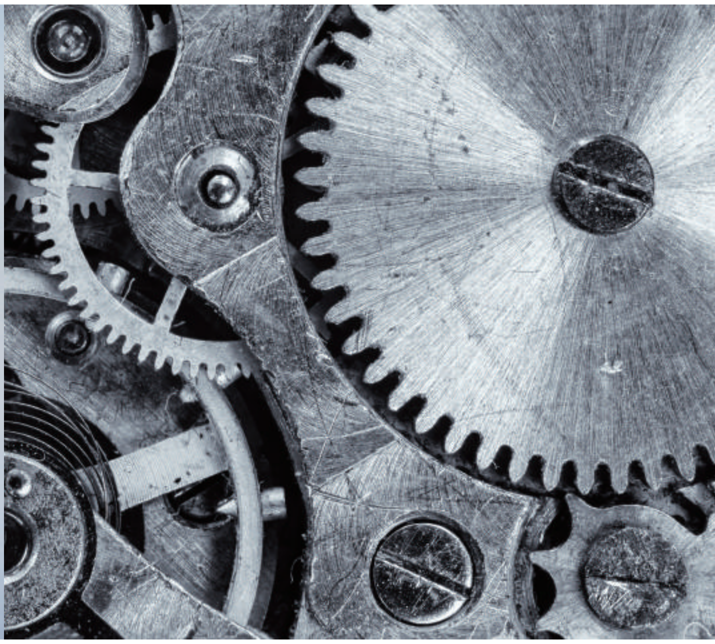
Industrial
Value Chain
Reference
Architecture-
Next

Strategic implementation framework of industrial value chain for connected industries

IVRA Next

Industrial Value Chain Initiative
Industrial Value Chain Reference Architecture

What is the Industrial Value Chain Initiative 《 IVI 》?

The IVI is a forum founded in 2015 to promote smart manufacturing based on the concept of “loosely defined standard” , responding to needs in the IoT era when manufacturing and IT are rapidly merged. It supports companies to enhance their strength while opening areas on which different parties should collaborate.
The IVI consists of more than 600 members from 260 companies (mainly manufacturers) and organizations as of February, 2018.

CONTENTS

Chapter 1

Overview

What is Smart Manufacturing ?

In the world of IoT in which all manner of things are connected to the Internet, the definition of smart manufacturing differs based on the conditions and corporate principles of the companies and factories that use it.
However, even if their conditions are different, the three following things are constant for all companies and factories that attempt to achieve smart manufacturing.

①

Value chain by connected factories

Each of the manufacturing sites have the means to connect to the digital world so that they can provide greater value to the customers that consume the things that they produce. They are connected through the digital world to their suppliers who provide the materials and equipment.

Although analog communications are also important, network effects in a digital society cannot be overstated. Manufacturers must synchronize with the needs of their customers and the markets, and always provide value in a timely manner.

②

Autonomous systems on loosely defined standard

Two competing companies will not reveal their hands to one another, and as a result of this, in areas where they do not compete they are actually duplicating their investments in many ways.

In smart manufacturing, the parts of individual companies that contribute to their competitiveness are kept closed, but common areas are boldly opened. In finding a common ground on which to connect, things are not based on strict standards.Rather, the characteristics of individual companies are maintained, and loosely defined standards that recognize individual differences are adopted.

③

Ecosystem on data-driven platforms

In addition to the existing physical locations, physical goods, and realities that comprise the analog aspects of manufacturing, the ratio of the cyber and digital worlds will increase. When this occurs, platforms that will allow the various activities to be connected in the digital world must not be optimized only internally.

In smart manufacturing, individual platforms must be mutually linked as a decentralized ecosystem (system of systems), and they must grow while also involving stakeholders with diverse values.

Three Layers of the Architecture

The structure of manufacturing that can realize smart manufacturing is defined as the Industrial Value Chain Reference Architecture.

The IVRA has three independent layers that supplement one another.

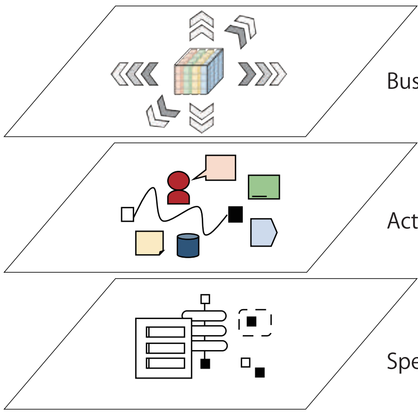


Fig. 1 Three layers of manufacturing

①

Business Layer

In the business layer, from a perspective of enterprise management, the focus of discussions is placed on the fundamental structure of manufacturing, organization forms for manufacturing, presence of essential perspectives and axes as well as a philosophy and concept of values underpinning the big picture.

The business layer includes views related to products or services that manufacturers provide to customers, positioning for business strategies, inter-company business transactions and commodity/service/intellectual property values.

②

Activity Layer

The activity layer has a view point of activities actually conducted at various places in manufacturers. People and machines acting voluntarily, human activity, machine processes, and information as an object of such activities and processes are brought up for discussion. In every production site of every manufacturer, concrete manufacturing activities are conducted in a different way.

In consideration of such diversity, systems that take advantage of the circumstances are defined in the activity layer.

③

Specification Layer

In the specification layer, the following will be considered: Specific operations based on human activities and machine processes and the things and information items that are their subjects, as well as the data and their attributes that are the subject of the processes executed by logic in software.

Within the specification layer, engineering is executed to mutually transmit, process, and reuse knowledge and know-how by objectively declaring and modeling the contents of the actual production mechanisms that individually differ.

Axes and Cycles of Smart Manufacturing

As a business organization, a manufacturer creates added value via a process that begins by purchasing materials, and continues through manufacturing products and selling them to customers. On the other hand, new types of manufacturers, such as fabless enterprises that have no factory and ones which earn income mainly from the added value of after-sales services, represent the progress of digitalization and the shift to service and software industries.

The following are three axes to view this transformation on.

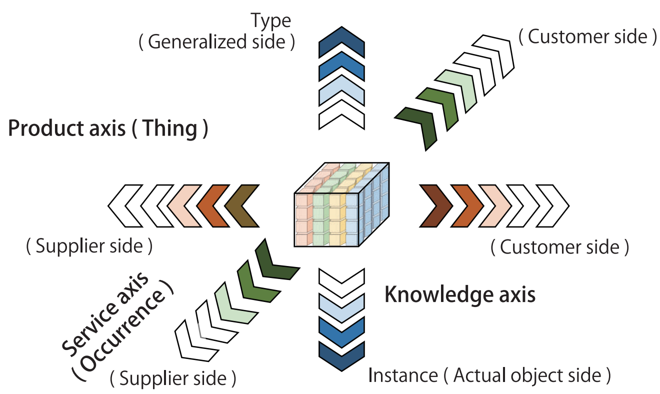


Fig. 2 Three axes of smart manufacturing

In the real world, each manufacturer deploys various activities along the product axis and service (occurrence) axis concerning services, including those provided by plant equipment. All of those activities form cycles. Such cycles are categorized based on the length of their targets as described in Figure 3.

The life cycle of a business (enterprise) is longer than such cycles.
Scrapping a business to rebuild it from the ground up and revolutionizing a business model represent disruptive (destructive) and transformative (revolutionary) innovation cycles, which exist at the outermost edge.

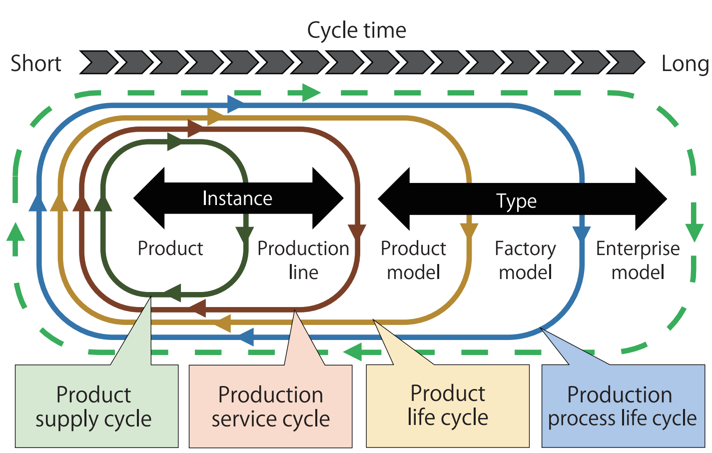


Fig. 3 Four cycles of smart manufacturing

Product Axis

The product axis includes the flow of materials along supply chains, which start as product materials and end as final products, as well as flows in demand chains that consist of needs and demands corresponding to the former. Technical information and engineering information on final products, constituent parts and (raw) materials are also included.

Service Axis

Production activities conducted in factories are defined as service activities. Therefore, human, equipment and production methods are dealt with in the service axis. Activities providing actions or production systems are also regarded as services.

Knowledge Axis

Things actually existing in a physical site are treated as instances (individual objects), whereas the category information or design information used to create them are included in types (generalization), which can be utilized by abstracting them or converting them into knowledge. Objects and occurrences conventionally categorized as instances are being digitalized with IoT. Conversion to data has become possible.

Product / Material Supply Cycle

In a supply chain, a set of processes in which materials received are processed into products that are shipped and delivered to consumers composes a cycle for each manufacturer. Such a cycle is repeated in daily production. The length of a cycle in a supply chain corresponds to a product's lead time, which differs depending on whether the focus is on a single enterprise or an entire supply chain.

Production/ Equipment Service Cycle

Equipment and devices that constitute production lines are allocated in factories as needed. Maintenance processes, such as replacing consumables, resetting parameters, repairing failures and renewing (if necessary), are conducted periodically (or occasionally) during the production period for targeted products.

Product Life Cycle

A product life cycle corresponds to a development case for a new product or a design change to an existing product. This cycle, which corresponds to the introduction of a new product model, includes processes such as planning, development, product design and production engineering (prototyping and (mass) production), and the eventual discontinuation of the model.

Production Process / Factory Life Cycle

When a product model is partially changed, its production line does not need major changes. But if a product in a totally new category is introduced, new processes have to be developed and implemented. In some cases, such as joint development with a new business partner, it can be a cycle to significantly change manufacturing systems in factory units.

