geographical locations, or individuals. To ensure the security of data exchange, the following principles should be considered:

By adhering to these data exchange security principles (see glossary), organisations can significantly reduce the risks associated with sharing sensitive information and maintain the confidentiality, integrity, and availability of their data.

Data exchange within one organisation in different geographies should be performed according to the global corporate policy on data security or using standardized data exchange infrastructure, such as data spaces. The exchange among different organisations within one geographic location pursues the principles dictated by domestic legislation. On the other hand, international data exchange should follow the international standards.

Recommendation: particularly in this field, an alignment with the existing international, regional, and national standards is needed.

Recommendation: standardization bodies to bring the efforts to alignment among the existing standards to enable secure international data related business activities.
An example is the integration of GDPR principles into the UK data security law (DPA). This practice can be referred to worldwide, bringing alignment and normalisation of the main data security principles, enabling international business activities on industrial data.

The main institutional challenge is the length of the standardization process. Data-related technology develops faster than a new standard or an alignment among the standards can be published.

6 Consistence of digital standards with established international standards and relation to EU single market

6.1 Breaking data boarders: enhancing digital standardization for future ready industries

The pace of digitalization development expanded the boundaries of industry expertise some time ago. Information technology (IT) and operational technology (OT) are becoming integrated, and the utilization of digitalization requires an even broader understanding and management of the overall picture. One of the key issues affecting the formation of this overall picture are the interfaces between the Standards Development Organisations (SDOs). Today, if a company wants to impact the relevant standards effectively, it typically needs to join multiple TCs. This creates both financial and worktime related demand for a company and its experts that wish to participate in the development of these standards.

For example, a large part of industrial data standardization is currently performed in the technical committees of both ISO and IEC, even though the standardization responsibilities have been separated between these two SDOs (Figure 3).

Two examples of ISO and IEC committees are:

- **ISO/TC 184** "*Automation systems and integration*" is the responsible committee 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.

- **IEC/TC 65** "*Industrial-process measurement, control and automation*" is the responsible committee for systems and elements used for industrial process measurement, control and automation.

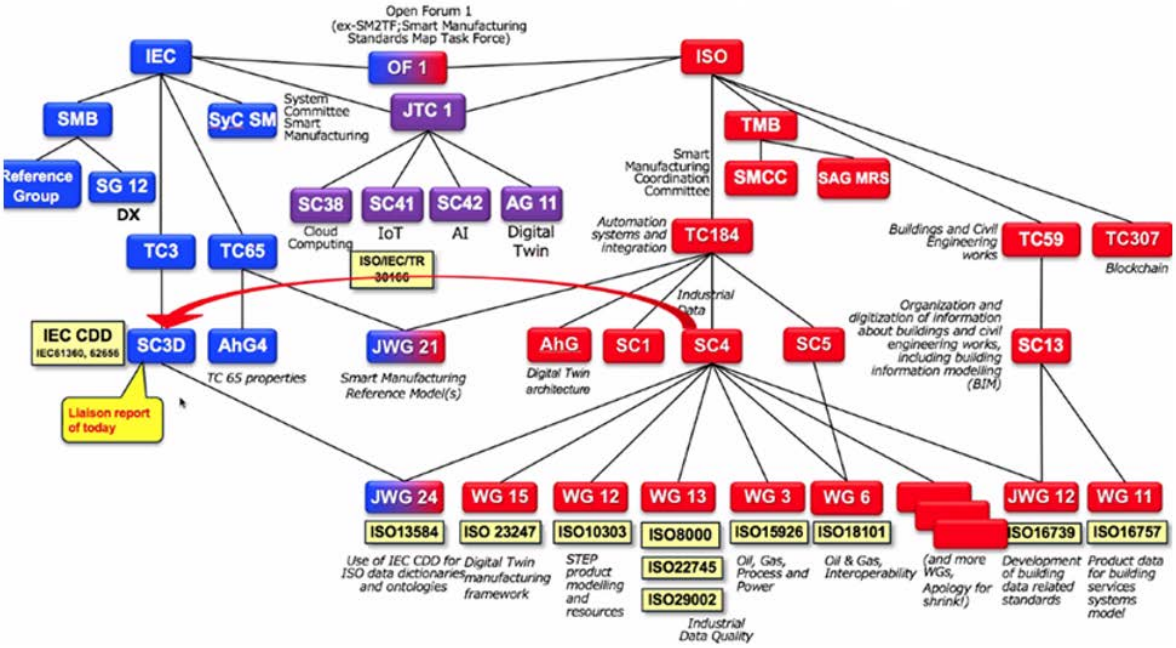


Figure 3. Examples of limited links between ISO and IEC regarding industrial data standardization.

Currently, the information transfer between these two committees occurs through the joint technical committees and through volunteer liaisons. This means that typically information transfer is not optimized as reporting is performed during yearly committee meetings. This slows the development of standards and can also lead to the duplication of work. A better visibility of the ongoing standardization work as well as the results should be one of the major goals of these organizations.

Similar "data borders" that hinder movement of information also exist in the European standardization field across CEN, CENELEC and ETSI. Industrial data demands a certain level of excellence in its exchange to reach interoperability and to be beneficial for business processes advances. Therefore, supporting systems for the transfer of information in horizontal fields such as industrial data, digitalization, and AI are required. In other words, a certain level of educative promotion of information on existing standards is essential to inspire technology developers and users to contribute to interoperability and become members of the open data interoperability forums.

