Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

A reference framework for the implementation of data governance systems for industry 4.0

Marta Zorrilla [*,a], Juan Yebenes [b]

[a] Lecturer in Computer Science Department at University of Cantabria (Spain) Facultad de Ciencias Avda. Los Castros s/n. 39005 Cantabria, España
[b] PhD student in Computer Science Department at University of Cantabria (Spain) Facultad de Ciencias Avda. Los Castros s/n. 39005 Cantabria, Espaa

ARTICLE INFO

Keywords:
Data governance
Data-Centric architecture
Industry 4.0
Big data
IoT

ABSTRACT

The fourth industrial revolution, or Industry 4.0, represents a new stage of evolution in the organization, management and control of the value chain throughout the product or service life cycle. This is mainly based on the digitalization of the industrial environment by means of the convergence of Information Technologies (IT) and operational Technologies (OT) through cyber-physical systems and the Industrial IoT (IIoT) and the use of data generated in real time for gaining insights and making decisions. Therefore data becomes a critical asset for Industry 4.0 and must be managed and governed like a strategic asset. We rely on Data Governance (DG) as a key instrument for carrying out this transformation. This paper presents the design of a specific governance framework for Industry 4.0. First, this contextualizes data governance for Industry 4.0 environments and identifies the requirements that this framework must address, which are conditioned by the specific features of Industry 4.0, among others, the intensive use of big data, the cloud and edge computing, the artificial intelligence and the current regulations. Next, we formally define a reference framework for the implementation of Data Governance Systems for Industry 4.0 using international standards and providing several examples of architecture building blocks.

1. Introduction

"Industry 4.0" (I4.0) term refers to the fourth industrial revolution, or said in other words, the transformation of production processes taking advantage of the abundant information available in each stage of the value chain, from suppliers to customers, of any industrial sector (manufacturing, energy, transport, supplies, mining, health, pharmaceutical, etc.) [1].

I4.0 is mainly characterized by the integration of Information Technologies (IT) and operational Technologies (OT) [2], that means, the convergence of the physical and digital world through cyber-physical systems and the Industrial IoT. This leads to a radical change in the production model, which becomes based on the ubiquity and connectivity of data, people, processes, services and cyber-physical systems, as if it were a social network in which all actors (network nodes) exchange and exploit the information generated at each level and whose main consequence is the increase in the amount and variety of data generated in real time from different sources. In this complex environment in which the generation of processable information is huge, data becomes a critical asset which must be conveniently governed.

In order to achieve the functionality required by I4.0, it is necessary to develop and adopt methods, technologies and tools aimed at managing the specific characteristics of industrial processes, such as having high computing capacity in any fixed or mobile environment (*Mobile Computing*); the ability to manage large volumes of data in real time coming from a large number of heterogeneous devices, many of them are legacy systems, satisfying strict latency requirements (*Big Data*); dynamic scaling of computing capacity according to changes in the workloads (*Cloud and Fog Computing*); the dynamic interaction of applications with intelligent environments and sensor networks (*IE and IoT*) as well as the use of artificial intelligence and machine learning (*AI and ML*) in decision-making tasks. All of these disciplines are hot topic in big data research [3].

Nowadays, third platforms (3P) are considered the most appropriate solution to the technological challenge posed by I4.0, given that, among other features, they are based on distributed and scalable architectures, which allow the interconnection of a large number of devices that can be dynamically dimensioned according to the required processing capacity.

In this complex environment, data becomes a key asset for the business, so adopting a data-centric model (Data-Centric) is of crucial

* Corresponding author.
E-mail address: marta.zorrilla@unican.es (M. Zorrilla).

https://doi.org/10.1016/j.csi.2021.103595
Received 9 January 2021; Received in revised form 14 October 2021; Accepted 30 October 2021

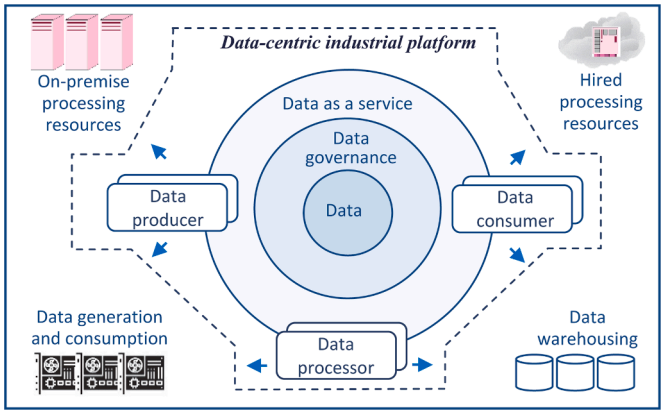


Fig. 1. General overview of RAI4.0 architecture.

importance [4]. In this model, data is separated from applications and technology platforms, which avoids the appearance of data silos and enables data to be shared and used by the entire organization [5] and its third parties.

However, in order for data to become a competitive advantage for the company, it must be managed and governed like any other strategic asset, and this is the reason why it is necessary to implement a Data Governance system (DG system) whose purpose is to establish and enable in the organization the necessary capacities to carry out shared and communicated decision-making, authority and control on the management of data assets and define who has the decision-making rights and responsibilities in the data-related processes [6].

Although most organizations carry out DG tasks [7] at some degree, the changes that I4.0 entails, such as the adoption of technologies that support 3P [8] and inter-company collaboration, regulatory aspects and service levels agreements (SLA) signed with third parties, add additional complexity to the DG system. This, along with the specific characteristics that industrial environment must meet, has led us to elaborate a framework for the development of data governance systems appropriate to the I4.0 supported by 3P, after checking, through a systematic literature review [9], its nonexistence. This framework is part of the RAI4.0 [10] reference architecture, where data and its government are situated in the center (see Fig. 1) and its design is based on three basic principles: Data-as-a-Service (DaaS), Platform-as-a-Service (PaaS) and Monitoring-as-a-Service (MaaS).

The main contribution of this paper is the proposal of a formal reference framework for the implementation of data governance systems for companies moving towards I4.0. Previously, this work relates both the set of requirements of DG and specific of I4.0 that must be met. This paper describes in greater detail and extends the work published in IEEE for the Spanish-speaking community [11].

After this introduction, Section 2 delimits the context of data governance and identifies the requirements that a governance framework must address and that are conditioned by the specific characteristics of I4.0. Section 3 sets out the aspects, both conceptual and normative, on which we have based the development of the reference framework. Section 4 presents the framework for the construction of DG systems for I4.0 and develops some building blocks. Likewise, this briefly describes the maturity model associated to DG framework proposed. Finally, Section 5 draws the conclusions and contributions of this work, while proposing future lines of research.

2. Data governance system requirements

As a previous step to the development of a framework for the implementation of DG Systems for I4.0, first it is necessary to establish the requirements that a DG system must meet.

2.1. Purpose of a DG system

A DG system is intended to enable and establish in the organization the necessary capabilities to exercise consensual and communicated decision-making, authority and control about the management of data assets and to define who has the decision-making rights and responsibilities in data-related processes [6].

The DG system is conditioned by the mission, strategy, standards and culture of the organization [12] so that this can manage its data as a strategic asset. For this reason, the DG system must orchestrate people, processes and technologies [13] and must be transversal to the main departments of the organization [14]. Likewise the DG must also guide activities related to data management. In short, the DG ensures that data is managed in the appropriate way, while the Data Management (DM) is responsible for the managing of data in order to achieve the organization's objectives [6], following the guidelines established by the DG.

The DG system must establish [15]:

- The scope of decision-making in relation to data governance. It refers to identify what activities and what specific aspects related to data should be governed.
- The roles involved in the decision-making processes. Some frequently mentioned roles in the literature are data stewards, data owners, and data committees, among others.
- How the roles involved are related to decision making. It refers to the decision-making rights, authority, and responsibilities assigned to roles.

2.2. General DG system requirements

According to [16], there are six requirements that a governance system must meet, which we assume and apply to our DG system:

- It satisfies the needs of stakeholders and generates value from the use of data.
- It is made up of a number of components that must work together as a whole.
- It is dynamic and, therefore, each time a change occurs, the impact it produces on the system must be considered.
- It clearly distinguishes between the activities and structures of Data Governance and Data Management.
- It must be adjusted to the needs of the organization.
- It covers and takes into account the whole organization (in I4.0, it covers the complete value chain from suppliers to the end customer).

2.3. Specific DG system requirements

The DG system must meet a set of I4.0 specific requirements, which will imply the evolution of the current capabilities of the organization and the adding of other new ones. Some could be organizational types; others focused on processes; while others could correspond to the use of automation, ML and AI technologies. Furthermore, the DG system must bear in mind the real complexities that an I4.0 environment presents, mainly, the existence of massively distributed systems, many of them are

legacy systems, and the integration of third-party services.

We organize these requirements into the following groups:

1. Principles: This collects requirements that must be met by the principles that govern the DG system.
2. Governance: This includes Strategic alignment requirements, Organizational requirements and Data governance and stewardship requirements.
3. Management: This gathers Classification and Metadata requirements, Data Quality requirements, Security, privacy and data risks requirements and Data Life Cycle (DLC) requirements.
4. Monitoring: This contains Requirements for monitoring, evaluation and assessment.

Next, these requirements, extracted from the literature, are specified and classified according to their nature, i.e., if they are general for DG or specific for I4.0.