Smart Manufacturing Unit: SMU

An autonomous body conducting smart manufacturing is called an SMU. An SMU is an organizational unit constituting a basic structure of a new type of manufacturing which is characterized by maximizing added value through connectivity. Here, new manufacturing means an industry seamlessly connected to other industries such as mining, agriculture, fishing, farming and service industries on the closer end to consumers. New manufacturing does not require defined borders. Moreover, by having such a system capable of connecting across sections, enterprises, industries, business types and enterprise sizes, an SMU makes it possible to dynamically reconstruct supply and engineering chains in order to respond to the needs of society.

An SMU generally corresponds to an enterprise or a smaller unit. However, among units for production processes, there are cases that cannot correspond to SMUs such as work centers, along with devices that cannot be SMUs. To be recognized as an SMU, a unit needs to have people who manage its internal structure and be able to modify itself when needed. In other words, an SMU can autonomously make decisions.

SMUs consist of three views.

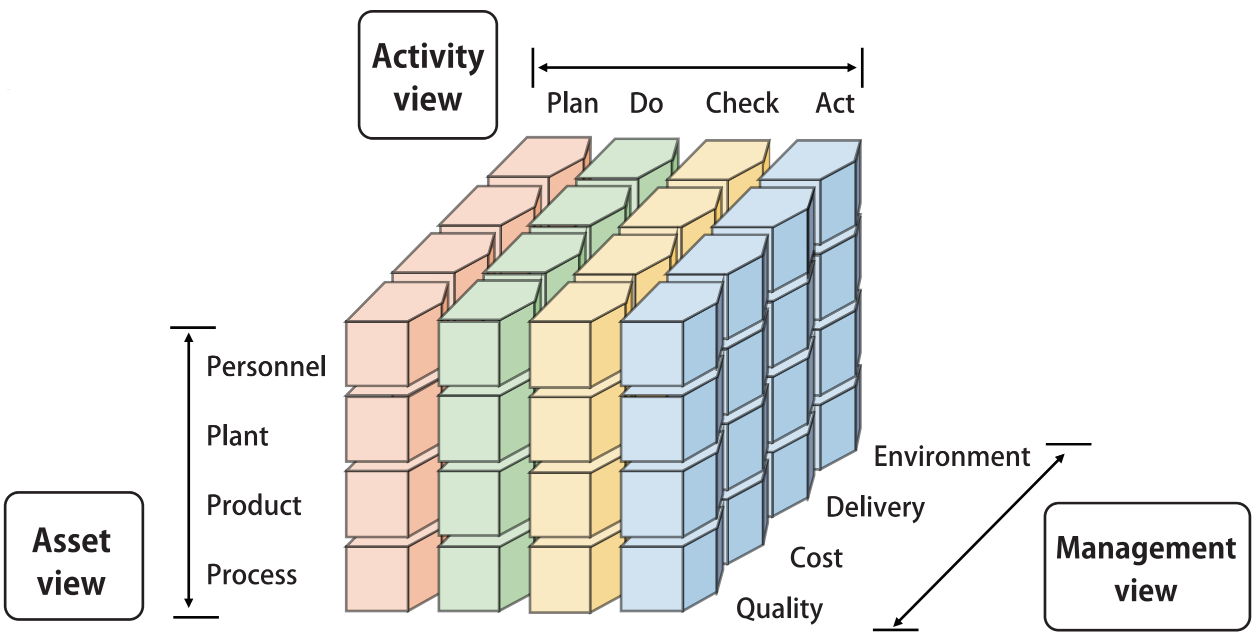
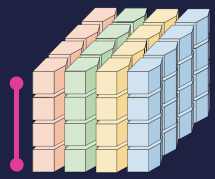


Fig. 4 Smart manufacturing unit (SMU)

Asset View



The asset view of an SMU shows assets valuable to the manufacturing organization. Assets identified in this view are properties of the SMU, and some of them can be transferred between different SMUs as needed.

An asset would be anything used for activities. It can also be a something that proactively executes such activities. For example, personnel in some cases conduct an activity after receiving instructions, and in other cases act based on their own decisions regarding the situation. In this view, there are four classes of assets as follows.

Personnel assets

Personnel working at production sites are valuable assets. Plant workers conduct operations such as producing a product in the physical world. Personnel also make decisions and give instructions to others, regardless of whether they are a manager or not.

Product assets

Both the products created as an outcome of manufacturing and materials used during production are assets. In addition, materials that eventually become a part of product such as components and assemblies are also counted as product assets.

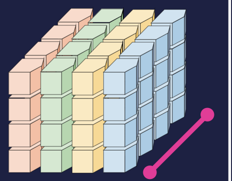
Plant assets

Equipment, machines and devices used for manufacturing products are regarded as assets of the plant. Things necessary for equipment operation such as jigs, tools, and subsidiary materials that are also part of a plant belong to this type of asset.

Process assets

Manufacturing sites have valuable knowledge of the operation such as production processes, methods and know-hows. This process knowledge also counts as a manufacturing asset.

Management View



The management view shows purposes and indices relevant for management.Assets and activities of SMUs should be appropriately steered in terms of quality, cost, delivery and environment, which represent the management view. An SMU can be examined to determine whether it will be fully optimized.

Each item of the view can be managed independently. Management classes such as quality management, cost management, delivery management and environment management exist across different asset views or activity views within the targeted SMU.

Quality

Quality is an index to measure how the characteristic of a product or service provided by an SMU serves the needs of customers or the external world. It is possible to discuss improvement of various kinds of qualities e.g. product quality which is directly connected to the values of customers, quality of plants or equipment to make the products or services, and the values of methods and personnel.

Delivery accuracy

Delivery accuracy is an index showing whether or not the time required to deliver the product or service meets the needs of the SMU' s customers. Location and methods used to provide products or services to the customers are also considered. It is necessary to both meet the requested deadline and fulfil exact time and place delivery in a way that is optimized for each customer.

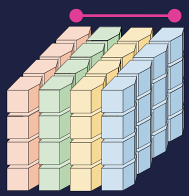
Cost

Cost is understood as the sum of financial resources and goods spent directly and indirectly in order for an SMU to provide a certain product or service. The concept of cost includes materials used that are converted into products, services invested for operating equipment, energy consumption, as well as financial resources and goods indirectly spent to maintain and manage plants. Here, the value of pre-existing assets is not included.

Environment

Environment is an index measuring the degree to which an SMU' s activities harmonize with the environment without placing an excessive strain on the natural world. This entails maintaining a favorable relationship with the environment and neighboring regions, managing emission of toxic substances and CO2 as well as material flows, and optimizing energy consumption.

Activity View



Smart manufacturing creates value from the outcome of human and machine activity. The activity view covers such activities performed by SMUs at manufacturing sites in the real world, which can be viewed as a dynamic cycle continuously improving targeted issues proactively.

Regardless of the purpose or the object of an activity, the activity view is composed of the cycle of four key activity classes: "Plan", "Do", "Check" and "Act".

Plan

"Plan" covers activity to make a list of action items to be executed either within a certain period or by a deadline. It may also decide the goal of behaviors in order to complete a given mission or to accomplish the objectives of an SMU.

Check

"Check" is an elementary class of activities to examine whether the goal set by planning activities has been achieved. It consists of analytically measuring how the physical world has changed as a result of executing planned actions, as well as investigating causes when the goal has not been achieved.

Do

"Do" refers to efforts taken to achieve a certain goal by executing concrete activities at the actual site in the physical world. These efforts can create new assets or change the state of existing assets based on the given goal.

Act

"Act" is a KAIZEN element improving the function of an SMU by defining the ideal situation and tasks for fixing any problems of the target. The action tries to change the structure or the system of the SMU itself in order to fill the gap of the current condition. Although machines and devices do not modify their own structures by themselves, an SMU in which a human intervenes changes its mechanism autonomously.

Chapter 2
Evolutional Model in Manufacturing

AS-IS Model and TO-BE Model

In the activity layer of the IVRA, contents of an SMU are described in the level of activities conducted by individual actors. Two types of models – AS-IS model and TO-BE model – are used for describing concrete activities in SMUs.

AS-IS Model

For both the cyber world and the physical world, existing "things" and real "occurrences" in the activity layer can be picked up and described according to a particular problem recognition. A model described in such a way is referred to as an AS-IS model. An activity scenario described as an AS-IS model is referred to as an AS-IS scenario.An AS-IS scenario is what expresses the current way of working. The real situation is expressed as it is by intention in order to enable discussions on its good/bad points and where problems lie.

The purpose of an AS-IS model is to clarify the problem with which to be concerned. A problem with which to be concerned means a state in which the situation in reality is different from a desired state. For this purpose, the real situation should be visualized and shared among stakeholders. In general, a problem can be described in the form of "XX is YY" .

TO-BE Model

Likewise, things that should exist and occurrences that should happen in reality are described as a desired state of the future. This model is called a TO-BE model. An activity scenario described as a TO-BE model is referred to as a TO- BE scenario. TO-BE is what expresses how a situation should be. It does not mean an ideal state. A TO-BE scenario describes a status which is expected to be realized by utilizing digital technologies such as IT and IoT.

The target of a TO-BE model is to clarify the problem to be solved. A problem to be solved means actions that should be taken to bring the reality to a desired state. For that, how the situation should be is described and the means to achieve this are clarified. Generally it can be written in the form of "XX will be made YY" .