Recommendation: standardization organisations should break-up the current "data borders", for instance on the EU level, between European ESOs (CEN, CENELEC and ETSI) in horizontal fields such as industrial data, digitalization, and AI. Increasing links between SDOs of these horizontal fields would likely increase stakeholder participation, lessen the duplication of work, and make it easier for stakeholders to form an overall image of the current level of standardization.

List of actions to improve coordination in the EU single market by creating an open standardization dataspace:

1) Making CEN, CENELEC and ETSI document portals compatible so that documents can be shared and transferred easily between related TCs;
2) Creating fixed and automated links between related TCs in the online portals for sharing of related documents. Current liaison system depends on the efforts of independent experts and typically reporting occurs mainly on an annual basis;

3) Organizing current industrial data, digitalisation, and AI standardization efforts into one coordinated database. Thus, making it possible for experts to access the data (name, scope etc.) from one database portal. Access could be limited to experts that are already participating in one of the related TCs in either CEN, CENELEC or ETSI;

4) Creation of horizontal technical committee between CEN, CENELEC and ETSI for industrial data. The standardization field has a broad scope, it could be "cut" into smaller groupings using sub-committees. This would make the distribution of information easier and would also make it possible to coordinate the standardization efforts at the level of one TC secretariat.

Digitization is an ongoing process linked to variety of aspects within the industrial value creation. Standardization is influenced by the digitalization penetration and is affected by the following:

1. The growing request for development of standards related to digitization and its products, such as digital twins, required semantics for data exchange, etc.
2. The requirement for machine-readable format as standard content to be applicable at different steps in industrial value creation processes.

It is undisputable that digitalization will be integrated gradually into the industrial process and that more data related needs will be covered by regulations and standards. Currently, a process to make this happen can be seen in standardization initiatives around data semantics. Aspects of semantic dictionaries and ontologies play central roles in interoperability of data exchange. Such dictionaries span semantics of data related to the broad variety of industrial spheres. Therefore, internationally standardized dictionaries could be a basis for semantic interoperability across industrial sectors.

According to IEC 61360-series, IEC 61987-series, IEC 62683-series, IEC 63213-series, IEC Common Data Dictionary (CDD) is an example of a globally standardized semantic dictionary. Traditionally this data dictionary is used to describe properties of products. However, it could be extended to describe the semantics of standards paving a way to machine readable standards.

Recommendation: a joint effort of the international standardization bodies should be aligned around the data semantics dictionaries. Data has no international boundaries; therefore, dictionaries should be internationally aligned.

Recommendation: standardization organisations should start to provide machine readable artefacts of their text-based standards for industrial applications where applicable.

An additional aspect which needs to be considered is the legal framework. In the EU single market, there is a well-established procedure to substantiate EU directives or regulations by so-called harmonized standards. This procedure is described within EU-directive 1025/2012.

The example of the DPP, presented in chapter 4, demonstrates a chance to interconnect the EU single market and the principles according to directive 1025/2012 with technical trends related to industrial data. Since industrial data platforms across value chains in different economic sectors (industrial data spaces) are connected directly to the industrial value creation, both aspects need to be considered together.

Recommendation: European Standardization Organisations and the EU Commission should start a dialogue on including aspects of so-called industrial data spaces in the EU regulatory framework of the EU single market.

6.2 Consistency with international standards

A protracted effort to develop and maintain standards for industrial data is being carried out in ISO/TC 184 SC 4, mainly promoted by various industries and industrial service sectors. The goal is to produce standards that cover the interoperability of systems and organisations in both the product description and process fields that span the entire product life cycle.

The most significant effect of the sharing of dictionaries, ontologies, reference models, and semantics has been the implementation of software tools by numerous vendors that can support entire value chains. Where the data and information thus produced become the subject of sharing among value chain actors, their governance and management also require a shared and interoperable approach.

A framework for data quality was thus developed in ISO standardization, addressing industrial data quality with the ISO 8000 series. In addition to defining general aspects of data and information quality, the focus is on *data governance* and *data quality assessment and management*. This family addresses master data, events, and transactions, IoT and sensors, and product shape data quality. The **ISO 8000 family** also deals with the exchange between organization of the *characteristic data* with ISO 29002. One key issue about the ISO 8000 approach is that data should not only be readable and understandable by a person, but also by a machine, in order to enable knowledge discovery and problem-solving using tools such as artificial intelligence as mentioned in sub-chapter 6.1.

As an example as foundation of industrial standards, the following two families of ISO standards are constantly reviewed to provide the updated basis for processes along the value chain of plant lifecycle, with focus on design, procurement, construction, operation & maintenance, dismission:

1. **ISO-10303 family**: established for the machine-interpretable representation and exchange of *product manufacturing information*.

2. **ISO-15926 family**: relates to industrial infrastructures, e.g. oil & gas plants, providing a strong basis for processes along the value chain of plant lifecycle, with focus on design, procurement, construction, operation & maintenance and dismission.

With the aim of supporting robust explicit semantic construction for interoperability, machine reasoning and knowledge discovery, the scientific and industrial community is developing industrial ontologies, for example in the EU project ONTO Commons (https://ontocommons.eu/).

ISO/TC 184 is developing an international standard for such a purpose, ISO-23726-3, an *Industrial Data Ontology* at working draft stage that defines an OWL2 ontology designed to support machine automated reasoning over information used in the design and through-life operation of complex, long-life, engineering assets. This standard in turn draws on many other generic or domain specific ontologies (ISO/IEC 21838, ISO-15926-2, ISO-15926-12).

Although there are conflicting positions within technical committees with respect to the practical manageability and length of the processes of defining complex tools such as ontologies, it is strongly advisable in the process of defining explicit semantics rules to develop, only if necessary, or better use one or more ontologies that are compatible with those already provided for or being developed in international standards.