1. Principles:

   This group details the requirements that must be taken into account when drawing up the list of principles that govern the implementation of a DG system.

Section	Principles
General req.	The principles [17] that guide the conduct, behavior and philosophy of the company regarding the use, management and governance of data must be established. The principles should be oriented towards a data-centric architecture. Each principle must be aligned with DG and support its goals and objectives.
I4.0 req.	N.A.

2. Governance

   This establishes the requirements for efficient data governance and administration, such as the need for the DG program to be aligned with the business plan of the organization, requirements related to organizational aspects of DG that must be taken into account and those referred to roles, decision-making rights, definition of policies, etc.

Strategic Alignment Requirements

Section	Goals, objectives and strategies of DG
General req.	DG goals, objectives and strategies aligned with those of the organization must be defined[6]. A monitoring method to verify and ensure that the previous requirement is met must be established. The information needs of the organization must be collected and this information must be available for decision-making [18].
I4.0 req.	N.A.

Organizational Requirements

Section	DG bodies and roles
General req.	DG must define governing bodies, governed bodies and roles, the latter, in data-related activities, that are the object of governance [19]
I4.0 req.	I4.0 roles should be assigned to profiles with the capacity for dynamic evolution, easily adaptable to regulatory and technological changes [20]. In defining roles, the different levels of vertical and horizontal integration of I4.0 should be taken into account, with special emphasis on the roles related to data security and quality [21]. The roles must be aligned with the industrial architecture that is being applied in the organization to implement the I4.0 model (IIRA, RAMI, IVI, IOT-A, IDS-RAM, etc.) [22]

Section	Organizational Model
General req.	The organization model with which DG will operate (Centralized, Replicated, Federated, etc.) must be established [6].
I4.0 req.	The extension of the DG system to third parties that comprise its value chain (suppliers, distributors, etc.) should be considered. This will lead to sign contracts with commitments for implementing those DG rules that affect them [23].

Data Governance and Administration requirements

Section	Policies and standards
General req.	Policies and standards must be defined for both DLC activities and data features (quality, security, metadata) [24]. Policies must be oriented towards the implementation of the principles and the fulfillment of DG objectives[17]. Polices must contemplate the fulfillment of the internal norms and regulations of the company as well as the sectorial and legislative ones that affect DG. DG policies life cycle management must be also considered. Issues about performance monitoring and the compliance with the established policies must be defined[25].
I4.0 req.	The increase in the quantity and complexity of data requires the automation of DG policies and processes, through the implementation of concepts such as "Continuous Governance", methodologies such as "DataGovOps" and technologies such as "Governance as code", ML and AI [26]. Policies and rules must be defined and applied at the different levels of vertical and horizontal integration of I4.0. The standards and procedures must evolve and align with the new architectural models that are being incorporated into the operational and analytical I4.0 environment (e.g. microservices architecture) [21].

Section	Governance model
General req.	A governance model based on the functions of Evaluating, Directing and Supervising [24] must be defined. DLC activities to be governed as well as specific aspects of the data (quality, security, metadata) involved in these activities [27] must be defined.
I4.0 req.	Agile and DataOps principles must be applied with the aim of fostering collaboration of data stewards, data scientists, and data engineers working closely to codify governance policies across DLC and DG automation.

Section	Responsibilities and decision rights
General req.	DG must assign decision rights, authority and responsibilities over data assets to roles previously defined [6].
I4.0 req.	In data-intensive environments, DG must be agile and dynamic and therefore responsibilities and decision rights must be extended based on Agile, DataOps and DataGovOps models.

3. Management

Classification and Metadata Requirements

Section	Collection, cataloging and management of metadata
General req.	A Business Glossary, a Data Dictionary and a Data Catalog must be established as well as the policies and processes for their management.

(continued on next page)

(*continued*)

	Metadata should facilitate understanding of the context, importance and associations of the data. Metadata should collect information about data lineage. Metadata should gather safety and regulatory issues, both at data item and data set level. Policies and processes for managing the lifecycle of metadata must be established. Processes for analyzing the impact of changes to data artifacts must be incorporated.
I4.0 req.	A common language and a reference model to address the wide variety of data that defines business concepts and the relationships between them must be developed [28]. Due to the large number of systems involved, federated models of metadata management must be explored. In a DataGovOps model, the Glossary, Dictionary and Catalog updates should be automated by including them in the change management process (as if they were code updates) [29]. Metadata must describe the nature, semantics and quality of the data required by the agents that process it. Among others: the estimation of the volume, speed and variety of the data to be managed and the security requirements (authentication, integrity, confidentiality and availability) against external risks and reliability requirements against system failures as well as productivity and utilization metrics that must be evaluated in the production phase for the dynamic management of resources and processes. DG should contemplate the automation of metadata discovery, ingestion, interpretation, and enrichment processes and inclusion of advanced techniques and approaches in metadata cataloging and classifying through the use of ML and AI technologies. Data lineage must be collected by automating DataGovOps, which implies recording and organizing all the metadata related to the data, including the code that acts on the data [26].

Data Quality Requirements

Section	Data quality
General req.	Policies, standards and processes to ensure data quality must be established. Parameters by which data quality will be measured (e.g. accuracy, reliability, completeness, timeliness, etc.) must be identified.
I4.0 req.	Use of scalable automation technologies such as ML and AI for the automatic, continuous and real-time evaluation and validation of the quality of the data in each phase of the DLC, issuing alerts in real time or even correcting the detected problems must be pursued. Due to the great variety of data, their large volume and their changing nature, data quality rules for each use case and data type must be specified [30].

Data Security, Privacy and Risk Requirements

Section	Data security, privacy and risk
General req.	Sensitive data must be identified and classified taking into account the business requirements, regulations, standards and legislation that are applicable to them. Policies about what can be done with data, who can do it, under what terms and conditions, etc. (authentication, authorization and non-repudiation) according to data classification must be defined. Policies designed to ensure the confidentiality, integrity and high level of availability of the data must be defined. Policies and mechanisms to validate that both input data sources and data consumers are authenticated must be established. Backup and data recovery policies to deal with possible data damage and disaster recovery [31] must be defined.
I4.0 req.	DG must evolve towards the standards incorporated as a consequence of the use of 3P platforms. Data security models adapted to I4.0 must be applied [32] with the aim of protecting operational and security data used, stored or moved on the endpoint; system configuration data; operation and interconnectivity data of the networks as well as data related to the monitoring of the systems.

(*continued on next column*)

(*continued*)

	Different data protection mechanisms and approaches depending on whether the data is in use, in motion or at rest [22] must be used. An extremely fast response capacity to security problems and threats must be established. Specific policies, different from the usual ones, for information protection, backup and disaster recovery tasks are required. Security policies must be applied to different levels of the value chain and throughout all stages of DLC.

Data Life Cycle Requirements

Section	Planning and Design (Data Architecture, Modeling and Design)
General req.	Data architecture must be aligned with the DG. Data stewards and data architects must work together to define the data entities and the enterprise data model (Conceptual, Logical, and Physical). Organization data architecture requirements must be defined and software projects must be conformed to those requirements. Designs, tools and lifecycle tasks related to the data architecture must be managed. Policies, standards, rules and guidelines about how data must be used in the organization must be defined.
I4.0 req.	Data architecture must be aligned and coherent to the industrial architecture that is being applied to implement the I4.0 model (IIRA, RAMI, IVI, IOT-A, IDS-RAM, etc.). Data architecture must take into account the exchange and sharing of data throughout all the levels of vertical and horizontal integration of the value chain. Data architecture must include a common and distributed metadata repository in order to have a thorough description of the different types of data (Structured, Semi-structured, Unstructured) of the organization.

Section	Capture or Collection
General req.	Policies, standards, processes and procedures about data integration and interoperability should be established as well as how these data should be extracted, processed for the creation of useful data (clean, accurate, complete and rigorous) and stored. Data transformation is included here to give data structure and format according to its destination. Different data moving and capture strategies, latency and other non-functional requirements must be taken into account. Data Sharing Agreements that gather the responsibilities and acceptable use of captured data must be established. These agreements must be approved by the steward responsible for the data.
I4.0 req.	Policies regarding the management of data sources (registration and acceptance, modification, cancellation, etc.) must be established. Systems for automatic and real-time data validation must be incorporated. These must issue alerts in real time when necessary, and establish policies that allow stopping data entry from a source with errors [33]. The criticality of the data arriving from cyber-physical systems must be evaluated and policies, rules and processes must be established in this regard. The application of standards (e.g. International Data Spaces) that facilitate the exchange and sharing of data along the value chain is highly convenient, while allowing the different actors to define software readable contracts attached to data (Self-Aware Contracts).

Section	Storage
General req.	Policies, standards and processes for the storage, maintenance, improvement of data (data does not change intrinsically), archiving as well as auditing stored data must be established. Legal requirements for storing and archiving data must be considered.
I4.0 req.	Policies on data storage must be defined at the different levels of vertical and horizontal Integration, mainly at the edge due to its technical complexity.

Section	Preparation
General req.	Policies, standards, and processes for data preparation must be established according to its destination. Data can be aggregated and/or combined with others in order to be distributed, archived, deleted or analyzed.
I4.0 req.	Policies on data transformation at the different levels of vertical and horizontal integration (e.g. data selection and filtering at the edge) must be defined.

Section	Use
General req.	Policies, standards and processes related to the consumption, use and analysis of previously prepared data for decision making must be established.
I4.0 req.	Policies on data analysis at the different levels of vertical and horizontal integration must be defined.