Four Stages for Autonomous Evolution

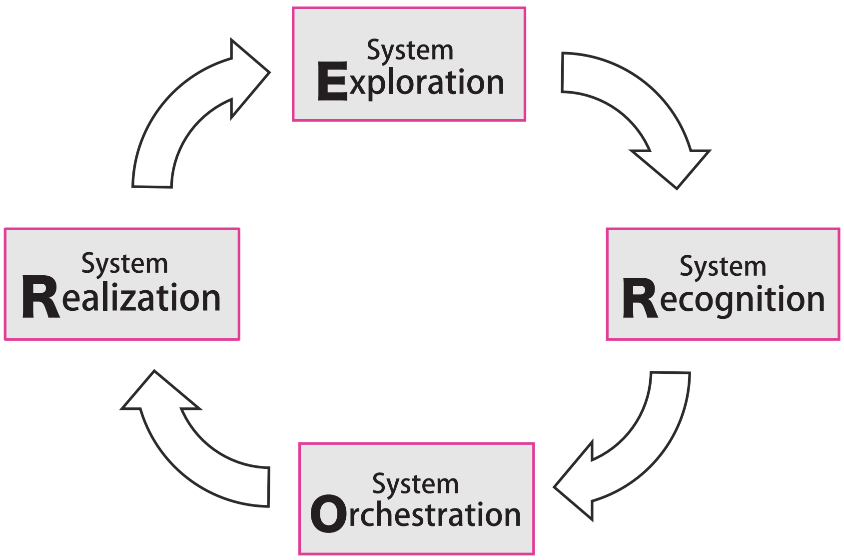


Fig. 5 EROR cycle for self-evolution

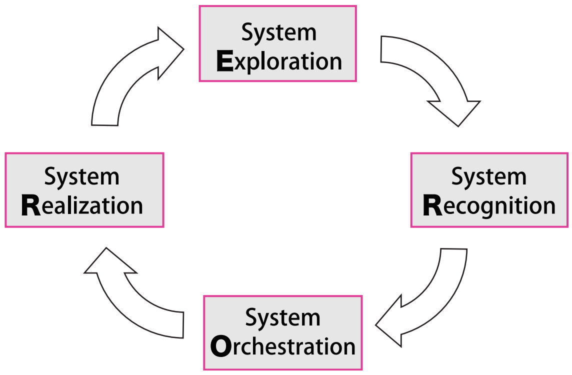
An SMU is a unit for smart manufacturing that thinks by itself and autonomously changes. It defines its own current condition, problems, and tasks as well as its desired form. Based on that, it evolves by modifying its structure or composition elements.

A PDCA cycle in the activity view of SMU is a KAIZEN cycle that originates in a production site. This cycle is suitable for solving relatively small problems. In the case of a larger change, such as a change in organization structure or a workflow, an EROR cycle is executed.

An EROR cycle to realize smart manufacturing starts from the current system at all times and is evolutionary. In other words, a system existing at a point of time is referred to as the origin when a new system for connected manufacturing is designed and embodied. This cycle is executed repeatedly.

An EROR cycle is composed of four steps: Exploration, Recognition, Orchestration and Realization. A cycle usually completes in one to three months and at most one year.

Four Stages
for Autonomous Evolution



STAGE 1	STAGE 2	STAGE 3	STAGE 4
System Exploration	System Recognition	System Orchestration	System Realization

In the stage of system exploration, fundamental issues such as where a problem lies and what the problem is are discussed. Firstly, the range or scope of a targeted problem is set. Then, through conducting as many hearings as possible from actual persons in charge and persons concerned, the actual situation such as who has a problem and where is grasped concretely, and the details are arranged. After that, the problem structure that has been revealed and the nature of a problem which can be detected from the structure are discussed. For example, brain storming, the KJ method (affinity diagram) and ethnography are effective means.

In the stage of system recognition, persons concerned need to mutually understand the actual situation correctly. Given that a concern is an interpretation of a situation, it becomes possible to share an understanding of the matter by expressing a situation in which the issue concerned arises as an activity scenario.

An activity scenario shows a picture in which multiple actors conducting operations in a manufacturing site perform various activities through exchanges of things and information.

In system orchestration, a problem to be solved is clarified by expressing a desired state of manufacturing organization or a system as an activity scenario based on the problem in the current situation.

In comparison to an activity scenario for the current situation (AS-IS scenario), useless parts are eliminated from information flow in a scenario for a desired state (TO-BE scenario) and added value is increased by automation as well as adoption of cyber technology.

Means to achieve such targets or goals are also discussed in the stage.

Current flows of operations or ways of working must be changed in order to realize an activity scenario of a desired state (TO-BE scenario).

At the same time, uselessness is eliminated and efficiency is enhanced by digitalization of traditional activities and by taking advantage of platforms that effectively utilize the cyber world.

By gradually expanding the world connected with digital technology, new operation flows which were once impossible to realize will be created, and added value will be drastically enhanced.

Scenario-Based Modeling Methodology

Here, activity scenarios are excerpted from operation flows as meaningful bundles and used as contents to write models. A scenario has the same meaning as that of a play or a novel. A scenario always has a writer who describes it based on his/her intention, but the contents are composed of elements existing (or likely to exist) in reality.

Activity scenarios are easy to understand and memorable for listeners and readers as stories unfolding from a perspective of an actor who appears there. Expressing manufacturing activity models in the activity layer as scenarios is effective for building consensus and communicating accurately, since it helps stakeholders understand the contents.

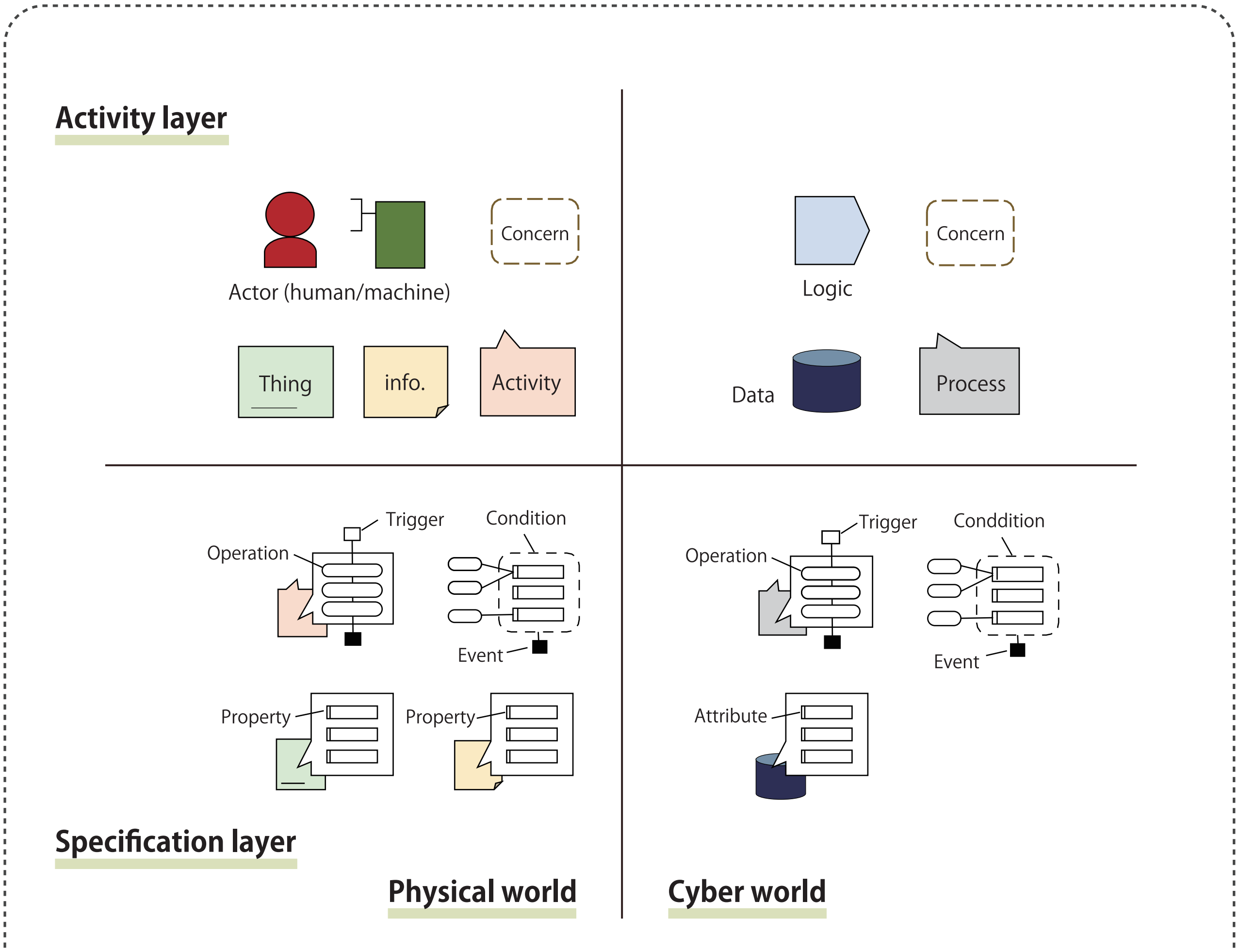


Fig. 6　Icons of scenario defining elements

Scenario-Based Modeling Methodology

Activity scenarios start with concerns. Concerns are represented as sentences that describe the problems at each work site (AS-IS) or as they should be (TO-BE). The physical and cyber-world steps from stage 1 to stage 2 in the previous section should be assessed from an objective point of view that is removed from the subject activity.

At the same time, in modeling activity scenarios, the four elements in the physical world and the three elements in the cyber world as below are used in order to represent the activities that are the subject of the concerns.

Physical world

Actor

An actor conducts activities related to production by independently making decisions. Not only workers in charge but also automated machines can be regarded as actors. An actor in charge of a work in each scene is defined by his/her role. Actors are named in a manner in which the role (function) is obvious instead of using proper names.

Activity

An activity is a unit of work conducted by an actor. It is defined as a unit of work for which output can be taken over by another actor. In other words, if an activity is stopped in the middle and the remaining part can be continued by a substitute actor, it is regarded as a single set of activity.

Thing

A thing is a visible object existing physically. It exists at a point in the physical space at a certain point of time. All products, parts, equipment and tools in a manufacturing site can be “things” but here the term indicates targets of concrete operations in activities.

Information

Information is what expresses contents needed by actors to make some decision. In reality, physical things such as paper, boards and display devices become media. Here information means contents shown on them.

Cyber world

Logic

When an activity which was once conducted by an actor is done in the cyber world, a part of it is executed by an alternative existence. This is logic in the cyber world. It is embodied by software in a component using digital technologies to work in a platform.

Process

A process is a unit of function constituting logic which corresponds to an activity in the physical world. Processes involve data input and output, and as a result, the state of the data changes. Therefore, the functions of a process can be defined by their states before and after.