Recommendation: European Standardization Organisations and the European Commission should take these standards into consideration to maintain compatibility with IT and process support tools for product/process development already used in many key industries. The European Standardization organizations should also participate in the process of defining and aligning the industrial ontologies underlying the development of reference models that are already standardized and require new standards.

Recommendation: technical committees of ISO, CEN, IEC and CLC dealing with industrial applications should be encouraged to provide semantic properties on aspects of the standards of their scope according to CDD. This enables semantic interoperability in data driven applications.

Recommendation: standardization organisations should include the aspect of industrial data in their efforts for digital standards. This includes technology, processes, and people's skills.

7 Recommendations and Conclusions

This paper, drafted by the CEN-CENELEC-ETSI Coordination Group on Smart Manufacturing (SMa-CG) Task Group on Industrial Data, discussed the complexities surrounding industrial data. It aimed to provide a foundational understanding, to assess current initiatives, and to explore the necessity of a comprehensive roadmap in the context of data handling, interoperability, security, and utilization in industrial settings.

Industrial data is identified as information crucial for the lifecycle of goods and services, with a specific focus on business-to-business relationships. This definition paves the way for an examination of various initiatives, specifications, and standards that play a pivotal role in managing industrial data effectively.

1. **Interoperability as a core requirement:** The document underscores the importance of interoperability in reducing implementation workloads, enhancing the value chain, and supporting the product lifecycle. A call for alignment at both technological and at SDOs levels is emphasized to foster seamless integration across the board.
2. **Collaborative efforts and standardization:** The growing number of organizations dedicated to developing new technologies related to industrial data, such as data spaces and digital twins, highlights the need for increased cooperation among standardization bodies. This collaboration is essential for achieving clarity, compliance, and facilitating international commercial activities without compromising quality.
3. **Adoption of new standardization processes:** Recommendations include urging standardization bodies to adopt new processes tailored to the nuances of the software development world e.g. for AI, data and cybersecurity. If the goal is to encourage new IT professionals to participate in standardization, effective management and open information sharing has to become the norm.
4. **Tailoring data security and exchange policies:** Policies should reflect the specific nature of a business, including its structure, risk profile, and available resources. Aligning with existing standards at international, regional, and national levels is crucial for ensuring comprehensive data security.
5. **Alignment amongst standards:** Efforts should be directed towards aligning existing standards to secure international data-related business activities. For instance, integrating GDPR principles into national laws can serve as a global model for data security.
6. **Breaking down data borders:** The paper advocates for increased collaboration between Standardization Organisations (SDOs) to eliminate "data borders," thereby enhancing stakeholder participation and streamlining standardization efforts.
7. **Focus on Data Semantics and Machine-Readable Standards:** A unified effort towards aligning data semantics dictionaries and providing machine-readable standards is called for to support semantic interoperability and facilitate the application of industrial data.
8. **Inclusion of industrial data in EU regulatory framework:** Dialogues between European Standardization Organisations and the EU Commission should begin to

incorporate industrial data spaces into the EU regulatory framework, ensuring compatibility with existing IT and process support tools.

This recommendation has brought up a few examples of Industrial Data initiatives, standards and processes to consider during the application of data related actions.

One of the main concerns is the issue of the development and publication of a commonly agreed document through a standardization body. A general challenge is the time taken for a data related initiative to become an adopted standard. The data related technology might develop and update its principles faster than the standardization process and adoption would happen without a standard.

On the contrary, speaking about industry related technology, slower adoption might become an advantage enabling the industrial stakeholders to integrate the data related technology deeper into the regular processes. The relatively "slow" speed presents an opportunity to deliver interoperability and guarantee that the standard adoption is well integrated into the existing process. **Therefore, the CEN-CENELEC-ETSI Coordination Group on Smart Manufacturing (SMa-CG) Task Group on Industrial Data recommends reviewing the current practices based on the provided recommendations.**

8 Glossary on the Basic Principles of Data management

8.1 Data Security

1. **Confidentiality**: Ensuring that data is only accessible to authorized individuals or systems. This typically involves user authentication, access controls, and encryption to prevent unauthorized access.

2. **Integrity**: Guaranteeing that data is accurate and has not been tampered with. Measures such as checksums, digital signatures, and version control help maintain data integrity.

3. **Availability**: Making sure that data is available when needed. Redundancy, backups, and disaster recovery plans help ensure data availability even in the face of hardware failures or other disruptions.

4. **Security Policies and Procedures**: Establishing clear security policies, guidelines, and procedures to govern data handling, access, and protection within an organisation.

5. **Security Awareness and Training**: Security is only as strong as the weakest link, which is usually the user. Educating employees and users about security best practices, potential threats, and the importance of data security.

6. **Authenticity**: Confirming the origin and legitimacy of data. Digital signatures, certificates, and audit trails can help establish data authenticity.

7. **Non-repudiation**: Protection against an individual falsely denying having performed a particular action. In data security context, it means an assurance that the sender is provided with proof of delivery, and the recipient is provided with proof of the sender's identity. Digital signatures and secure logs can provide non-repudiation.

8. **Data Classification**: Categorising data based on its sensitivity and importance. This allows for the application of appropriate security measures to protect the more-critical data.

9. **Access Control**: Implementing policies and mechanisms to limit access to data based on user's roles and privileges. The principle of least privilege is often applied to restrict access to only what is necessary for an individual's job.

10. **Encryption**: Encoding data to make it unreadable without the appropriate decryption mechanisms, such as public and private keys. Encryption is a fundamental component of data security, both in transit and at rest.