Section	Distribution
General req.	Policies, standards and processes for the distribution of data to third parties (e.g., Administration, partners and collaborators, external customers) or internal users must be defined. Data Sharing Agreements that gather the responsibilities and acceptable use of the distributed data must be signed. These agreements must be approved by the steward responsible for the data to be distributed.
I4.0 req.	The application of standards (e.g. International Data Spaces) that facilitate the exchange and sharing of data throughout the value chain is highly convenient, while allowing the different actors to define Self-Aware Contracts.

Section	Decision making
General req.	A delegation process that ensures that the decisions made, manual or automatic, be defined. Decision making must be compliant to the level of responsibility of the role that makes them. DG must establish appropriate controls, including manual intervention, to address any bias in the decision-making process. Processes to assess the usefulness of the data used for decision making must be defined. This new metadata can be used to enrich this data and improve future decision making.
I4.0 req.	N.A.

Section	Destruction
General req.	Policies, standards, processes, etc. for the permanent deletion of the data must be defined.
I4.0 req.	N.A.

4. Monitoring

Monitoring and evaluation requirement

Section	Monitoring and Evaluation
General req.	Policies, processes and a system of metrics and Key Performance Indicators (KPI's) must be defined in order to monitor the performance of the use of data in the organization and to ensure that the strategies related to data have been implemented correctly as well as that the use and data management are carried out according to internal policies and established external requirements. Monitoring processes must encompass three groups of metrics: those related to the evaluation of the degree of maturity of the processes; the ones referred to the performance of the processes in the disciplines of data management (DM) and metrics about DG (policies, principles, organization, etc.).
I4.0 req.	Automation of monitoring processes in real time throughout the DLC by means of ML and AI technologies must be pursued.

3. Data governance as a system

On the one hand, in ISO/IEC/IEEE 24765 [34], a system is defined as a "interacting combination of elements to accomplish a defined objective" or as a "combination of interacting elements organized to achieve one or more stated purposes". It is also said that "a complete system includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services, and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment". According to these statements, governance in general and DG in particular can be conceived as a system, as pointed out in ISO/IEC/IEEE 38505-1 [24].

On the other hand, it must be taken into account that DG is a business function [35] and as such, it must be aligned and consistent with the goals, objectives and strategies of the organization [6]. Furthermore, as indicated in ISO/IEC/IEEE 42010 [36], an architecture is used to define and represent a system, which is expressed through an "architecture description" that, in turn, identifies the referred system. This is valid for any system, including a DG system. In this sense, The Open Group, based on the ISO/IEC/IEEE 42010: 2011 standard, developed TOGAF® Standard [17], a framework to build business architectures whose scope can be the entire company or specific areas or parts of it, as may be the case of the DG. Consequently, we can propose the development of a DG system and represent it through an enterprise architecture.

In the systematic literature review carried out in [9], we found that there are specific models and proposals that partially address the problem of data governance in the Cloud, Big Data, Data Lake environments, etc. as well as some international standards whose main purpose is IT Governance, which include some aspects related to DG within their scope. Likewise, there are a few books and publications that deal with the field of DG in greater or lesser depth. However, we have found neither a framework that provides a comprehensive approach that encompasses data governance for I4.0 supported by 3P technologies nor a reference architecture that allows us to define a DG system for I4.0 consistently. We have also checked that the analyzed frameworks do not include a clear procedure to verify that a DG system is aligned with the goals and strategies of the organization and with the objectives and strategies related to data.

That is why our research work is focused on the development of a Framework for the construction of DG Systems for I4.0 and its representation through a DG architecture, supported on the concepts defined in the standard ISO/IEC/IEEE 42010:2011 and the TOGAF® Standard V9.2 framework, for the development of enterprise architectures. Furthermore, our framework aims to be complementary and compatible with the use of other IT governance frameworks, such as COBIT® 2019 [16], or data management frameworks such as DAMA-DMBOK® [6] and MAMD model for data improvement [37], among others.

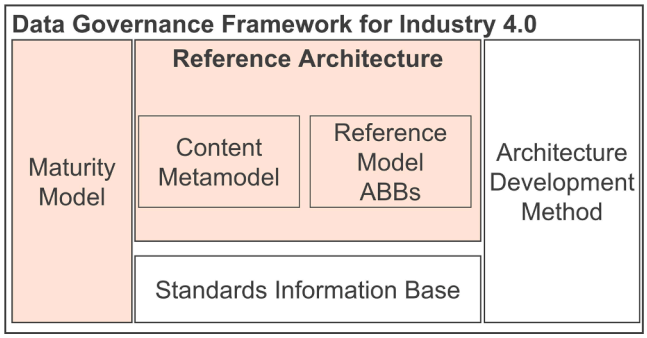


Fig. 2. Reference framework.

4. Framework for the implementation of DG systems in I4.0

Once the requirements have been specified and the foundations of our work have been established, we proceed to formally define a framework for the building of DG systems for I4.0 (see Fig. 2). This framework consists of a Reference Architecture for the representation of the DG systems, a Method which indicates the steps to follow for the development of the architecture, a list of recommended standards and a maturity model [38]. All of these elements will allow us to instantiate DG systems aligned with the organizations business strategy and describe the architecture of the DG system in an Industry 4.0.

Next, the reference architecture and the maturity model are described as well as two Architecture Building Blocks (ABB) of the reference model.

4.1. Reference architecture

The reference architecture is made up of a Content Metamodel and a Reference Model which contains a set of Architecture Building Blocks (ABB). This reference architecture makes it possible to describe a sound architecture of a DG system.

We use the content metamodel defined in the TOGAF® Standard v9.2 framework (see Fig. 3), to which we have added a new entity, named Policy, by specializing the Principle entity of the TOGAF® metamodel. This metamodel provides a formal structure of entities with their attributes and relationships and the rules that govern these relationships, which allows defining, structuring and presenting architecture content in a consistent way.

The content metamodel is a conceptual tool that provides a definition of all the basic elements that can exist within our architecture,

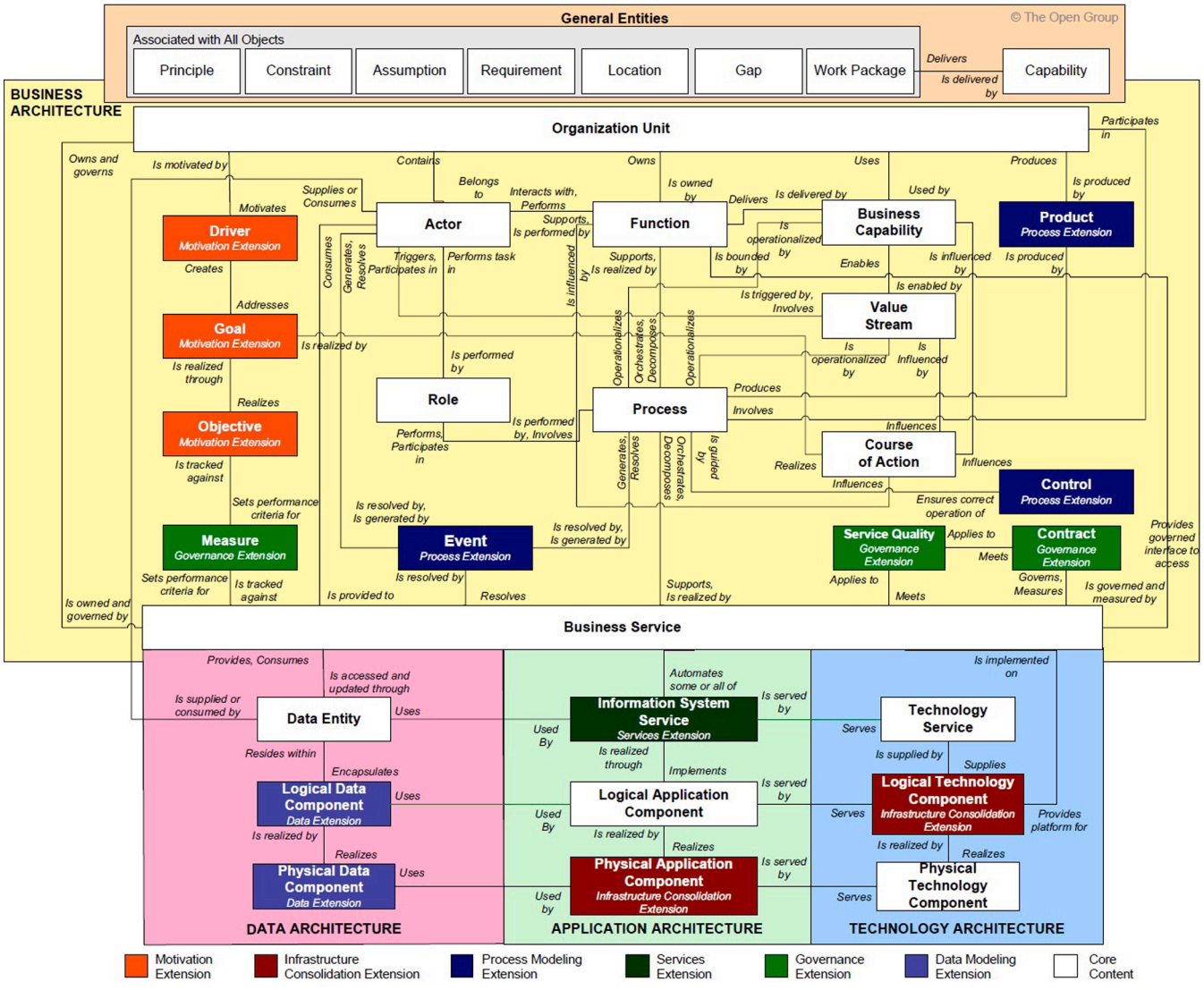


Fig. 3. TOGAF® Standard v9.2 Content Metamodel.