Data

Data is a unit existing in the cyber world which has contents describing things and information in the physical world. In practice, a unit of data is composed of multiple attributes which have values (qualitative and quantitative). It becomes an input or an output of a process, and in some cases data can be correspondent to things or information.

Among the steps that lead to Stage 3 System Orchestration and Stage 4 System Realization in the EROR cycle, system definition, analysis, design, and implementation are executed to solve the concern. These are discussed in the specification layer of IVRA, and the five following configuration elements are available for notation.

Operation

An operation is a unit expressing contents of an activity of an actor in the physical world or a process in a service defined in the cyber world. It is possible to differentiate the term by referring to it as an activity operation in case of the physical world and as a process operation in the cyber world.

Property

A property is a unit that expresses a concrete content of a thing or information in the physical world. In some cases, it is specified as a thing property or an information property. Contents of properties are modified by activity operations. For example, when a thing is lifted, a value of the property of location (altitude) is changed.

Attribute

An attribute is a constituent element to express contents of data in the cyber world. It is also called a data attribute. For a unit of data, one or more attributes are defined. The data is specified by values of attributes. A value of an attribute is set or changed by a process operation. Also, a condition category is changed by a combination of attribute values.

Condition

In the cyber world, a category of cyber condition is decided depending on values that data attributes have, and it changes from time to time. In the physical world, the conditions are defined by the thing and information properties. The category of a condition is used to define the event, and as criteria for determining the logic and activities inside various processes.

Event ／ Trigger

An event is an occurrence that is defined beforehand. It is specified in a condition or a process. Events are defined in both the cyber world and physical world and are mutually linked. For example, a phenomenon in which temperature exceeds a certain threshold defined in the cyber world. Among events, ones which start certain processes are referred to as triggers.

Relation of the Cyber World and the Physical World

A cyber-physical system is a system in which the physical world such as production sites and the digitalized cyber world are seamlessly combined.

In fact, digital technologies and network technologies have been used for years on factory floors. This is to say, in addition to digitalization by data input conventionally done by workers, IoT has made it possible to create data directly from things as well as to send data directly from networks to things. Figure 7 shows a cross section of an activity scenario in which the physical world consisting of actors, activities, things and information is interconnected with the cyber world consisting of data and services.

Things and information in the physical world which are connected to data in the cyber world are distinguished by attaching digital marks (small icons indicating data). Information with a digital mark is equivalent to a device such as a display device. On the other hand, a thing with a digital mark is a so-called IoT device characterized by sending data from the thing on the factory floor to the cyber world.

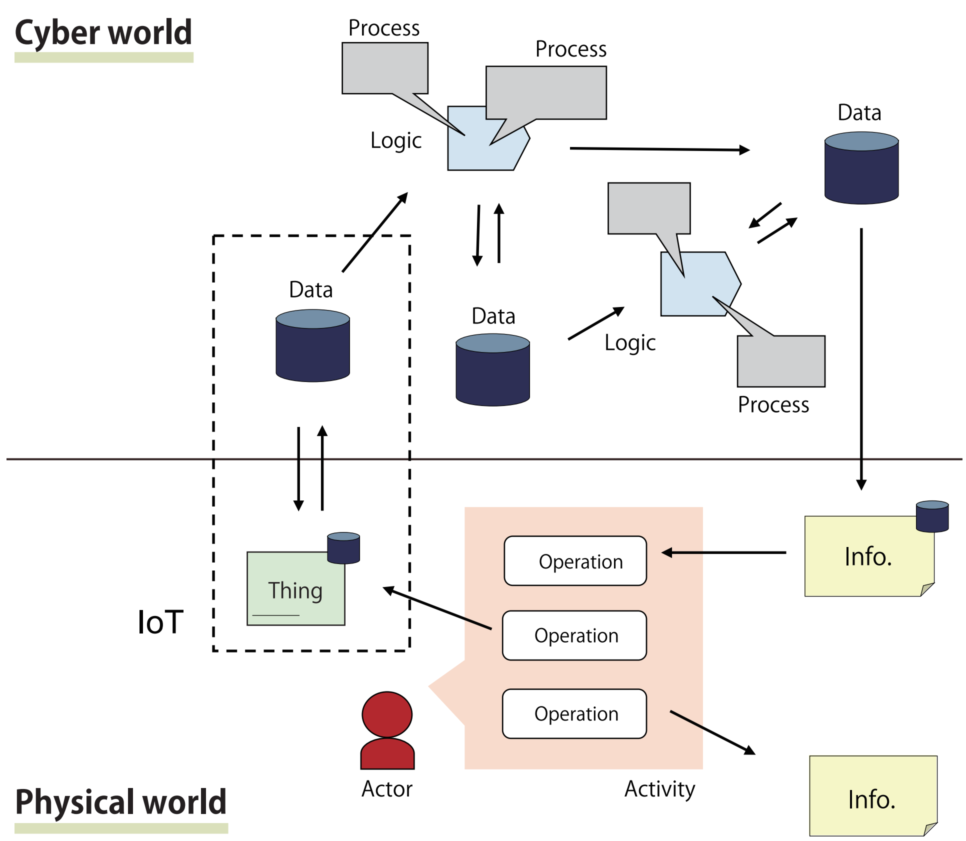


Fig. 7 Cyber and physical integration

PLU – a Basic Unit for SMU Connection

An SMU, which is a unit executing manufacturing, cannot create the final form of value by itself. The activities executed by an SMU at a given place and time follow the product axis and service axis, and are finally delivered to the user to complete the value chain. These SMU linkages form the necessary chains and are required to achieve efficient and effective value chains even if the different companies have different principles and values.

As SMUs have physical and spatial sites in the physical world, transfers of actors, things and information are particularly needed in connections among SMUs. It is also necessary to manage such transfers of physical objects together with transfers of data and money in the cyber world. A unit managing transfers of a set of actor, thing, information, data and value between SMUs is referred to as a portable loading unit (PLU).

In the business layer a PLU corresponds to an economic transaction in which a product or service is exchanged between SMUs. Not only exchanges among businesses but also those within an enterprise can be managed by PLUs if the units such as sections, factories and groups are profit centers.

Furthermore, by establishing a control center that is independent of SMUs and PLUs, movement in both the physical and cyber worlds is secure, and at the same time the movement history can be understood from a neutral standpoint. In Figure 8, the Hyper Connection Server (HCS) is connected to the Hyper Connection Terminals (HCT) of each SMU as the management center in order to assure security and traceability. These mechanisms are described in Chapter 4.

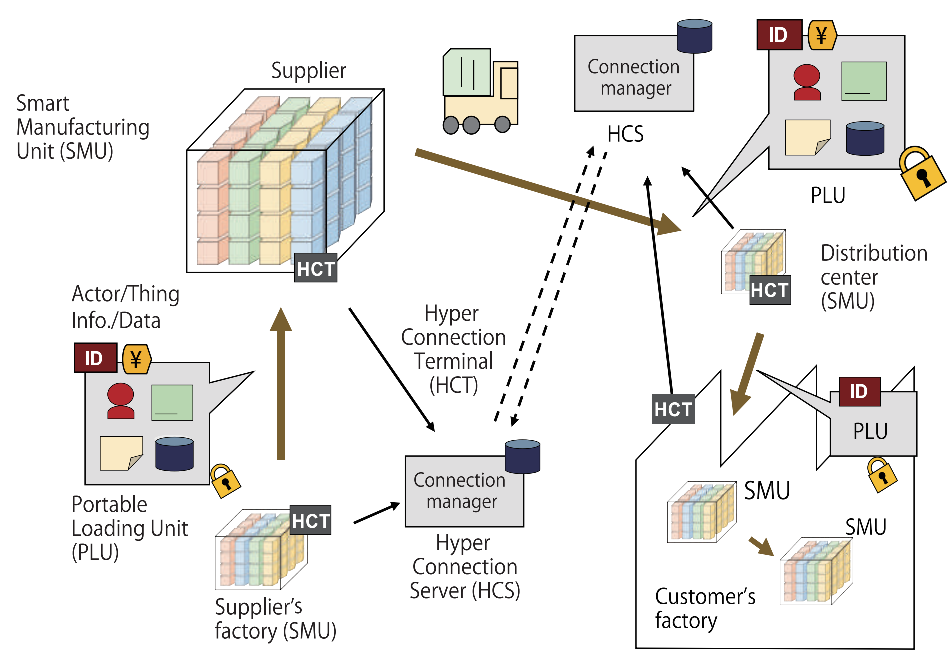


Fig. 8 Cross border management by PLU

Chapter 3 Platform Reference Architecture

Positioning of Platform in IVRA Layers

The term "platform" has several different meanings, and here it is defined as "a mechanism for mutual use of data between different work and systems." In the three IVRA layers, first the position is clarified in the business layer, and specific ways of using a platform (use cases) are discussed in the activity layer. The contents and structure of a platform are described in the specification layer.

As Figure 9 shows, platforms are mainly involved in the cyber world. In production sites of the manufacturing industry, various actual activities are converted to the cyber world by using digital technology, and new developments are being discovered through processing in the cyber world.

From a viewpoint of an activity scenario, a platform can be defined as a system to effectively utilize the cyber world. Therefore, a use case of a platform indicates a form of usage such as how data or digital technology in the cyber world can be utilized by an activity scenario. To look from the perspective of the system granularity or hierarchy, platforms, which are positioned in the cyber side of the IVRA, have the following relationships:

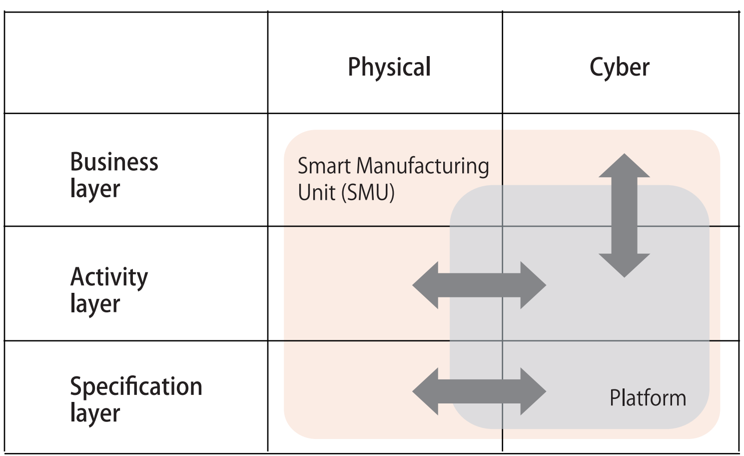


Fig. 9 Positioning of platform in SMU

Platform ecosystem

The uppermost level of the hierarchy is platform ecosystems. A platform ecosystem is a state in which different constituent platforms are loosely connected by some relations. Each platform in an ecosystem is its constituting element but is not in a position being able to control the ecosystem. Thus, a platform ecosystem as a whole is made up based on autonomous decision-making of individual platforms.