11. **Security Software**: Using firewalls, intrusion detection systems, antivirus software, and other security tools to prevent and detect security breaches.

12. **Incident Response and Recovery:** Developing a plan for responding to security incidents and recovering from data breaches or system failures.

13. **Compliance with Regulations**: Ensuring that data security measures align with industry-specific regulations and data protection laws, such as GDPR, HIPAA, or CCPA, as applicable.

8.2 Data storage & locality

1. **Data Classification**: Classify data based on its sensitivity, importance, and regulatory requirements. Assign appropriate storage and security measures to each class of data.

2. **Data Redundancy**: Implement data redundancy by maintaining multiple copies of critical data to ensure high availability and fault tolerance. Redundancy can be achieved through replication, backups, geographically dispersed data centres or clustering.

3. **Data Integrity**: Use checksums, hashing, and error-checking mechanisms to verify data integrity and detect any corruption or tampering during storage or transmission. ALCOA+ principles could be used as a guideline.

4. **Access Control**: Implement strict access controls and authentication mechanisms based on classification categories to ensure that only authorized users and systems can access and modify data. Enforce the principle of least privilege.

5. **Backup and Recovery**: Regularly back up data and establish a robust data recovery plan. Test backups periodically to ensure they can be restored successfully in case of data loss.

6. **Data Lifecycle Management**: Define clear data lifecycle policies that include data retention, archiving, and disposal. Automate data clean-up and archival processes to reduce storage costs and risks.

7. **Storage Scalability & capacity Planning**: Design storage systems to scale horizontally or vertically to accommodate growing data volumes and changing requirements. Continuously assess storage capacity needs and plan for future growth to avoid unexpected storage shortages.

8. **Data Compression**: Implement data compression techniques to reduce storage space and optimize data transfer speeds. Compress data before storage and decompress as needed. This reduces the potential for bottlenecks on the interface between the storage location and the application.

9. **Data Deduplication**: Eliminate excessive copies of data to save storage space and improve efficiency. Deduplication can be particularly useful for backup and archive systems.

10. **Hierarchical Storage Management (Storage Tiering)**: Use storage tiering to match data access patterns with appropriate storage media types. Frequently accessed data should be on high-performance storage, while less frequently accessed data can be moved to lower-cost, lower-performance storage.

11. **Data Storage Monitoring and Analytics**: Continuously monitor storage systems for performance, capacity, and security. Use diagnostic analytics to identify trends, predict resource needs, and detect anomalies.

12. **Data Versioning**: Implement version control for critical data to track changes, recover previous versions, and maintain a history of data modifications as well as audit trail.

13. **Data Replication**: Replicate data across geographically dispersed locations for disaster recovery and high availability. Replication can be synchronous or asynchronous, depending on the use case.

14. **Data Governance**: Establish data governance strategy, policies and practices to ensure data quality, integrity, consistency, security and compliance with regulatory requirements.

15. **Data Ownership**: Clearly define data ownership and responsibility within the organisation to ensure accountability for data management and protection.

16. **Regular Storage Maintenance**: Perform routine maintenance tasks, such as defragmentation and disk health checks, to optimize storage performance and reliability. Hence, the storage device's downtimes, repair time and cost will be minimized.

17. **Documentation**: Maintain comprehensive documentation of your data storage infrastructure, including configurations, policies, and procedures.

18. **Legal and Compliance**: Comply with relevant data protection laws and regulations, such as HIPAA, or CCPA, depending on your jurisdiction and industry.

19. **Data Placement**: Store data as close as possible to the processes or applications that require it. This can involve placing data on the same server, node, or storage device where the processing occurs.

20. **Caching**: Implement caching mechanisms to store frequently accessed data in memory or on faster storage devices. This reduces the need to fetch data from slower, remote sources, improving response times.

21. **Data Partitioning**: Divide large datasets into smaller, manageable partitions. This allows for parallel processing and reduces the amount of data that needs to be accessed at once.

22. **Co-location of Compute and Storage**: Whenever feasible, run computation and data storage on the same physical or virtual machines. This reduces the need for data to travel over a network.

23. **Data Replication**: Replicate data in multiple locations when high availability and fault tolerance are critical. This ensures that data remains accessible even if one copy becomes unavailable.

24. **Data Sharding**: Distribute data across multiple storage nodes or databases based on a pre-defined criterion, such as a range of values or a hash function. Sharding can improve data access parallelism, horizontal scaling and reduce contention.

25. **Data Affinity**: Assign data to specific processing nodes based on affinity rules, ensuring that the same data is consistently processed by the same node, without the cost of extra network calls and extra wire data.

26. **Load Balancing**: Use load balancing techniques to distribute data access requests evenly among available resources, preventing overloading of individual nodes.

27. **Data Movement Optimization**: When data movement is necessary, employ efficient data transfer protocols and algorithms to minimize the time and resources required for the transfer.

28. **Data Indexing**: Create and maintain efficient indexes for datasets to facilitate quick data retrieval, especially when querying large datasets.

29. **Data Access Patterns Analysis**: Monitor and analyse data access patterns to make informed decisions about data placement and optimization strategies.

8.3 Data Exchange

1. **Encryption**: Encrypt data both in transit and at rest (end-to-end encryption) using strong cryptographic algorithms. This ensures that even if data is intercepted, it remains unreadable without the appropriate decryption keys. In machine-to-machine communication preferable to disable a function of direct data penetration from hardware to the controlling cloud system.

2. **Authentication**: Verify the identity of both the sender and receiver before allowing data exchange. Use robust authentication mechanisms such as multi-factor authentication (MFA) to prevent unauthorized access.