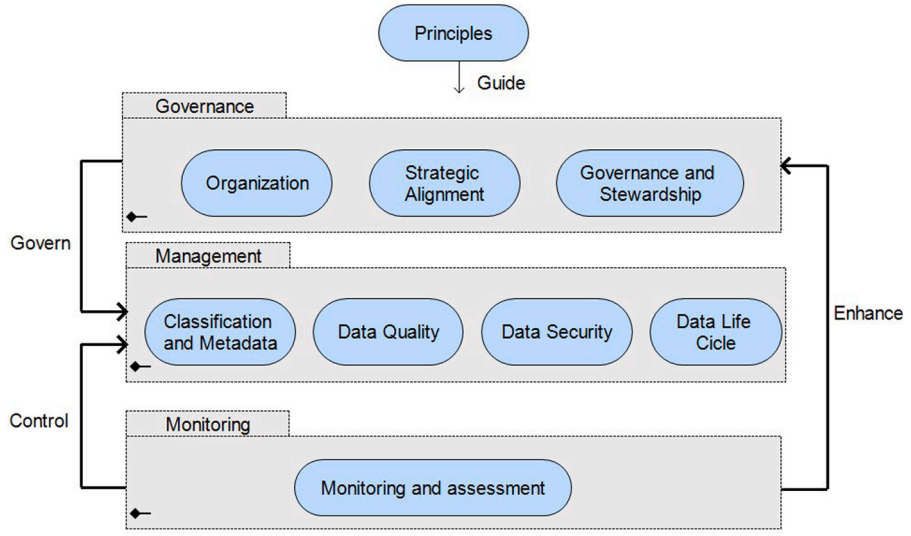


Fig. 4. Reference Model.

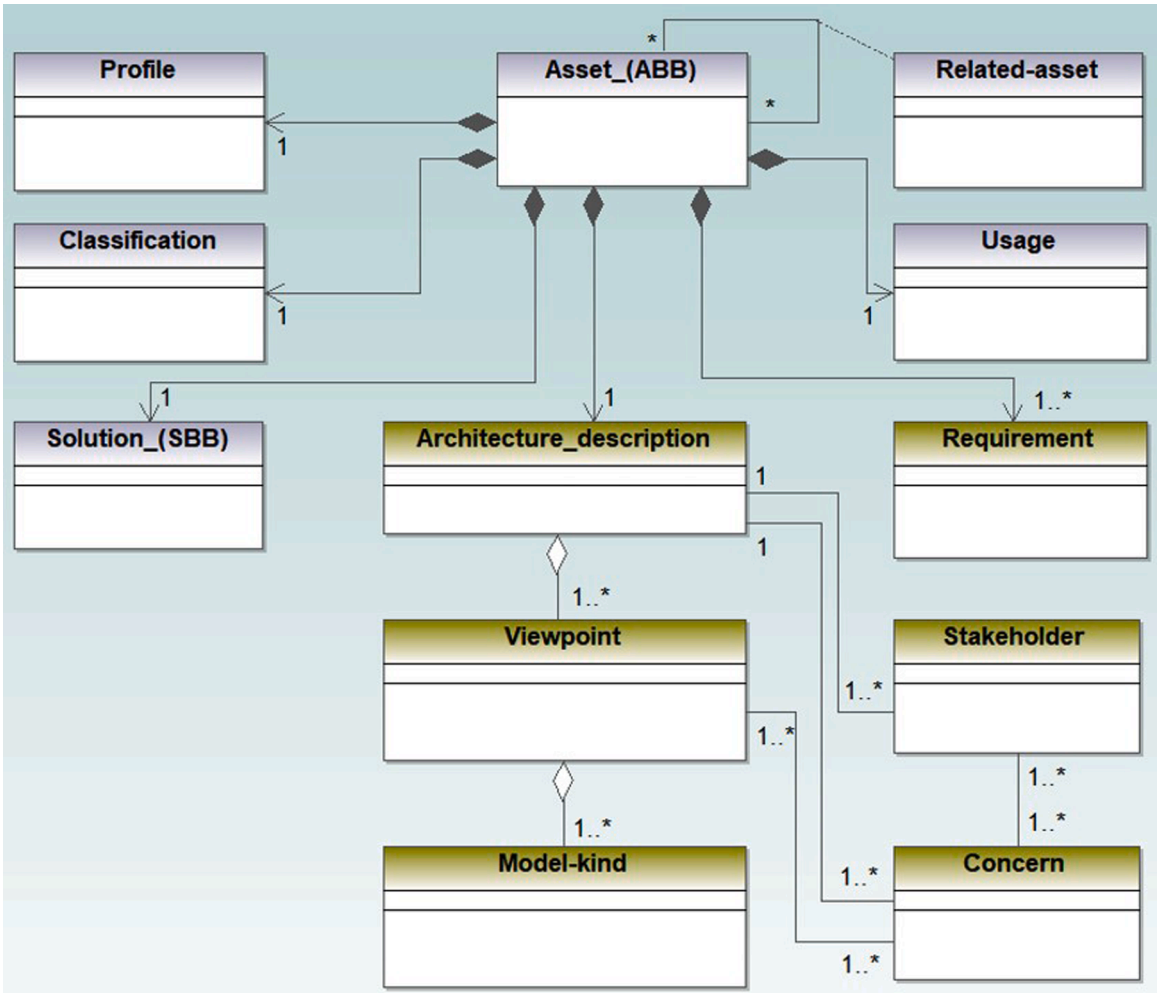


Fig. 5. ABB profile.

showing how these can be described and related to each other. Therefore, the metamodel provides us with a tool to define the ABBs that make up the architecture. Furthermore, these ABBs and their relationships are described and represented using the Architecture description model described in ISO/IEC/IEEE 42010:2011.

The reference model for the Data Governance architecture (see Fig. 4) defines a set of ABBs, each of which is a part of the architecture and specifies functionality and capabilities that the architecture must implement. These ABBs model the requirements expressed in Section 2. For the representation of these highest-level ABBs, we have chosen the Business service entity from the content metamodel.

In order to formally specify, describe and manage reusable ABBs, we have created ABB-profile (see Fig. 5), which is an extension of the Default Profile from the OMGs Reusable Asset Specification (RAS) standard, Version 2.2 [39].

Therefore, each ABB is specified by the following classes:

Asset_(ABB)	It defines the ABB. It contains three required attributes: Name, Id and Description.
Profile	It describes the asset type and provides information about its lineage.
Classification	This class contains a set of descriptors to classify the ABB. Classification allows the ABB to be managed and located in a repository.
Usage	Depending on the level of detail of the ABB, this class describes the activities to be performed for implementing or using the asset, so that it can guide the development of Solutions Building Blocks (SBBs) which are the products and components that help implement the functionality and capabilities defined in the ABB.
Related-asset	It specifies the relationship to another ABB. At least, name and relationship-type attributes are required.
Solution	It describes the SBBs that will be instantiated to implement the Governance System defined by the architecture.

Likewise, we have extended the RAS Default Profile with new classes as follows:

Requirement. It describes each requirement that ABB implements.

Architecture-description. This class describes and communicates different parts of the architecture defined by ABB, according to the ISO/IEC/IEEE 42010: 2011 standard. It is made up of the following classes:

- Stakeholder. This class identifies a DG system stakeholder (an individual, team, organization, or class thereof, having an interest in a system).
- Concern. It describes an interest in the DG relevant to one or more of its stakeholders.
- Viewpoint. It establishes the conventions for the construction, interpretation and use of ABB architecture views to frame specific DG system concerns.
- Model-kind. This class establishes the modelling conventions for each type of model, related to a Viewpoint, taking the Content Metamodel as a reference.

In this paper we develop two Asset_(ABB), namely Architecture Principles and Policies and standards (the latter is part of the Asset_(ABB) Government and Stewardship). Each one consists of several viewpoints that are described and clarified by means of examples taken from the DG system of a hypothetical electric power supply company.

4.1.1. *Case study: DG system for an electric power supply company*

This fictitious company has a software system for the automatic and autonomous management of the power grid of a smart city, through the electrical equipment, cyber-physical elements and IT resources deployed in it (see Fig. 6). In addition to the control and monitoring of the facilities, the system provides other companies (power trading and power production companies, etc.) as well as other stakeholders and interested agents (users, public administration, etc.) with the information they may require on the power grid status and operation and collects from them the information needed to be able to operate in a profitable, reliable and efficient manner.

Among others, it manages in real time the equipment deployed in the power grid to both control and meter the electricity supply; it supplies, collects, manages and records information relating to the electricity supply and the quality of service being offered to users; it detects anomalous situations and when these cannot be managed automatically by the system, it sends out an alarm signal. To this end, several elements have been deployed, such as smart meters at consumption points and equipment, located in the street transformers, to control the configuration of the power lines. Also, field computers, located in the district and city substations, which belong to the cyber-physical elements that carry out supervision and control operations of the electricity infrastructure as well as the computers of the distribution management center that provides computing capacity to the digital platform.