Component

Components include software that is designed in advance and meets a quality level to be provided as products, as well as necessary hardware. A component has some function independently which can be provided to users. But in many cases, it needs to connect to other components in order to execute its function. The connecting of components is the reason for the existence of platforms.

Platform

A platform is a unit which beforehand ensures or supports interoperability of its components by some rule or terms.
A provider of a platform (a platformer) has two aspects: It collects components constituting the platform, and at the same time it provides a service gathering users who actually utilize the platform for manufacturing.

Service

Services are the software that make up components, and specifically, they correspond to the logic and processes in the specification layer.
These are units that directly or indirectly provide value to customers. If a connection of services is within a component, it is provided in a form defined by the component in advance.

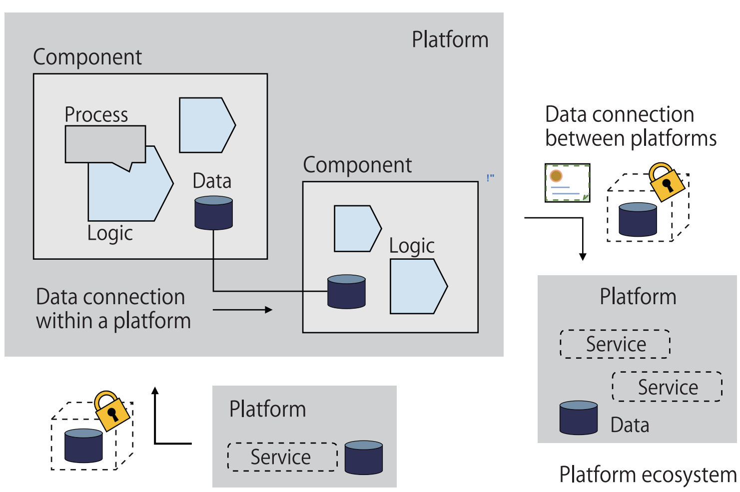


Fig. 10 Specific hierarchical structure of platforms

Categories of Components

A platform is a system that realizes connected manufacturing in the cyber side. It is composed of the following four kinds of components. In a precise sense, they are types of services constituting components, that is to say, types of functions which provide those services.

【 Four kinds of components 】

IoT Device

An IoT device is located on the border of the physical world and the cyber world and conducts conversion between things or information needed in operations, and data used in the cyber side. Such conversions consist of those from the physical world to the cyber world, as well as those in the opposite direction.

Service Tool

A service tool has a secondary function to facilitate efficient and proper working of devices and applications. Secondary functions of tools include those specific for devices (but not specific for applications) and those which are shared among different devices and applications. For example, existing tools include construction tools, diagnostic tools, conversion tools and optimization tools.

Application

An application serves a function in the cyber world which was formerly performed in an operation. It consists of one or more services. In general, these also have input and output devices, but here things have been simplified and they are defined as conversion functions that input data and output data.

Data Infrastructure

In the cyber world, data infrastructure stores and saves data, and if necessary, has functions to retrieve data, and transfers data between different locations. In addition, it has secondary functions to achieve the aforementioned functions, as well as common secondary functions to support the operation and functions of physical security, platforms and components.

Object Models for Problem Specifications

In an SMU, the physical world and the cyber world are integrated to practice connected manufacturing. Processes constituting services as well as data and data attribute as their targets are correlated with actors, things and information in the physical side. Figure 11 illustrates the relationship of objects in the cyber world and ones in the physical world.

Elements in the cyber world and the physical world indicate relationships between data attribute and properties of things, or between data attributes and properties. In addition, they are also connected with triggers based on events as shown in Figure 12.

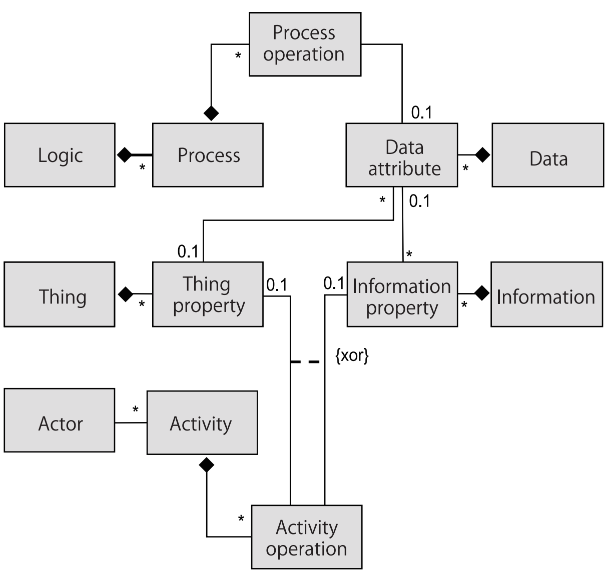


Fig. 11　Object diagram of scenario elements

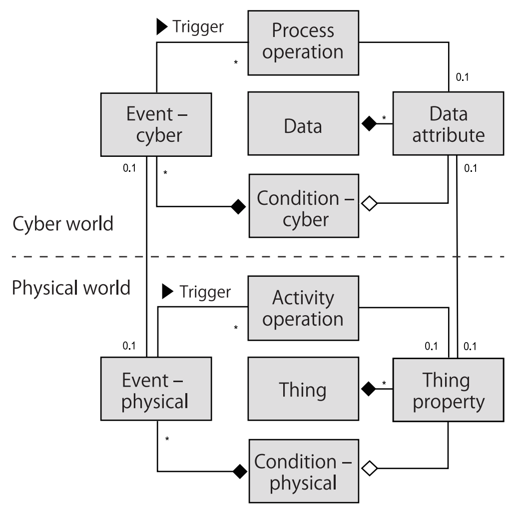


Fig. 12　Crossing between the cyber and physical worlds

Hierarchy of System of Systems

In a cyber-physical system, production sites in the physical world and the cyber world with platforms as its core realize connected manufacturing by mutually complementing functions. A cyber-physical system is a system of systems in which systems in different levels are interconnected. That makes it possible to deal with problems at high levels that cannot be solved by a single system.
Connections of systems are classified by granularity (hierarchy) of objects to be connected as follow.

1. Connection among Services

A service is a unit the result of which can be evaluated by physical users or upper level users in the business layer. Connections in this level are managed by individual components.

2. Connection among Components

A component is a unit of multiple services which are tightly coupled. Mutual connections of components are ensured in the range assumed by the suppliers. Thus, connections among components are conducted by the users or platforms.

3. Connection among Platforms

In most cases, connections among platforms are autonomous decentralized systems without core management functions. Thus, it is not fundamentally ensured that connections are correctly made. However, it is possible to connect multiple platforms as an ecosystem when the platforms agree with a unified rule, terms or connection procedures.

There are two ways of mutually coupling components: Coupling them through a platform and coupling them directly. It is necessary to specifically consider all the individual requirements at the implementation level, and there are two types of coupling: The tight coupling inter-operation and loose coupling inter-operation.

1. Tight coupling inter-operation

The tight coupling inter-operation is a form of connection in which components mutually boot a service of another component and utilize it by using API (Application Interface) and SDK (Software Development Kit). This type enables speedy and high-quality connections, but has issues in serviceability, for example, when a function of one of the components is extended.

2. Loose coupling inter-operation

The loose coupling inter-operation is a form which minimizes effects of future function extension of the other components as well as enables components' own function extension by loosening the degree of coupling between components. API protocols in the lower implementation level are limited to versatile ones which are already widespread, and those semantic usages are described in profiles.

Types of Profiles for Interoperability

Given that a platform is a system to improve interoperability among components, component profiles are necessary to connect constituent components through the form of loose coupling inter-operation. When components are connected across platforms, profiles for messages exchanged there are also needed. The following are types of profiles related to connection:

① Platform Profile

A platform profile specifies contents of a platform. It includes an internal profile concerning components composing the platform and an external profile describing external features of the platform.

② Component Profile

A component profile describes contents of the component service and necessary data. Component profiles are written in a manner understandable for developers of systems, in order to connect systems in accordance with individual model dictionaries or a common model dictionary.

③ Message Profile

A message profile shows contents of a message and the condition in which the message is sent, so that a message delivered from a sender to a receiver can be managed when it is separated from the environment.

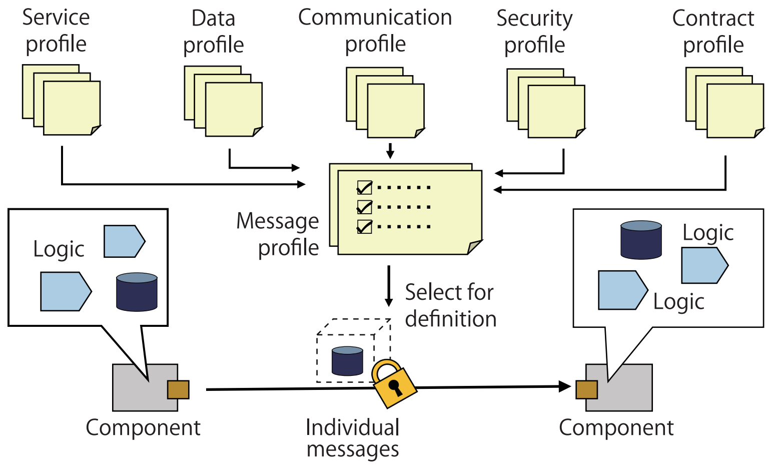


Fig. 13 Data distribution with profiles

As Figure 13 shows, message profiles have the following contents. If necessary, these contents are defined in platform profiles and component profiles.