3**. Data Integrity**: Employ measures such as hash functions to verify that data has not been tampered with during transit. Any alteration to the data should be detectable.

4. **Secure communication Protocols**: Use secure communication protocols such as HTTPS, SFTP, or SSH to transmit data. Avoid outdated and vulnerable protocols such as FTP or HTTP.

5. **Data Validation**: Check data for its consistency, accuracy and validity towards the indicated purpose.

6. **Logging and Monitoring**: Implement comprehensive logging and monitoring systems to track data exchange activities. This helps in detecting suspicious or unauthorized access and provides an audit trail for investigation.

7. **Data Minimization**: Only exchange the data necessary for the intended purpose. Minimize the amount of sensitive information in transit to reduce the potential impact of a breach.

8. **Secure APIs**: If using APIs for data exchange, secure them with proper authentication and authorization mechanisms. Implement rate limiting and consider API security best practices.

9. **Incident Response Plan**: Develop and regularly update an incident response plan to mitigate the impact of data breaches. This should include steps for containment, investigation, and notification.

10. **Vendor Assessment**: If working with third party vendors or partners for data exchange, assess their security practices and ensure they meet your security standards and policies.

11. **Regular Audits and Penetration Testing**: Conduct regular security audits and penetration testing to identify vulnerabilities and weaknesses in your data exchange processes and systems.

12. **Continuous Improvement**: Security is an ongoing process. Continuously review and improve your data exchange security measures based on evolving threats and industry best practices.

Annex

Smart Manufacturing Standards Mapping

1. ISO/IEC TR 63306-1 *Smart manufacturing standards map (SM2) - Part 1: Framework*
2. ISO/IEC TR 63306-2 *Smart manufacturing standards map (SM2) - Part 2: Catalogue*
3. IEC SRD 63456 *Navigation tools for smart manufacturing*
4. IEC 63339 TR ED1 *Unified reference model for smart manufacturing SMRM* (A meta-modelling analysis approach to smart manufacturing reference models) - The objective of the TR is to review the current status about smart manufacturing reference models and propose a meta-model to describe smart manufacturing reference models.
5. IEC TR 63283 *Smart manufacturing Series*
   i. IEC TR 63283-1 *Industrial-process measurement, control and automation - Smart manufacturing - Part 1: Terms and definitions*
   ii. IEC TR 63283-2 *Industrial-process measurement, control and automation - Smart manufacturing - Part 2: Use cases*
   iii. IEC TR 63283-3 *Industrial-process measurement, control and automation - Smart manufacturing - Part 3: Challenges for cybersecurity*

Manufacturing Operations View

1. IEC 62264 Series - *Enterprise-control system integration*
2. ISO 22400-1 *Automation systems and integration Key performance indicators (KPIs) for manufacturing operations management Part 1: Overview, concepts and terminology*
3. ISO 22400-2 *Automation systems and integration Key performance indicators (KPIs) for manufacturing operations management Part 2: Definitions and descriptions*
4. ISO/TR 22400-10 *Automation systems and integration Key performance indicators (KPIs) for manufacturing operations management Part 10: Operational sequence description of data acquisition*
5. IEC PAS 63088 *Smart manufacturing - Reference architecture model industry 4.0 (RAMI4.0)*
6. ISO/TR 18828-1 *Industrial automation systems and integration Standardized procedures for production systems engineering Part 1: Overview*
7. ISO 18828-2 *Industrial automation systems and integration Standardized procedures for production systems engineering Part 2: Reference process for seamless production planning*
8. ISO 18828-3 *Industrial automation systems and integration Standardized procedures for production systems engineering Part 3: Information flows in production planning processes*

9. ISO 18828-4 *Industrial automation systems and integration Standardized procedures for production systems engineering Part 4: Key performance indicators (KPIs) in production planning processes*
10. ISO 18828-5 *Industrial automation systems and integration Standardized procedures for production systems engineering Part 5: Manufacturing change management*
11. OPC-UA Foundation 'Companion' Standard adopted into formal IEC 61850 Series

Manufacturing Operations (Asset Management View)

1. ISO 55000 *Asset management Overview, principles and terminology*
2. ISO 55001 *Asset management systems requirements*
3. ISO 55002 *Asset management systems guidelines for the application of ISO 55001*

Manufacturing Operations (Energy View)

1. VDMA 34179 *Measurement instruction to determine the energy- and resource demand of machine tools for mass production*
2. ISO 14955 *Machine tools - Environmental evaluation of machine tools*
    iv. *Part 1: Design methodology for energy-efficient machine tools*
    v. *Part 2: Methods for measuring energy supplied to machine tools and machine tool components*
    vi. *Part 3: Principles for testing metal-cutting machine tools with respect to energy efficiency*
    vii. *Part 4: Principles for measuring metal-forming machine tools and laser processing machine tools with respect to energy efficiency*
3. ISO 20140 Series - *Evaluating energy efficiency and other factors of manufacturing systems that influence the environment*
    i. Part 1: Overview and general principles
    ii. Part 2: Environmental performance evaluation process
    iii. Part 3: Environmental performance evaluation data aggregation process
    iv. Part 5: Environmental performance evaluation data (References ISA 95 ISO 62264) Relationship between different aspects of the production facility
4. IEC 63376 *Industrial Facility Energy Management System (FEMS) - Functions and Information Flows*
5. IEC TS 62872-1 *Industrial-process measurement, control and automation. Internet of Things (IoT) - Application framework for industrial facility demand response energy management*
6. ISO 14040 *Environmental Management - Life cycle Assessment - Principles and framework*