The company also has implemented an I4.0 Architecture whose functional domains are depicted in Fig. 7. This is compliant to IIRA [32].

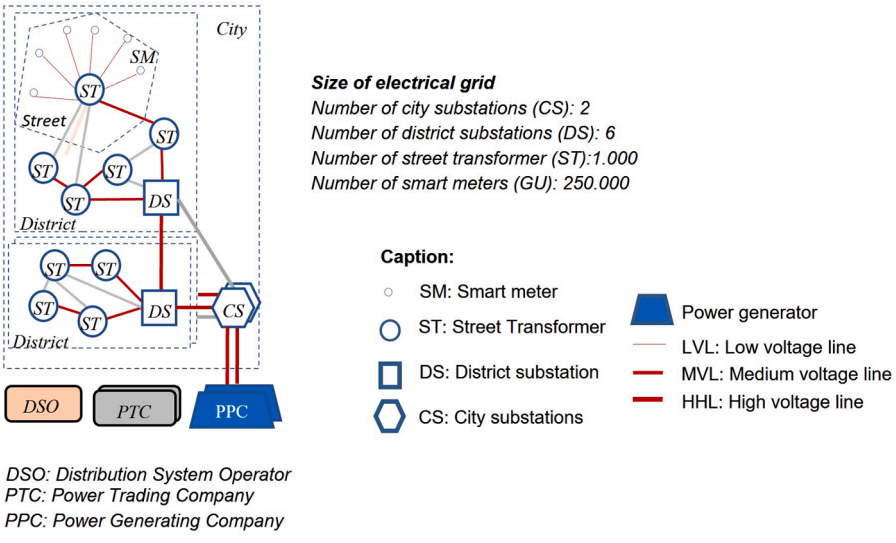
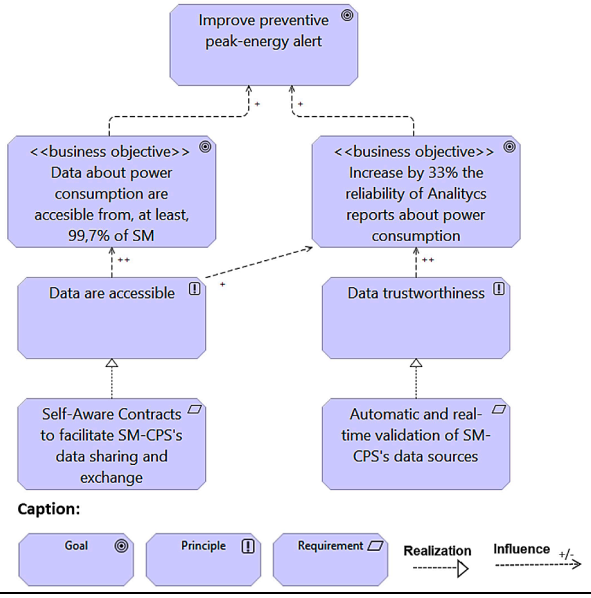


Fig. 6. Power grid of a fictitious smart city.

Viewpoint name	Principles alignment diagram.
Description	It models and relates the principles to each other and to the companys requirements, goals and objectives that motivate these principles and to which they contribute. It is a way of verifying and demonstrating that the principles reflect the system requirements and contribute to the achievement of the companys goals and objectives.
Type	Diagram
Stakeholders	Data governance bodies, directors, business and ICT architects, business analysts, requirements managers.
Concerns	Mission, strategy, motivation.
Model-kind	The Requirement, Constraint, Principle, Goal and Objective entities of the content metamodel are used, relating them through the Realizes or Is realized relationships as follows: **Requirement / Constraint entity realizes Principle one**, that means the requirements and constraints are established so that the principles are met, thus the requirements / constraints carry out or influence on the realization of the principles. **Principle entity Realizes Objective one**, that means, the application of the principles allows (or influences on) the achievement of the objectives. **Objective Realizes Goal**. Objectives realize or influence the achievement of goals. Example (using Archimate v3.1)



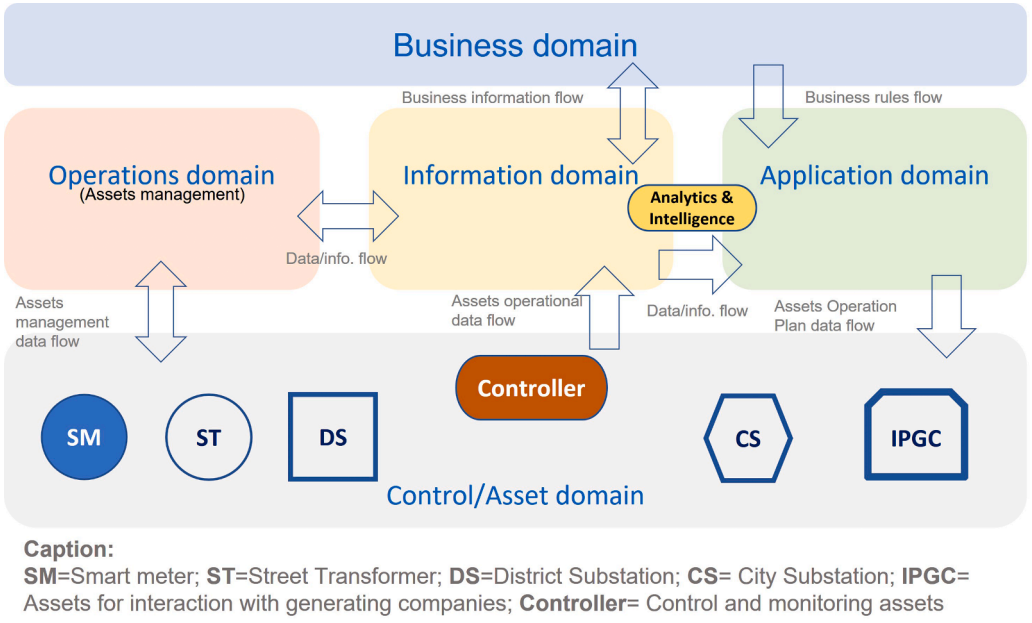


Fig. 7. IIRA functional domains.

4.1.2. Asset_(ABB) architecture principles

Next, the Asset_(ABB) Architecture Principles is shown in Fig. 8.

Name	Architecture Principles
Description	This ABB makes it possible for the principles to be defined, cataloged and managed. The DG Architecture Principles establish, in turn, high-level requirements that govern the architecture process, affecting the design, development, maintenance and use of the DG architecture. The Architecture Principles are defined from a business, DG and data point of view.
Requirement	The ABB contributes to implement the requirements of the Principles group
Classification	Principles; Business principles; DG principles; Data Principles; Motivation; Decision making
Usage	It is used for the recording and managing of the principles that govern the DG system as well as for being a reference for decision making, to justify other system requirements, and to demonstrate consistency between the Principles and the objectives and goals they support.
Related-asset	Name. Catalog management service. It allows inserting, modifying and removing principles into the catalog as well as the access management to the catalog. Relationship-type. Composition.
Related-asset	Name: Principles development process. It represents a sequence of activities to be carried out in order to define the principles. Relationship-type. Composition.
Related-asset	Name: Principles catalog. Data entity that contains the principles defined. Relationship-type. Composition.

The Architecture-description class within the Architecture Principles Asset (ABB) is made up of two Viewpoints namely Principles catalog and Principles alignment diagram, which are defined below.

Viewpoint name	Principles catalog
Description	This catalog captures the DG Architecture Principles according to a specific structure (see Model-kind) which helps to verify that they meet the requirements described in the principles group.
Type	Catalog
Stakeholders	Data governance bodies, directors, business and ICT architects, business analysts, requirements managers.
Concerns	Mission, strategy, motivation.
Model-kind	It is made up of "Principle" entities of the metamodel and has the following attributes: **Id**. Unique identifier of the principle. **Entity name**. Principle. **Description**. A principle is a qualitative statement of intent that should be met by the architecture. **Category**. The following categories of principles apply: Business Principles, Data Governance Principles and Data Principles. **Owner**. Responsible for defining and updating the principle. **Name**. The name given to the principle. **Statement**. It sets out the principle in an unambiguous, concise and clear way. **Rationale**. Reasons justifying adhering to the principle, highlighting how it contributes to fulfill business objectives and strategies, the benefits of applying the principle and the relationships with other principles, including priority levels or situations where one principle would be given precedence or have more weight than another. **Implication**. It sets out the consequences of adhering to the principle or not. If deemed appropriate, it details the resources, activities and costs necessary to comply with the principle. **Date**. Principle effective date and, where appropriate, date of review and justification. **Metric**. It describes the mechanisms used to measure whether the principle has been fulfilled or not.