①

Service Profile

A service profile describes contents of a service that a component has. It contains information such as service contents, use cases, restrictions and authority in usage of the service.

②

Data Profile

A data profile describes the structure and properties of data which is input/output by a component or included in a message. Contents of an individual data dictionary or a common data dictionary are used in a data profile, depending on the level.

③

Communication Profile

A communication profile documents contents corresponding to a communication protocol in a broad sense, such as timing or procedures of data exchanges and responses to authentication or errors, when a component uses a service of another component.

④

Security Profile

A security profile describes contents concerning security such as authorization related to contents or usages, authentication and encryption.

⑤

Contract Profile

The contract profile sets the data transmission and usage rules for the contents of contracts and similar documents that have been decided between companies in the business layer.

Chapter 4

Framework for Connected Industries

Data Sovereignty Control

As the manufacturing industry transitions towards a digital society, the spotlight is on the value of data in the production place. Data is not tangible, so the concept of ownership does not apply to it. Therefore, unless the data is something creative for which copyrights can be applied or managed as a trade secret once data is released it cannot be retrieved, posing a great barrier to open connections.

In the world of the Internet, big data, in which Silicon Valley companies are taking the lead, is prompting economic development which can be called disruptive. The data handled within these trends mainly concerns consumption activities. In comparison, most of the data handled by the manufacturing industry is deep data that has strong diversity, dependency and decentrality.

Deep data that is handled by the manufacturing industry is not suitable for distribution by third parties in the same way as big data. In order to distribute data for connected manufacturing, the connection will basically be directly between businesses and peer-to-peer.

If such a cooperative distribution type of architecture is the prerequisite, then the party providing the manufacturing data can maintain its sovereignty while allowing multiple users the rights to use the data. By maintaining the usage and access rights to data that one has generated as well as the authority to set those rights, i.e., by systematically and technically assuring data sovereignty, connected manufacturing will be practical as a business.

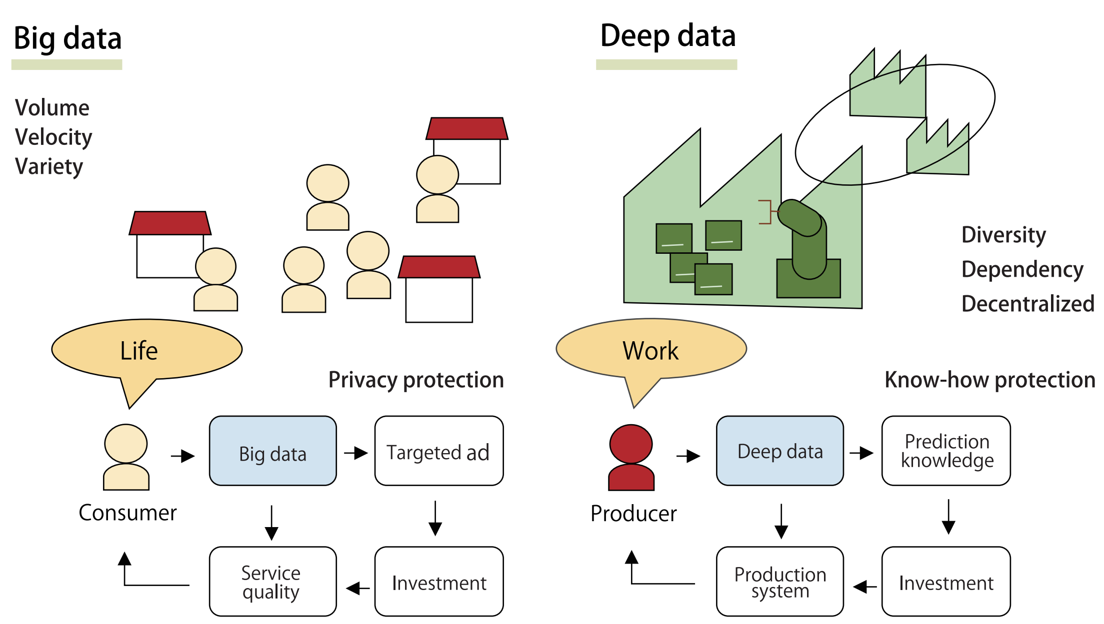


Fig. 14 Big data and deep data

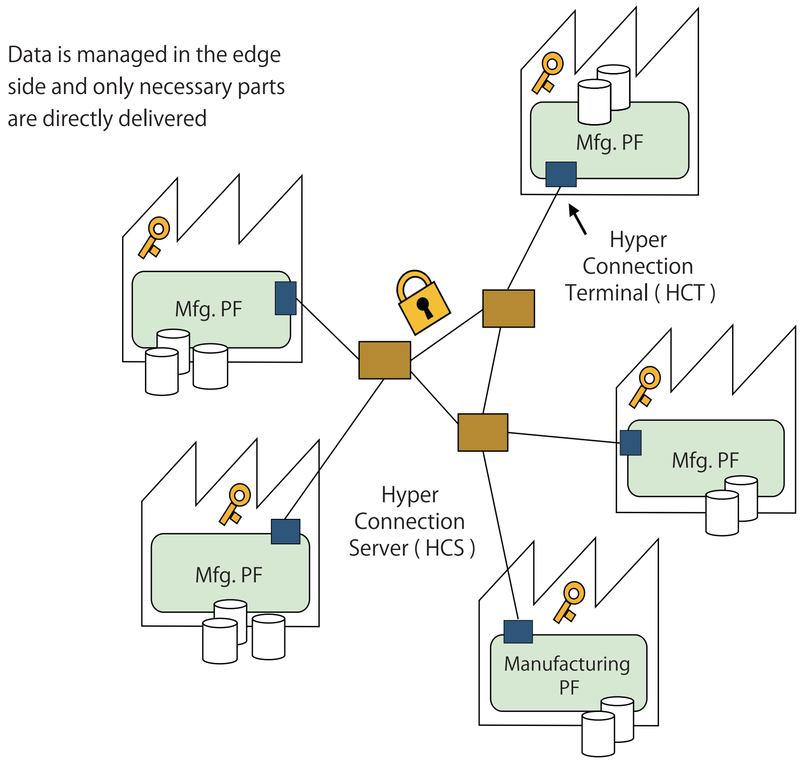


Fig. 15 Decentralized architecture for data distribution

Data distribution process between parties

A form of transactions in data distribution based on assured data sovereignty as an example, the following steps are possible.

【 Step 1 】
The data user specifies the type of data, its use and period, and sets a service to automatically process the received data. Then, a data provider refers if the data can be provided.

【 Step 2 】
The provider specifies the service to generate the required data, confirms that the data can be provided automatically responding to the request, and then responds.

【 Step 3 】
The data provider and user set their communication profiles and security profiles, and after agreeing to contract conditions, set the contract profile.

【 Step 4 】
After the message profile is completed, it is registered in the system via a Hyper Connection Terminal (HCT), and an ID is also allocated concurrently to the corresponding component.

【 Step 5 】
The data user sends a request to the HCT using the profile ID. The data provider's component regularly sends inquiries to the HCT, and provide data according to the profile ID if there are any request.

【 Step 6 】
The data user pays the data provider the usage fee for the contents of the data received based on stipulations of the contract.

General Framework for PLU Distribution

Transfers between SMUs in the cyber world and the physical worlds, which are managed in correspondence by PLUs, have different routes. Transfers in the physical world are mostly done in daily work of logistics service providers, and are managed by physical containers. On the other hand, transfers in the cyber world are managed by cyber containers which are correlated as PLUs by setting unified IDs.

A PLU also involves a transfer of value. The transfer of value is established when the cyber container and physical container are matched at the receiving side.

Therefore, a mechanism can be made to link payment processing by a financial institution with such transaction data which a third party can verify.

In transfers of PLUs in the physical world, it is common that there are some stopping points between a loading site and a receiving site due to physical restrictions, institutions of countries and regions, and business restrictions of enterprises. Here, such stopping points are also defined as SMUs. Their basic elements such as actors, things, information and activities as well as relationships among them can be defined in the activity layer.

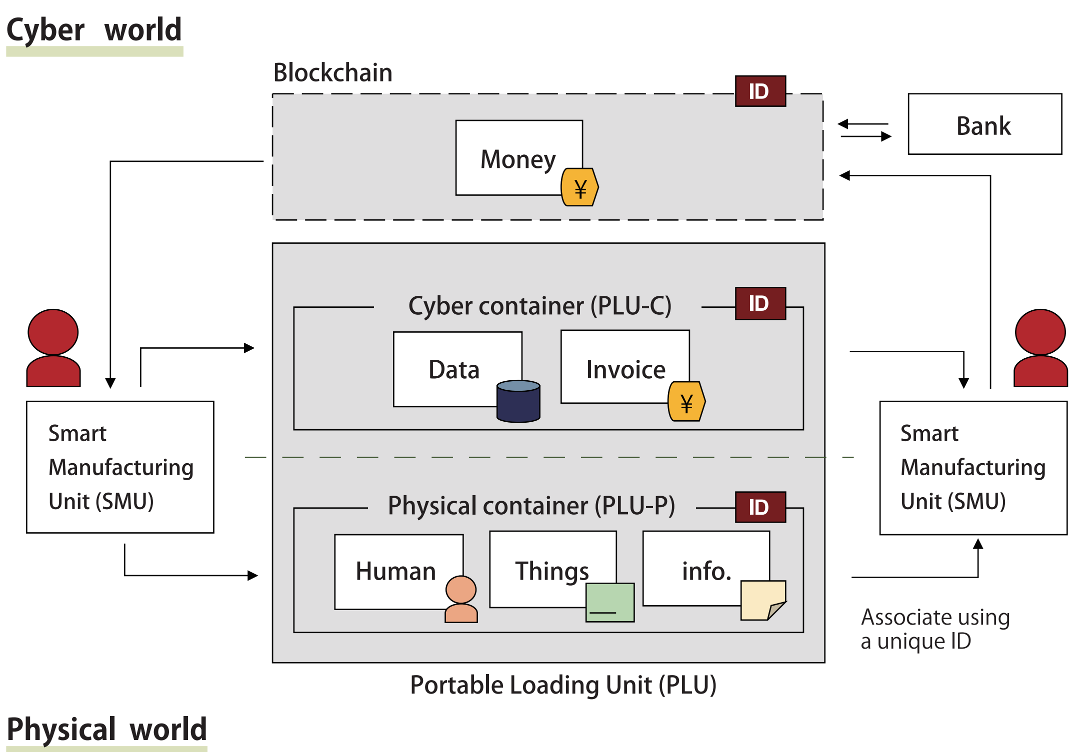


Fig. 16 Cyber-physical correspondence in PLU

General Framework for PLU Distribution

SMUs including stopping points which are related to transfers of PLUs manage receipts and shipments by Hyper Connection Terminals (HCTs) in sites, and send the contents to Hyper Connection Servers (HCSs) managing traceability each time. HCTs at loading sites and receiving sites handle both cyber containers (PLU-Cs) and physical containers (PLU-Ps) correspondingly and send sets of those contents to traceability servers. PLU-Cs and PLU-Ps are treated separately in other SMUs between two points, since they take different routes.