Information Security

1. ISO/IEC 27001 /Amd 1 *Information security, cybersecurity and privacy protection – Information security management systems - climate action changes*
2. ISO/IEC 27002 *Information security, cybersecurity and privacy protection Information security controls*
3. ISO/IEC 27003 *Information technology Security techniques Information security management systems Guidance*

4. ISO/IEC 27004 *Information technology, Security techniques Information security management - Monitoring, measurement, analysis and evaluation*
5. ISO/IEC 27005 *Information security, cybersecurity and privacy protection - Guidance on managing information security risks*

IEC 62443 Industrial communication networks - network and system security series

1. IEC 62443-1-1 *Terminology, concepts and models*
2. IEC TS 62443-1-3 *DC Performance Metrics for IACS Security*
3. IEC TS 62443-1-5 *DTS Scheme for IEC 62443 security profiles*
4. IEC 62443-2-1 *Security program requirements for IACS asset owners*
5. IEC 62443-2-2 CD *IACS Security Protection*
6. IEC TR 62443-2-3 *Patch management in the IACS environment*
7. IEC 62443-2-4 *Security program requirements for IACS service providers*
8. IEC TR 62443-3-1 *Security technologies for IACS*
9. IEC 62443-3-2 *Security risk assessment for system design*
10. IEC 62443-3-3 *System security requirements and security levels*
11. IEC 62443-4-1 *Secure product development lifecycle requirements*
12. IEC 62443-4-2*Technical security requirements for IACS components*

Knowledge Management

1. ISO 30401 *Knowledge management systems – Requirements*
2. ETSI GS CIM 006 – *NGSI-LD Information model*

ISO 8000 Data Quality Series

1. ISO/TS 8000-1 *Data quality - Part 1: Overview (ED2 Draft)*
2. ISO 8000-2 *Data quality - Part 2: Vocabulary*
3. ISO 8000-8 *Data quality - Part 8: Information and data quality: Concepts and measuring*
4. ISO/DIS 8000-51 *Data quality - Part 51: Data governance: Exchange of data policy statements (ED1 in Development)*
5. ISO/TS 8000-60 *Data quality - Part 60: Data quality management: Overview*
6. ISO 8000-61 *Data quality - Part 61: Data quality management: Process reference model*
7. ISO 8000-62Data quality - *Part 62: Data quality management: Organizational process maturity assessment: Application of standards relating to process assessment*
8. ISO 8000-63Data *quality - Part 63: Data quality management: Process measurement*
9. ISO 8000-64 Data quality - *Part 64: Data quality management: Organizational process maturity assessment: Application of the Test Process Improvement method (ED1 in Development)*
10. ISO 8000-65 *Data quality - Part 65 Data quality management: Process measurement questionnaire*
11. ISO 8000-66 *Data quality - Part 66: Data quality management: Assessment indicators for data processing in manufacturing operations*
12. ISO/TS 8000-81 *Data quality - Part 81: Data quality assessment: Profiling*

13. ISO/PRF TS 8000-82 *Data quality - Part 82: Data quality assessment: Creating data rules (ED1 in Development)*
14. ISO 8000-100, *Data quality - Part 100: Master data: Exchange of characteristic data: Overview*
15. ISO 8000-110 *Data quality - Part 110: Master data: Exchange of characteristic data: Syntax, semantic encoding, and conformance to data specification*
16. ISO/AWI 8000-114 *Data quality - Part 114: Master data: Application of ISO/IEC 21778 and ISO 8000-115 to portable data (ED 1 In Development)*
17. ISO 8000-115, *Data quality - Part 115: Master data: Exchange of quality identifiers: Syntactic, semantic and resolution requirements*
18. ISO 8000-116 *Data quality - Part 116: Master data: Exchange of quality identifiers: Application of ISO 8000-115 to authoritative legal entity identifiers*
19. ISO/DIS 8000-117 *Data quality - Part 117: Application of ISO 8000-115 to identifiers in distributed ledgers including blockchains*
20. ISO 8000-120 *Data quality - Part 120: Master data: Exchange of characteristic data: Provenance*
21. ISO 8000-130 *Data quality - Part 130: Master data: Exchange of characteristic data: Accuracy*
22. ISO 8000-140 *Data quality - Part 140: Master data: Exchange of characteristic data: Completeness*
23. ISO/TS 8000-150 *Data quality - Part 150: Master data: Quality management framework*
24. ISO/AWI 8000-210 Data quality - Part 210: Part 210: *Sensor data: Data quality characteristics*
25. ISO/TS 8000-311 *Data quality - Part 311: Guidance for the application of product data quality for shape (PDQ-S)*
26. ISO/AWI TR 8000-320 *Data quality — Part 320: AI training data quality for smart manufacturing*
27. ISO/FDIS 55013 *Asset management - Guidance on the management of data assets (Value)*

Digital Product Passport - Using AAS (Asset Administration Shell) with industrial components products

1. IEC 63278-1 *Asset Administration Shell for industrial applications - Part 1: Asset Administration Shell structure*
2. IEC 63365 *Industrial process measurement, control and automation - Digital nameplate*
3. IEC 61406 (DIN SPEC 91406) is part of the sub-model "Identification",
4. VDI 2770 is part of the sub-model "Documentation"
5. DIN SPEC 9012 *Aerospace Digital Certificate of Conformity (e-CoC) - Requirements, design and structure*

Industrial Control System (Focused Data Semantics)

1. IEC 62683-1 *Switchgear and control gear - Product data and properties for information exchange - Part 1: Catalogue data*
2. IEC 61360 CCD (*Common Data Dictionary*),