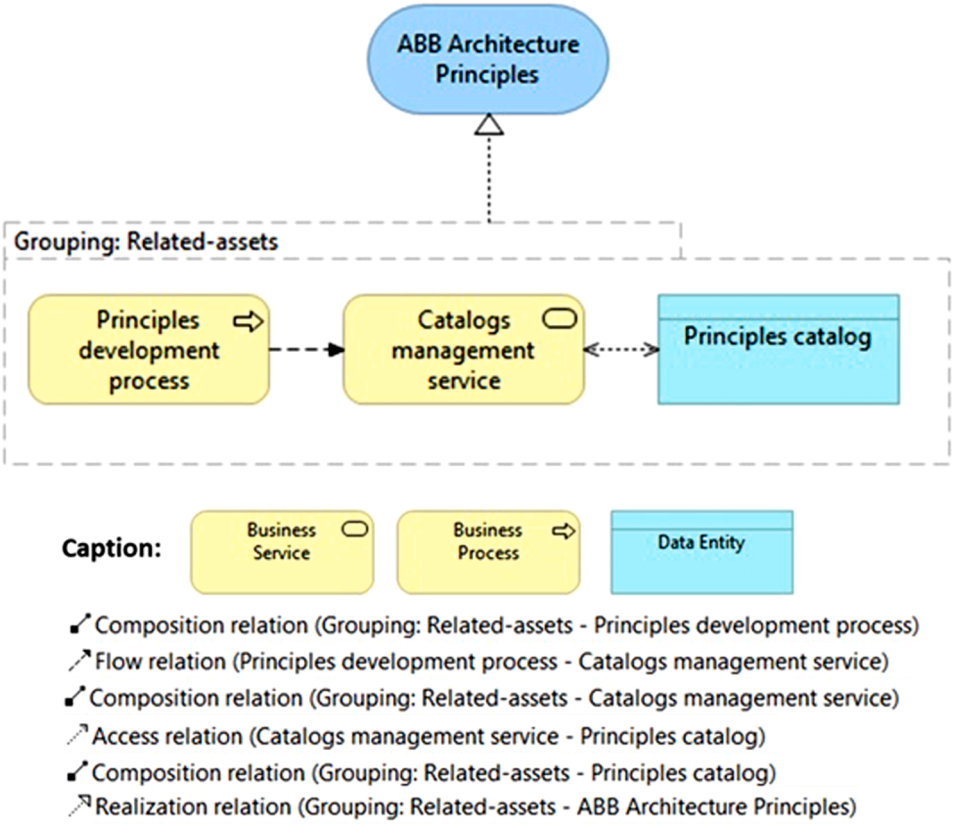
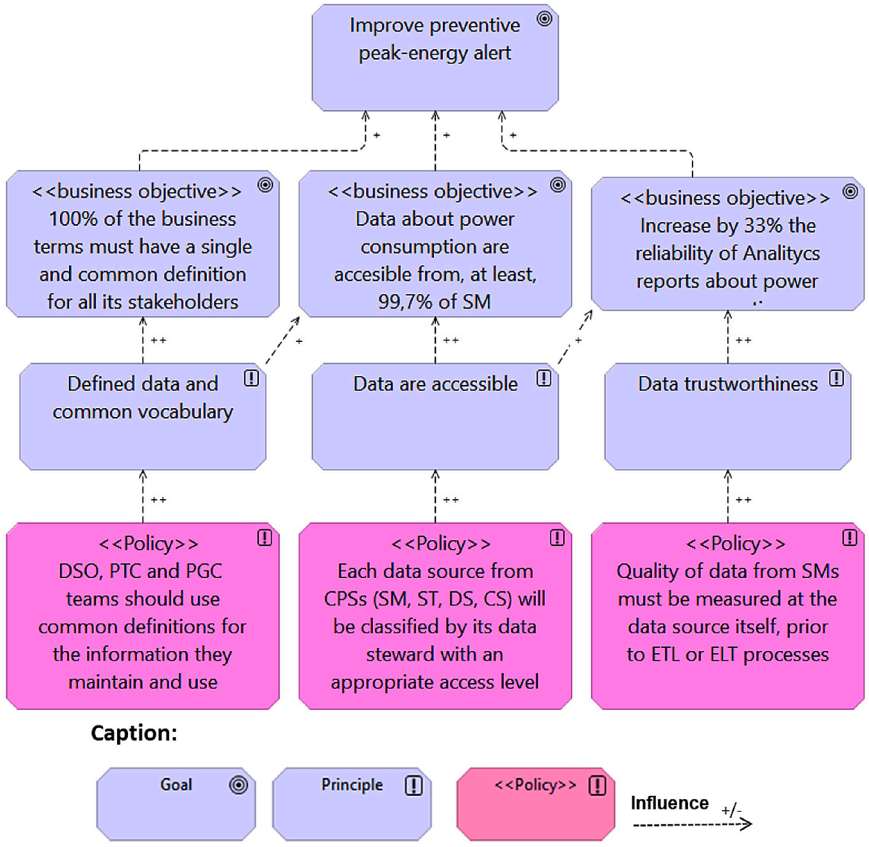


Fig. 8. Asset_(ABB) Architecture Principles designed with Archimate v3.1 .

Viewpoint name	Policies and principles diagram.
Description	It visually allows to justify that a given policy contributes to the application of a principle.
Type	Diagram
Stakeholders	Data stewards, business and ICT architects.
Concerns	Goals and objectives, motivation, application of principles, coherence between policies and principles.
Model-kind	Metamodel Policy, Principle, Goal and Objective entities are used and related through the following relationships: **Policy entity realizes Principle one**. Policies are defined based on the principles to materialize their compliance, so that policies contribute to and influence compliance with the established principles. **Principle entity Realizes Objective one**, that means, the application of the principles leads to (or influences) the achievement of the objectives. **Objective entity Realizes Goal one**. The objectives realize or influence the achievement of the goals. Example (using Archimate v3.1)



Next, an example of an entry in the principles catalog in the context of our case study is shown.

Id	BP6
Entity name	Principle
Description	A principle is a qualitative statement of intent that should be met by the architecture.
Category	Business principles.
Owner	Director of legal advisory services.
Name	Current legislation compliance.
Statement	DG must ensure that the information management processes comply with current legislation and regulations.
Rationale	Compliance with external laws, policies and regulations related to data management is mandatory for the company.
Implication	Failure to comply with the law can cause significant damage to our image and results. Changes in law or regulations may lead to changes in our processes and applications.
Date	June 16, 2018
Metric	See KPIs definition.

4.1.3. *Asset_(ABB) policies and standards.*

Next, the Asset_(ABB) Policies and standards is shown in Fig. 9. This is framed within the Asset_(ABB) Government and Stewardship (see Fig. 10), inside the Governance group.

Name	Policies and standards
Description	Based on the principles, it makes it possible to specify the policies and standards that must be applied along the DLC activities. It also facilitates the identification of issues to be considered for monitoring performance and compliance with established policies. Finally, it promotes the automation of DG processes through the implementation of new concepts such as “Continuous Governance”, methodologies such as “DataGovOps” and technologies such as “Governance as code”.
Requirement	This block implements the requirements related to: i) the specification of policies and standards; ii) compliance with standards and regulations related to data, both internal and external to the organization; iii) issues to be considered for monitoring performance and compliance with established policies; iv) the automation of DG policies.
Classification	Strategy implementation; DG policies; DataGovOps; Process automation; Continuous Governance.
Usage	It is used for the development, management and implementation of DG policies as well as a reference for decision making; it serves to translate from Principles to Policies and Rules and to check coherence between Policies and Principles from which they are derived; also, to develop policy automation.

(*continued on next page*)

(*continued*)

Related-asset	Name. Catalog management service. It allows inserting, modifying and removing polices into the catalog as well as the access management to the information of the catalog. Relationship-type. Composition.
Related-asset	Name: Policy development and standards selection process. It defines a sequence of activities to be carried out to develop policies and select appropriate standards. Relationship-type. Composition.
Related-asset	Name: Policy implementation and automation service. It makes possible the implementation of policies and standards by applying rules that are executed either manually or automatically. In the latter case, policies in natural language are read from the catalog, and translated them into technical rules that can be executed by a rule engine, so that they can be automatically applied to data. Relationship-type. Composition.
Related-asset	Name: Policies catalog. Data entity that contains the defined policies. Relationship-type. Composition.

The Architecture-description class within the Policies and standards Asset (ABB) is comprised of two Viewpoint namely Policies catalog and Policies and principles diagram, which are defined next.

Viewpoint name	Policies catalog.
Description	This catalog includes policies that have been defined to comply with the principles and apply DG strategies along the DLC activities.
Type	Catalog
Stakeholders	Data stewards, business and ICT architects.
Concerns	Mission, strategy, principles implementation.
Model-kind	It is made up of Policy type entities, derived from the Principle metamodel entity and has the following attributes: **Id.** Sole and unique identifier of the policy **Entity name**. Policy. **Description**. A policy is a statement addressed to achieve a set of goals. Policies are directives that govern and guide the actions of the organization about data and its governance [6]. Policies make it possible to translate principles into rules that govern data management. Policies describe the "What" of the DG and the standards and procedures the "How". **Category**. Policies can be classified based on the activities of the DLC and data-specific aspects of governance (quality, security, metadata, etc.). Therefore, a category could be: "Data storage security policies". **Owner**. Responsible for defining and updating policies.