From a business viewpoint, it is not ensured all stopping points and the receiving site for a PLU convey facts of receipt to a traceability server via HCTs. Although costs for digitalization at production sites are decreased because of progress in IoT technologies, it will not be realized if benefits do not meet the costs. Hence, a mechanism of SMU connection with PLUs should coordinate with payment systems of financial institutions such as banks in order to make commercial transactions close only after facts of receiving PLUs are reported.

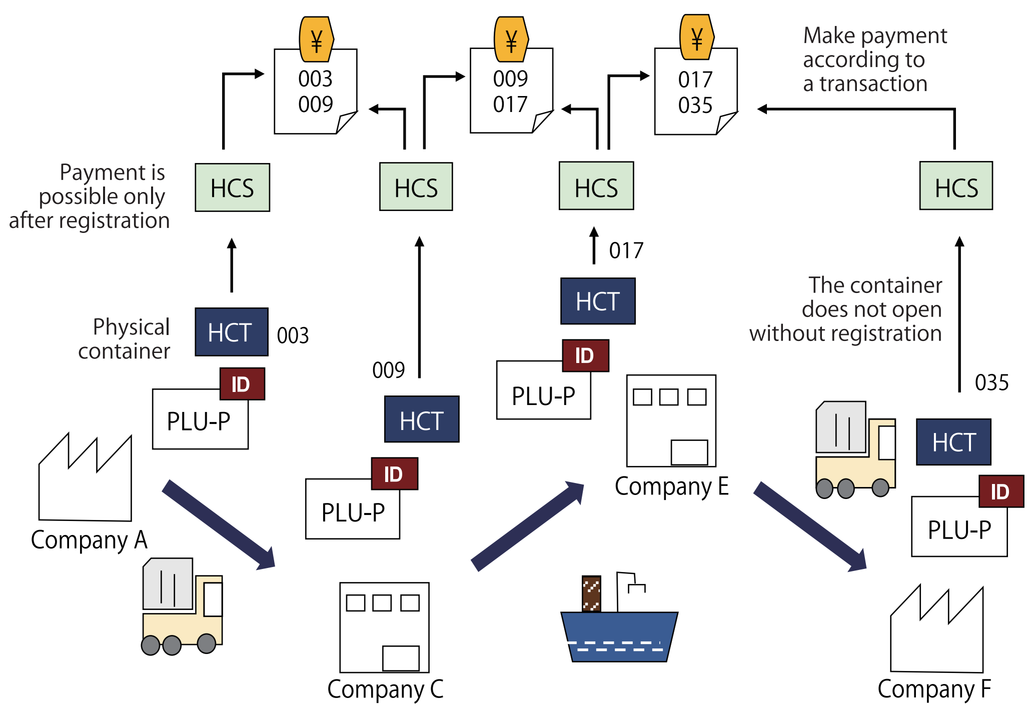


Fig. 17 Traceability management by HCS

Structure of Hyper Connection Server

Hyper connection terminals (HCTs) are base points for connections among SMUs in the cyber world. They directly manage activities of SMUs as starting points, stopping points and last stops of PLUs.

On the other hand, a hyper connection server (HCS) has functions enabling HCTs to mutually send and receive PLU-Cs.

They are composed of data connection servers, transaction-history servers (traceability servers), common dictionary servers and public key servers that assure security. In addition to these, an authentication server registers authentication of each HCT as well as an SMU under that and its services, and then manages service IDs of starting points and final stops in PLU connections.

Data connection server

A data connection server sends a request to the request destination in response to a data request from a terminal. Once a response is received, the data connection server will send the data to the terminal. The data provider receives the request, references the corresponding terminal and component, and returns the result.

Transaction history server

A transaction history server contains all records of transfers of PLUs in cyber space and the physical space to secure traceability.

Records are set in a manner so that senders, receivers and data contents to be sent can be specified.

Common dictionary server

Terms used on factory floors are heterogeneous. A common dictionary server converts such terms used in an individual system to terms defined in a common dictionary and alleviate the gap in the meanings, in order to enable communication between different parties.

A common dictionary server manages such dictionaries and a commonalized dictionary.

Public key server

When connecting data, all data is encoded to be sent over the Internet. In order to assure that the encoded data can be decoded by the correct recipient, a public key server manages public and secret keys. A public key is sent to a trustworthy party beforehand, and it is used as a key to encode data sent to oneself.

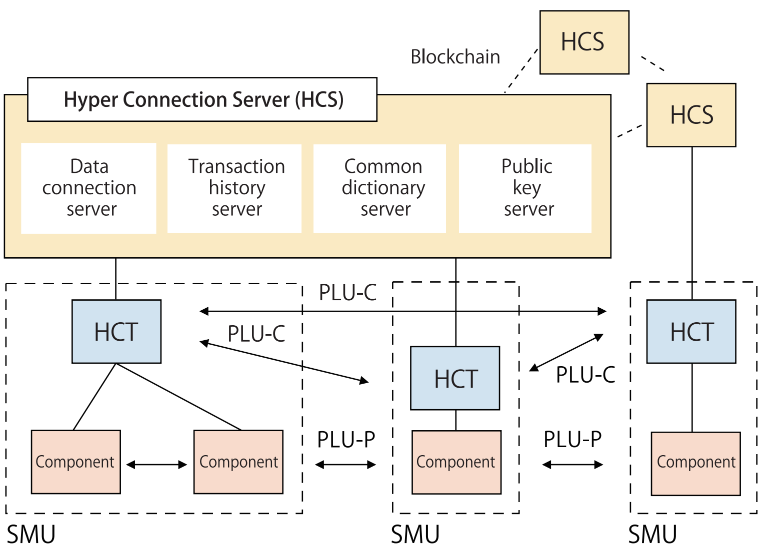


Fig. 18 System architecture of HCS

An HSC is not the only server. Based on blockchain technology, autonomous decentralized management is provided by multiple servers.

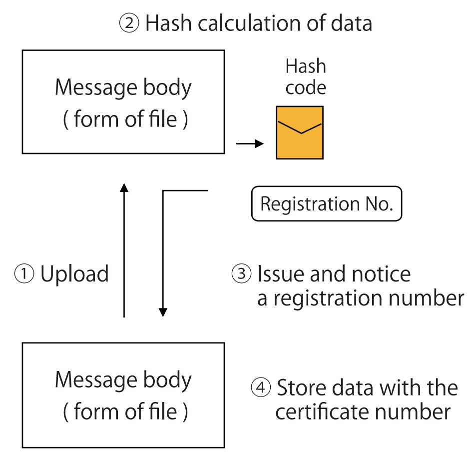
Proof of Delivery by Blockchain Management

When exchanging things, information, and data among multiple SMUs, Hyper Connection Servers (HCSs) play an important role. With conventional architectures, implementation of HCSs that must assure high security and reliability would require huge information system investment. However, by utilizing blockchain technology, such systems can be implemented relatively cheaply.

Blockchain technology enables to save a history of the fact that data was sent from a sending terminal to a receiving terminal. This can be used at a later date to trace the data, to certify the source generating the data, and to refer to the fact in business processes which accompanies the data transfer.

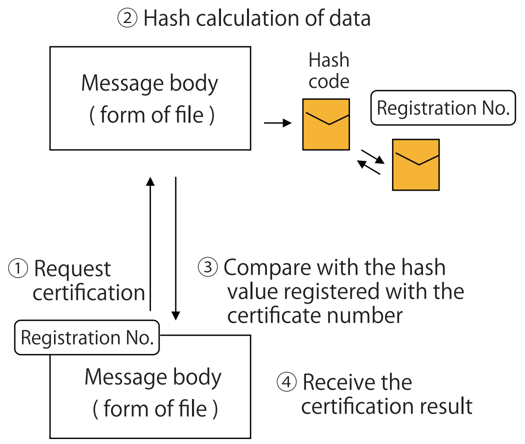
The basic principle is the same as cryptocurrencies such as Bitcoin, but many functions are not necessary. Here, decentralized ledgers in which falsification of data is practically impossible are managed. All transactions within specified time slots are placed into a block, and the blocks are stored on multiple servers.

Using such a system can alleviate a number of concerns related to data distribution, such as proving the ownership of data, proving the delivery of data, proving the usage of data, etc.



(a) Process of data registration

Fig. 19 Procedure of data



(b) Certifying registered data

sovereignty management

Proof of data sovereignty

This is a service in which a third party proves that a certain business held certain data at a certain time. This is logically impossible when the subject data is completely confidential, but when the data is disclosed to a trustworthy third party, then it is possible to assert the originality. Figure 19 shows this process.

Proof of data delivery

This is based on the same principle. It is a service in which a third party proves that data has been sent from business A to business B, or as an application, when a PLU that handles the parts in cyber world and physical world as a pair is sent from business A to business B.
PLUs are an essential element for connected factories. When they are used to connect multiple factories, transfer of ownership and rights becomes possible between the companies that own the factories. In order to assure fair transactions in such business dealings, a function to prove delivery with a very simple mechanism is necessary.