3. ISO 13584-42 *Description methodology: Methodology for structuring parts families*
4. IEC 61987 Series LOP (List of Properties), ISO 22745 Series OTD (Open Technical Dictionaries),
5. ISO/TS 29002 *Series ECD (Exchange of characteristic data)*
6. IEC 61804 *Series EDDL (Electronic Device Description Language)*
7. IEC 62453 *Series FDT (Field Device Tool)*
8. ISO 13399 *Series CTDR-E (Cutting Tool Data Representation and exchange)*
9. IEC 62832-1 *Digital Factory framework Series*
    i. *IEC 62832-1 PRV Industrial-process measurement, control and automation - Digital Factory framework - Part 1: General principles*
    ii. *IEC 62832-2 PRV Industrial-process measurement, control and automation - Digital Factory framework - Part 2: Model elements*
    iii. *IEC 62832-3 PRV Industrial-process measurement, control and automation - Digital Factory framework - Part 3: Application of Digital Factory for life cycle management of production systems*
10. IEC 62714 Series - *Engineering data exchange format for use in industrial automation systems engineering - Automation markup language*
11. IEC 60617 *DB Graphical symbols for diagrams*
12. IEC 81346-2 *Industrial systems, installations and equipment and industrial products - Structuring principles and reference designations - Part 2: Classification of objects and codes for classes*
13. DIN 3168 *Coolers for distribution boxes; concepts testing, marking*
14. IEC 61439 *Low-voltage switchgear and controlgear assemblies– Part 1: General rules*
15. IEC 81346-1 *Industrial systems, installations and equipment and industrial products - Structuring principles and reference designations - Part 1: Basic rules*
16. IEC 61355 *Collection of standardized and established document kinds*
17. IEC TR 60890 *A method of temperature-rise verification of low-voltage switchgear and control gear assemblies by calculation*

Part Library (Focused Data Semantics)

1. ISO 13584 *Part Library Series*
2. ISO/TS 15926 *Industrial automation systems and integration - Integration of life-cycle data for process plants including oil and gas production facilities*
3. ISO/TS 18101-1 *Automation systems and integration - Oil and gas interoperability - Part 1: Overview and fundamental principles*

BIM (Building Information Management)

1. ISO 23386 *Building information modelling and other digital processes used in construction — Methodology to describe, author and maintain properties in interconnected data dictionaries*
2. ISO 19650-1 *Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) - Information management using building information modelling*
3. ISO 16757 *Data structures for electronic product catalogues for building services document delivery - Exchange specification - Part 1: Container*

4. ISO 16739-1 *Industry Foundation Classes (IFC) for data sharing in the construction and facility management industries - Part 1: Data schema*
5. ISO 16354 *Guidelines for knowledge libraries and object libraries*
6. ISO/TS//WD 12911 *Framework for building information modelling (BIM) guidance*
7. ISO 12006-2 *Building construction - Organization of information about construction works - Part 2: Framework for classification*
8. IISO/DTR 23262.2 *GIS (Geospatial) / BIM interoperability*
9. ISO 23387 *Building information modelling (BIM) - Data templates for construction objects used in the life cycle of any built asset - Concepts and principles*
10. ISO 15686 *Buildings and constructed assets - Service life planning*

Digital Twin focused signposted standards

- note digital twins can come from any of the above listed and more semantic data standards but these IEC/ISO focused publications try to summaries these more formally

1. ISO/DIS 23247 Series - *Digital Twin framework for manufacturing Part 1-4*
2. ISO/IEC 30173 *Digital twin Concepts and terminology*
3. ISO 23247 Series *Automation systems and integration Digital twin framework for Manufacturing (Part 1-4)*
4. ISO/IEC TR 30172 *Internet of things (loT) Digital twin Use cases*
5. ISO/TR 24464 *Automation systems and integration Industrial data Visualization elements of digital twins*
6. ISO 16100 Series - *Industrial automation systems and integration - Manufacturing Software Capability Profiling for Interoperability*
7. ISO/TR 18161 *Automation systems and integration - Applications integration approach using information exchange requirements modelling and software capability profiling*
8. ETSI GR CIM 017 *Feasibility of NGSI-LD for Digital twins*
9. ETSI TR 103 844 *SmartM2M; Digital Twins and Standardization Opportunities in ETSI*
10. ETSI TS 103 845 *SmartM2M; Digital Twins Communication Requirements*
11. ETSI DTS/SmartM2M-103846 (TS 103 846) *SmartM2M; Digital Twins: Functionalities and communication Reference Architecture*
12. ETSI DTR/SmartM2M-103847 (TR 103 847) *SmartM2M; Digital Twins communication support in oneM2M*
    ETSI DEN/SmartM2M-303760 (EN 303 760) *SmartM2M; SAREF Guidelines for IoT Semantic Interoperability; Develop, apply and evolve Smart Applications ontologies*

1. Software and Systems Engineering - Interoperability Related Standards

1. ISO/IEC/IEEE 29119 Series - *Software and systems engineering - Software testing*
2. ISO/IEC/IEEE 15288 *Systems and software engineering - System life cycle processes*
3. ISO/TS 18876-1 *Industrial automation systems and integration - Integration of industrial data for exchange, access and sharing - Part 1: Architecture overview and description*