(*continued on next page*)

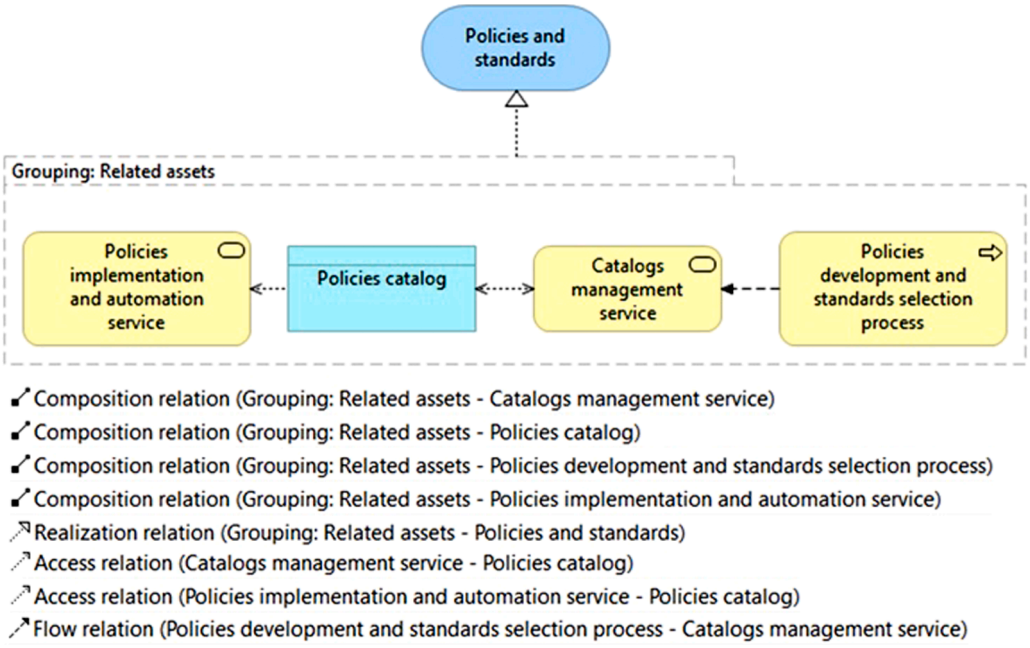


Fig. 9. Asset (ABB) Polices and standards designed with Archimate v3.1 .

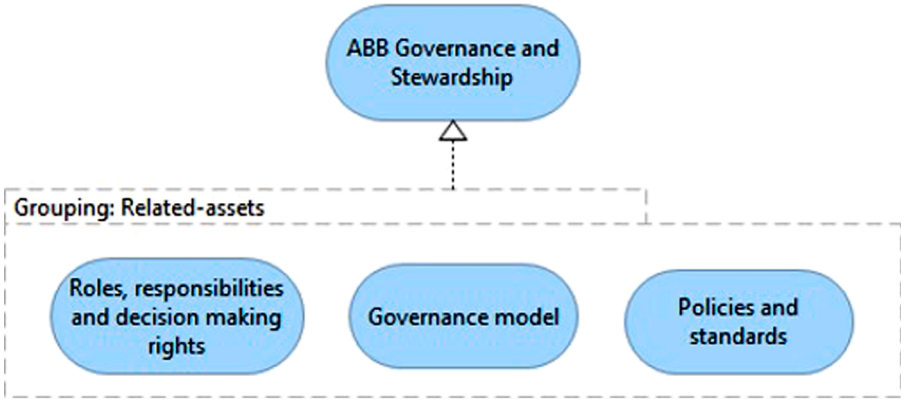


Fig. 10. Asset (ABB) Governance and stewardship designed with Archimate v3.1 .

(*continued*)

	Name. The name given to the policy. **Purpose/Objective**. Policy purpose and objectives that this Policy is intended to fulfill. **Statement**. It defines the policy in an unambiguous, concise and clear way. **Scope**. Audience affected by this policy. **Procedures**. It succinctly lists the procedures derived from this Policy. **Standards**. Standards that contribute to and help implement the Policy are referenced here. These standards will be included in a Repository of Architecture Standards. **Date**. Policy effective date and, where appropriate, date of review and justification. **Metric**. It describes the mechanisms that will be used to evaluate compliance with the Policy.

Next, an example of an entry in the principles catalog of our fictitious company is shown:

Id	IM6_11
Entity name	Policy
Description	Policies are directives that govern and guide the actions of the company regarding data and its governance. They translate the principles into rules that govern data management.
Category	Security policy for Personally Identifiable Information sharing.
Owner	Data Protection Officer.
Name	Information sharing policy.
Purpose	It provides guidance to organization staff in relation to when to conduct a Data Protection Impact Assessment and under what circumstances an information sharing agreement may be required.
Objectives	To provide a framework to clarify local procedures related to sharing of service user information. To ensure that only the minimum information necessary for the purpose should be shared. To ensure that when information needs to be shared, that sharing complies with the law, and best practice. To provide a mechanism for signatories of this policy to agree with the terms and directives contained within this policy.
Statement	This policy outlines organization standards for information sharing. The information exchange protocols offer guarantees regarding the standards that each party will adopt. However, they do not provide a legal basis for sharing confidential information. For this reason, it is mandatory to reliably inform the person, whose information you want to share, about the possibility of sharing it and the options they have to limit this exchange. If the person says NO to sharing, the confidential information will not be shared.
Scope	All organization staff.
Procedures	P01_IM_11 information evaluation and sharing.
Standards	Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
Date	Effective date: September 20, 2019
Metric	The authorization on the exchange of information will be verified. Policy violations will be logged.

(*continued on next column*)

(*continued*)

4.2. Maturity model

The maturity model that is included as part of the framework for the construction of DG systems presented in this work, establishes the fundamental guidelines so that the company can evaluate its current situation regarding the performance and capabilities of the processes of the DG system built, identify the existing gap between its current situation and the desired one and consequently determine a gradated path addressed to improve the capabilities and performance of these processes.

This maturity model is based on the proposals of various authors such as [6,40–42]. This is comprised of three core components: the first one refers to the different degrees of maturity that are considered in the model, also known as maturity levels; the second one gathers the domains that are subject to evaluation and to which a specific maturity level will have to be assigned; and, the third component is the evaluation method used to determine the degree of maturity.

Maturity levels. Our model establishes the five maturity levels defined in Table 1. Subsequently, the description of each of these levels is particularized and detailed for each activity specified in the domains to be evaluated.

Domains. The domains (Groups) of our maturity model are divided in Categories and in turn, in Process Areas which include the activities or practices to be evaluated. Following the scheme presented in the Architecture reference model (see Fig. 4), the Groups would be the ones depicted under the grouping element, that means, Principles, Governance, Management and Monitoring respectively. Within each Group, the Categories would correspond to the ABBs defined. For instance, the Categories included in the Management Group are: Classification and Metadata, Data Quality, Data Security and Data Life Cycle. Within each Category, Process Areas are established. One of them would be the Business Glossary inside the Classification and Metadata Category which include the Activities or practices to be evaluated for the different maturity levels (see Fig. 11).

Evaluation method. The method consists of associating to each of the Process Areas to be assessed a series of statements that make it

Table 1
Maturity levels.

Level	Description	Perspective
1: Initial	DG is defined and implemented ad hoc, primarily at the project level. Data governance functions are performed for at least one project. Ownership, stewardship, and accountability for data sets are primarily project-based assignments. DG is typically not applied across horizontal and vertical integration of I4.0. DG process discipline is primarily reactive. Solutions for automating and supporting DG and data management are scarce and limited.	DG as a requirement for the implementation of projects.
2: Managed	DG is planned and executed in accordance with policy; employs skilled people with adequate resources to produce controlled outputs; involves relevant stakeholders; is monitored, controlled and evaluated for adherence to the defined process. DG is partially applied across horizontal and vertical integration of I4.0. Some DG and data management functions are automated through specific and isolated solutions.	There is awareness of the importance of governing and managing data as a critical infrastructure asset.
3: Defined	Set of standard DG processes is used and consistently followed. Processes to meet specific needs are tailored from the set of standardized processes according to the organization's guidelines. DG is applied across horizontal and vertical integration of I4.0. DG and data management functions are automated through integrated solutions.	DG is treated at the organizational level as data is considered critical for successful mission performance.
4: Measured	Metrics are defined and used for evaluating the processes of DG and data management. These make use of statistic and data mining techniques for their computation. Their performance is managed and measured across the lifecycle of the process.	Data is treated as a source of competitive advantage.
5: Optimized	The performance of DG processes is optimized by applying Level 4 analysis for the identification of improvement opportunities. Best practices are shared with peers and industry.	Data is seen as critical for surviving in a dynamic and competitive market.

GROUP	CATEGORY	PROCESS AREA	PRACTICE/ACTIVITY	LEVEL	Valuation			
					1	2	3	4
Management	Classification and Metadata	Business Glossary (weight=15%)	Business terms are defined for a particular purpose.	1				
			Logical data models are created with reference to defined and approved business terms.	1				
			There is not any solution or tool for automating and managing business term.	1				
			A process is established, documented, and followed to define, manage, use, and maintain the business glossary.	2				
			Standardized business terms are readily available and promulgated to relevant stakeholders.	2				
			Each business term added to the business glossary has a unique name and unique definition.	2				
			Development, data integration, and data consolidation activities use business glossary terms as part of the definition process of data requirement.	2				
			There is some kind of tool or solution to support the automating and management of the business glossary.	2				

Fig. 11. An extract of a form for the assessment of the maturity level in the implementation of a DG system.

possible to determine whether the activities or practices related to the different maturity levels of the Area are carried out and to what degree (valuation 1 to 4). Subsequently, the maturity level in each Process Area is assessed according to the answers given and a value is assigned. Once the maturity level has been calculated for all Process Areas, the maturity level of the different Categories is calculated as the weighted average of each of the assessed Process Areas. The same procedure is used to calculate the overall maturity level of the DG system. Fig. 11 shows an excerpt of an evaluation form which exclusively gathers the activities corresponding to the Business Glossary process area.