Trail of data usage

Consider a case in which business A provides data to business B and authorizes its use. If a user with malicious intentions falsified the usage of the data received when applying for it, they could use it for another purpose after receiving the data (e.g., provide it to a third party, acquire knowledge from the data, etc.). In most such cases, the provider would not know about this fact or would not have any recourse.

Trail of data usage is achieved by understanding each individual usage. When a data provider sends data to a data user, the user's terminal (HCT) does not maintain the data in a tangible form within the component that is the final user. Instead, it uses the data within memory so that each individual use can be tracked. Trail of data usage allows providers to know when and how many times the user has used the data that was provided. By linking this with fee charging systems, a new business model can be developed.

Dictionary Management by Loosely Defined Standard

Each platform has a local dictionary to assure internal component connections and to facilitate adding new components. Conversely, when multiple platforms mutually link data, they cannot be connected as-is because they each have different dictionaries. Therefore, as Figure 20 shows, a common dictionary is created by a neutral organization to be used between the parties. Common dictionaries retrieve the common parts of the individual dictionaries within each platform.

The relationships between individual dictionaries and common dictionaries are defined in a conversion map. If there is no applicable term between dictionaries, then a tentative term is assigned, and these must be initially defined by a human being. However, utilizing such individual dictionaries will allow the use of features of individual production facilities and the platforms that cover them, and the dictionaries themselves will grow as loosely defined standards.

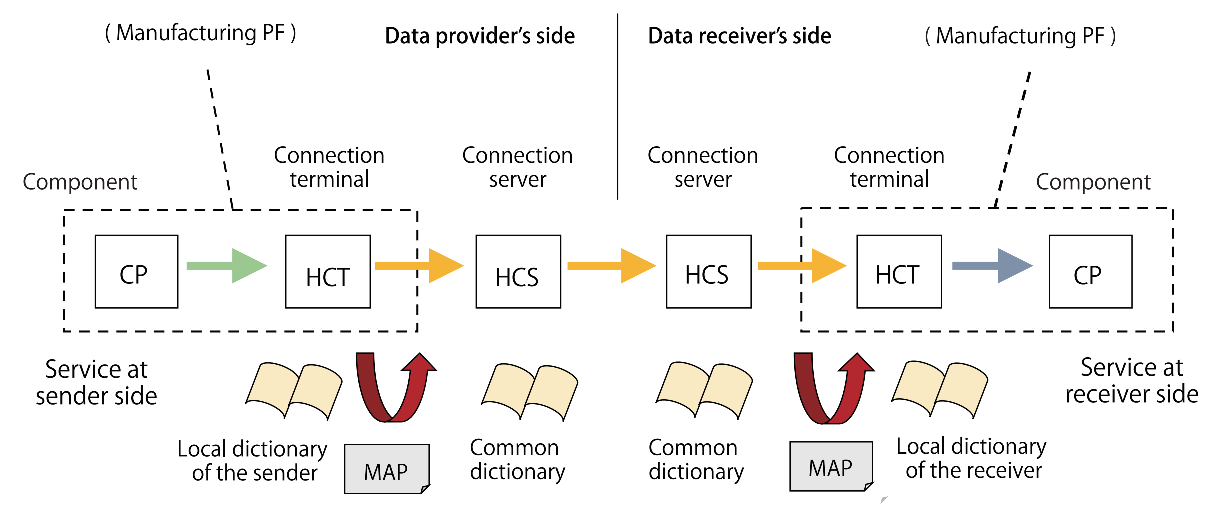


Fig. 20 Interoperability on local dictionary

A loosely defined standard in this case means that definitions in a data dictionary are not fixed in advance, but instead decided temporarily by commonalizing from actual situations of components in a bottom-up approach. When usage of the systems advances and an operation itself evolves, the temporal data dictionary is reviewed and updated.

A cycle of updating a data dictionary is usually from a half-year to one year. A cycle consists of four steps.

When a data dictionary registered at a point in time is utilized for an individual model, suitable terms are selected from it, but if there is a lack or an irrelevance of terms, terms are added or deleted as needed. Through gradually accumulating such differences, a new dictionary is created by remaining terms frequently used, adding important items which it lacked and removing ones not used.

Practically speaking, a problem may occur in terms of compatibility with an old system when a data dictionary is updated. Systems should be able to evolve by adaption in order to avoid such problems. Such a mechanism for dictionary maintenance is of particular importance in management of an integrated data dictionary for connections among platforms.

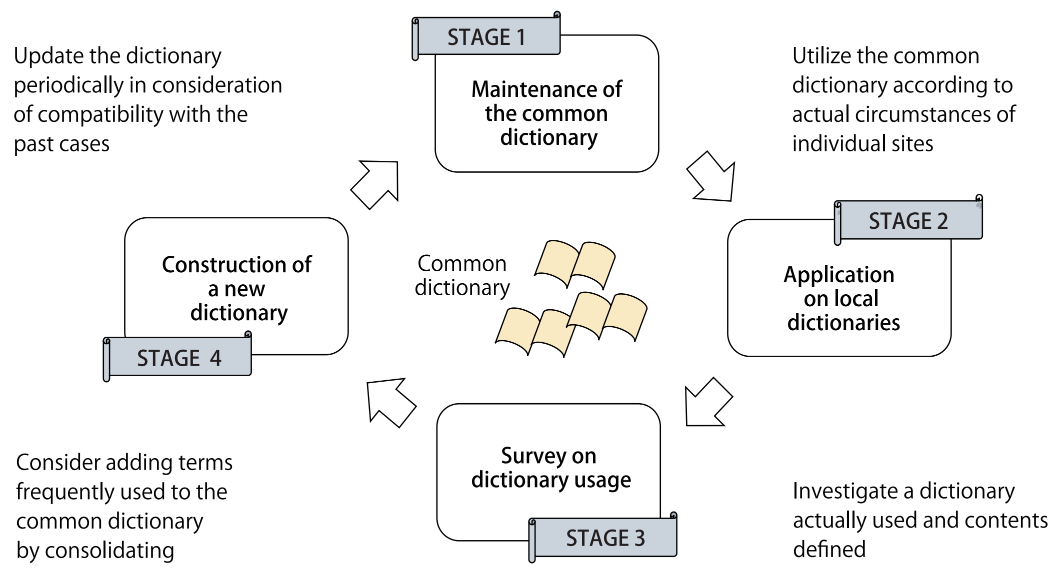
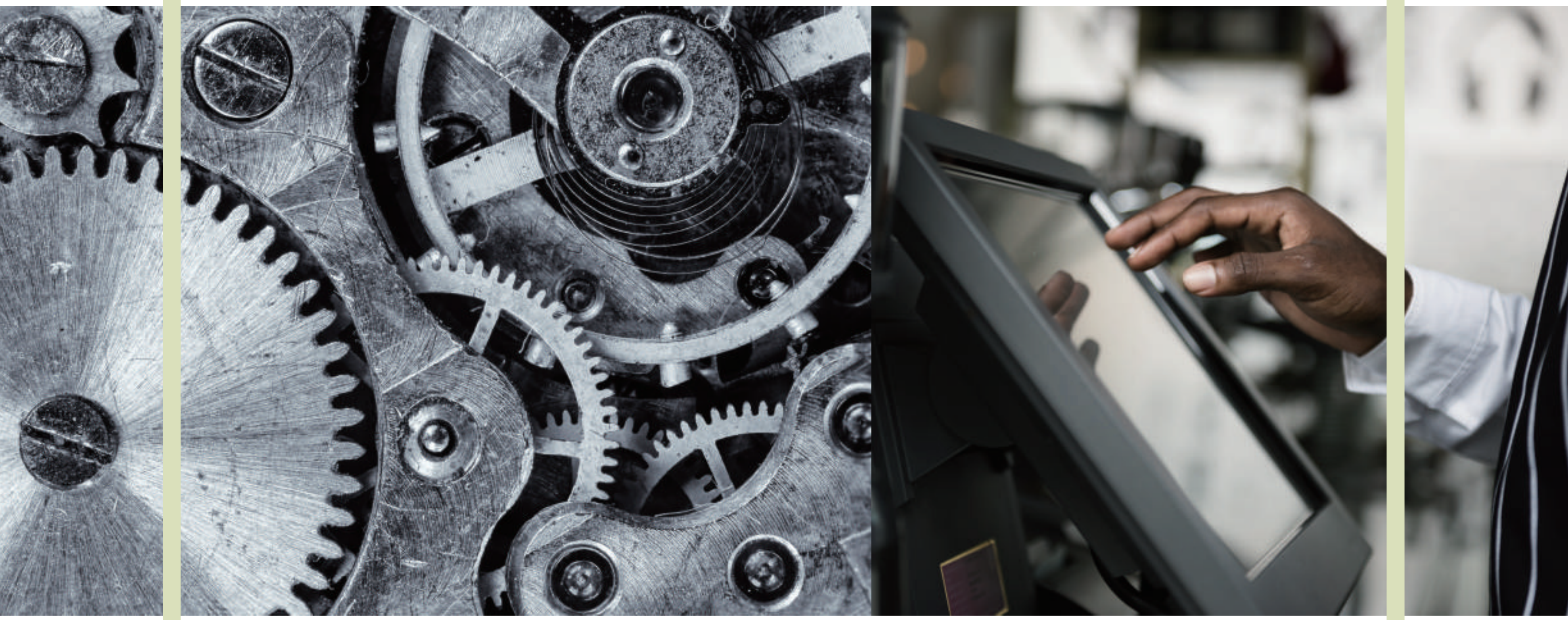


Fig. 21 Maintenance cycle of dictionary

IVRA Next

Strategic implementation framework of industrial value chain for connected industries



Published on March 1, 2018

——— Publisher ———

Industrial Value Chain Initiative

President：Prof. Dr. Yasuyuki Nishioka

Monodukuri Nippon Conference c/o

14-1 Koami-cho, Nihombashi, Chuo-ku, Tokyo

103-8548 Japan

MAIL：global_office@iv-i.org

URL：https://iv-i.org/wp/en/