4. ISO/TS 18876-2 *Industrial automation systems and integration - Integration of industrial data for exchange, access and sharing - Part 2: Integration and mapping methodology*
5. ISO 22549-1 *Automation systems and integration - Assessment on convergence of informatization and industrialization for industrial enterprises Part 1: Framework and reference model*
6. ISO 22549-2 *Automation systems and integration - Assessment on convergence of informatization and industrialization for industrial enterprises - Part 2: Maturity model and evaluation methodology*
7. ISO/TR 16161 *Automation systems and integration - Use case of capability profiles for cooperation between manufacturing software units*
8. IEC 61069-5 *Industrial-process measurement, control and automation - Evaluation of system properties for the purpose of system assessment - Part 5: Assessment of system dependability*
9. IEC 61709 *Electric components - Reliability - Reference conditions for failure rates and stress models for conversion (MTBF)*
10. ISO 16400-1 *Automation systems and integration - Equipment behaviour catalogues for virtual production system – Part 1: Overview*
11. ISO 16400-2 *Automation systems and integration - Equipment behaviour catalogues for virtual production systems - Part 2: Formal description of a catalogue template*
12. ISO 16400-3 *Automation systems and integration - Equipment behaviour catalogues for virtual production system - Part 3: Requirements and* recommendations for construction of an equipment instance model
13. ISO/AWI 16400-4 *Automation systems and integration - Equipment behaviour catalogues for virtual production system - Part 4: Application method*
14. ISO/AWI 16400-5 *Automation systems and integration - Equipment behaviour catalogues for virtual production system - Part 5: Part 5: Integration of EBC templates in production system design and operation*
15. ISO/IEC/IEEE 42010 *Software, systems and enterprise - Architecture description*
16. ISO/IEC/IEEE 42020 *Software, systems and enterprise - Architecture processes*
17. ISO/IEC/IEEE 42030 *Software, systems and enterprise – Architecture evaluation framework*
18. ISO/IEC/IEEE 24641 *Systems and Software engineering - Methods and tools for model-based systems and software engineering (MBSE)*
19. ISO/IEC/IEEE 41062 *Software engineering - Recommended practice for software acquisition*
20. ISO/IEC/IEEE 12207 *Systems and software engineering - Software life cycle processes*
21. ISO/WD 23726-3 *Automation systems and integration Ontology based interoperability Part 3: Industrial data ontology*
22. ISO 11354-1 *Advanced automation technologies and their applications — Requirements for establishing manufacturing enterprise process interoperability — Part 1: Framework for enterprise interoperability*
23. ISO 11354-2 *Advanced automation technologies and their applications - Requirements for establishing manufacturing enterprise process*

interoperability - Part 2: Maturity model for assessing enterprise interoperability.

24. ISO 16100-1 *Industrial automation systems and integration - Manufacturing software capability profiling for interoperability - Part 1: Framework*
25. ISO 16100-1 *Industrial automation systems and integration - Manufacturing software capability profiling for interoperability - Part 1: Framework*
26. ISO 16100-4 *Industrial automation systems and integration - Manufacturing software capability profiling for interoperability - Part 4: Conformance test methods, criteria and reports*
27. ISO 16100-6 *Industrial automation systems and integration - Manufacturing software capability profiling for interoperability - Part 6: Interface services and protocols for matching profiles based on multiple capability class structures*
28. ISO 16300-1 *Automation systems and integration - Interoperability of capability units for manufacturing application solutions - Part 1: Interoperability criteria of capability units per application requirements*
29. ISO 16300-2 *Automation systems and integration - Interoperability of capability units for manufacturing application solutions - Part 2: Capability templates and software unit cataloguing*
30. ISO 16300-3 *Automation systems and integration - Interoperability of capability units for manufacturing application solutions - Part 3: Verification and validation of interoperability among capability units*
31. ISO 16300-4 *Automation systems and integration - Interoperability of capability units for manufacturing application solutions - Part 4: Capability unit assessment for the manufacturing application requirements*
32. ISO 15745 Series (Part 1-5) *Industrial automation systems and integration - Open systems application integration framework*
33. ETSI GS CIM 009 – NGSI-LD API
34. ETSI TS 103 673: *SmartM2M; SAREF Development Framework and Workflow, Streamlining the Development of SAREF and its Extensions*
35. ETSI TS 103 264: *SmartM2M; Smart Applications; Reference Ontology and oneM2M Mapping"*
36. ETSI TS 103 548: *SAREF consolidation with new reference ontology patterns, based on the experience from the SEAS project*
37. ETSI TS 103 410-1: *SmartM2M; Extension to SAREF; Part 1: Energy Domain*
38. ETSI TS 103 410-2: *SmartM2M; Extension to SAREF; Part 2: Environment Domain*
39. ETSI TS 103 410-3: *SmartM2M; Extension to SAREF; Part 3: Building Domain*
40. ETSI TS 103 410-4: *SmartM2M; Extension to SAREF; Part 4: Smart Cities Domain*
41. ETSI TS 103 410-5: *SmartM2M; Extension to SAREF; Part 5: Industry and Manufacturing domains*
42. ETSI TS 103 410-6: *SmartM2M; Extension to SAREF; Part 6: Smart Agriculture and Food Chain Domains*
43. ETSI TS 103 410-7: *SmartM2M; Extension to SAREF; Part 7: Automotive Domain*
44. ETSI TS 103 410-8: *SmartM2M; Extension to SAREF; Part 8: eHealth/Ageing-well Domain*

45. ETSI TS 103 410-9: *SmartM2M; Extension to SAREF; Part 9: Wearables Domain*
46. ETSI TS 103 410-10: *SmartM2M; Extension to SAREF; Part 10: Water Domain*
47. ETSI TS 103 410-11: *SmartM2M; Extension to SAREF; Part 11: Lift Domain*