5. Conclusions

This work aims to develop a reference framework for the construction of Data Governance systems for Industry 4.0 supported by 3P technologies (IoT, Social Technology, Mobile Devices, Big Data and Cloud/Edge Computing). In order to fulfil this goal, we first describe a specification of the requirements that this framework must meet as well as the set of standards that allows us to formalise our proposal.

Regarding the requirements, the following issues are highlighted: i) it is highly convenient to have profiles and roles adapted to new disruptive technologies in constant updating; ii) likewise, the automation of policies, processes and procedures under the approach “Continuous Governance”, “DataGovOps” and “Governance as code” are essential; iii) as a consequence of the vertical and horizontal integration that I4.0 pursues, DG must be extended at all levels of the organization, including supplier and distribution companies whose collaboration should be collected in service level agreements (SLA’s); and iv)the large amount and variety of data that is generated and processed in the I4.0 environment requires the use of Big Data and Cloud Computing technologies and tools, which also represent a challenge in terms of assigning responsibilities for data management, security policies and data protection (in use, in motion or at rest). Furthermore, it is an unavoidable fact, the necessary integration of these technologies with massively distributed and heterogeneous legacy systems.

The requirements specification led to the definition of a Reference Framework for the construction of DG systems for the Industry 4.0. For its definition and formalization, we selected three international standards, ISO/IEC/IEEE 42010:2011, TOGAF® and RAS [39]. The reference framework provides different levels and dimensions for its implementation and includes Architecture Building Block (ABB) [17] from which the services, processes and software artifacts necessary to materialize the DG system can be instantiated and implemented by means of different commercial-of-the-shelf (COTS) products or components that have some out-of-the-box (OOTB) business or technical capabilities.

Likewise, a maturity model associated to the DG framework is included with the aim of facilitating organizations to identify and assess the gap between their current data governance processes and best practice. In order to facilitate the understanding of this framework and its instantiation, examples of a DG system developed for a fictitious electricity company has been presented.

In the near future both, the proposed framework and the maturity model will be instantiated in real use cases in the industrial arena. Later, as a result of experience, the Architecture Development method will be written down and refined.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This work has been funded in part by the Spanish Government and FEDER funds (AEI/FEDER, UE) under grant TIN2017-86520-C3-3-R (PRECON-I4).

References

[1] Deloitte Consulting LLP, Industry 4.0. Challenges and solutions for the digital transformation and use of exponential technologies. Technical Report, 2015.

[2] N. Velásquez, E. Estevez, P. Pesado, Cloud computing, big data and the industry 4.0 reference architectures, J Comput Sci Technol 18 (03) (2018) 258–266, https://doi.org/10.24215/16666038.18.e29.

[3] J. Akoka, I. Comyn-Wattiau, N. Laoufi, Research on big data a systematic mapping study, Computer Standards & Interfaces 54 (2017) 105–115, https://doi.org/10.1016/j.csi.2017.01.004.SI: New modeling in Big Data

[4] C. Zunino, A. Valenzano, R. Obermaisser, S. Petersen, Factory communications at the dawn of the fourth industrial revolution, Computer Standards & Interfaces 71 (2020) 103433, https://doi.org/10.1016/j.csi.2020.103433.

[5] Stratio, Data-centric architecture A model for embracing the machine age., 2018, (????).

[6] DAMA International, DAMA-DMBOK2 : Data management body of knowledge, 2nd, Basking Ridge, New Jersey : Technics Publications, 2017, 2017.

[7] I. Alhassan, D. Sammon, M. Daly, Data governance activities: an analysis of the literature, Journal of Decision Systems 25 (December) (2016) 64–75, https://doi.org/10.1080/12460125.2016.1187397.

[8] M.M. Mabkhot, A.M. Al-Ahmari, B. Salah, H. Alkhalefah, Requirements of the smart factory system: a survey and perspective, Machines 6 (2) (2018) 1–22, https://doi.org/10.3390/MACHINES6020023.

[9] J. Yebenes, M. Zorrilla, Towards a data governance framework for third generation platforms, Procedia Comput Sci 151 (2019) 614–621, https://doi.org/10.1016/j.procs.2019.04.082.

[10] P. Lpez Martnez, R. Dintn, J.M. Drake, M. Zorrilla, A big data-centric architecture metamodel for industry 4.0, Future Generation Computer Systems 125 (2021) 263–284, https://doi.org/10.1016/j.future.2021.06.020.

[11] J. Yebenes Serrano, M. Zorrilla, A data governance framework for industry 4.0, IEEE Lat. Am. Trans. 19 (12) (2021) 21302138.

[12] K. Weber, B. Otto, H. Österle, One size does not fit all - A contingency approach to data governance, Journal of Data and Information Quality 1 (1) (2009) 4:1—-4:27, https://doi.org/10.1145/1515693.1515696.

[13] MDM Institute, MDM Institute - Data Governance definition, 2018, (????).

[14] C. Gray, IBM Corporation, An overview of data governance elevator Pitch (Final), 2011.

[15] B. Otto, Data governance, Business and Information Systems Engineering 3 (4) (2011) 241–244, https://doi.org/10.1007/s12599-011-0162-8.

[16] ISACA, COBIT 2019 Framework. Introduction and Methodology, 2018, https://doi.org/10.1057/9780230299283_1.

[17] The Open Group, TOGAF® Standar Version 9.2, 2018.

[18] MIT Technology Review Insights, Data on demand: Dynamic architecture for a high-speed age. Technical Report, 2020.

[19] M. Felici, T. Koulouris, S. Pearson, Accountability for Data Governance in Cloud Ecosystems. Proceedings of the 2013 IEEE International Conference on Cloud Computing Technology and Science-Volume 2, 2013, pp. 327–332, https://doi.org/10.1109/CloudCom.2013.157.

[20] Deloitte Consulting LLP, O. Sohail, P. Sharma, B. Ciric, Data governance for next-generation platforms, 2018.

[21] O. Sohail, P. Sharma, B. Ciric, 4 Pillars to Guide Data Governance for New Platforms, 2018.

[22] Industrial Internet Consortium, Data Protection Best Practices, 2019.

[23] K. Wallis, J. Stodt, E. Jastremskoj, C. Reich, Agreements between enterprises digitized by smart contracts in the domain of industry 4.0, Computer Science & Information Technology (CS & IT) (2020) 23–32, https://doi.org/10.5121/csit.2020.101003.

[24] International Standard Organization - ISO, ISO/IEC 38505-1. Application of ISO/IEC 38500 to the governance of data. 2017.

[25] International Standard Organization - ISO, ISO/IEC TR 38505-2. Implications of ISO/IEC 38505-1 for data management. 2018.

[26] E. Strod, Continuous Governance with DataGovOps 2020.

[27] C. Ballard, J. Baldwin, A. Baryudin, G. Brunell, C. Giardina, M. Haber, E.A. O'neill, S. Shah, IBM Information governance solutions, 2014.

[28] B. Rivas, J. Merino, I. Caballero, M. Serrano, M. Piattini, Towards a service architecture for master data exchange based on iso 8000 with support to process large datasets, Computer Standards & Interfaces 54 (2017) 94–104, https://doi.org/10.1016/j.csi.2016.10.004.SI: New modeling in Big Data

[29] L. Madsen, C. Bergh, Redefining Data Governance with DataGovOps (Webinar), 2020.

[30] D. Williams, H. Tang, Data quality management for industry 4.0: asurvey, Data Quality 22 (2) (2020) 26–35.

[31] Collibra, The Need for Big Data Governance, 2018.

[32] Industrial Internet Consortium, The Industrial Internet of Things Volume G4 : Security Framework, 2016.

[33] DataKitchen, What Is-dataops. Ten Most Common Questions, 2020.

[34] International Standard Organization - ISO, ISO/IEC/IEEE 24765 Systems and Software Engineering - Vocabulary, 2017.

[35] P. Brous, M. Janssen, R. Vilminko-Heikkinen, Coordinating decision-making in data management activities: a systematic review of data governance principles, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 9820 LNCS (2016) 115–125, https://doi.org/10.1007/978-3-319-44421-5_9.

[36] International Standard Organization - ISO, ISO/IEC/IEEE 42010:2011 Systems and Software Engineering Architecture Description, 2011, https://doi.org/10.1080/21670811.2017.1279978.

[37] A.G. Carretero, F. Gualo, I. Caballero, M. Piattini, MAMD 2.0: Environment for data quality processes implantation based on ISO 8000-6X and ISO/IEC 33000, Computer Standards and Interfaces 54 (November 2016) (2017) 139–151, https://doi.org/10.1016/j.csi.2016.11.008.

[38] The Open Group, TOGAF deltTextregistered 9.1 Translation Glossary: English Castilian Spanish, 2014.

[39] The Object Management Group, Reusable Asset Specification, Version 2.2, 2005.

[40] IBM Corporation, The IBM Data Governance Council Maturity Model: Building a roadmap for effective data governance. Technical Report, 2007.

[41] CMMI Institute, Data Management Maturity Model (DMM). Technical Report, 2021.

[42] J. Merkus. Data Governance Maturity Model, Open University, 2015. Master's thesis.