Series

Toward Realization of Smart Manufacturing Systems

Case: Improvement of the Machining Process Productivity Based on the Machine Tool Technology

Robot Revolution Initiative

WG for manufacturing business revolution through IoT

The Industrial Machinery Steering Committee

April 2016

Contents

1. What is implementation of smart manufacturing?

Currently, new information technologies including IoT, big data, and artificial intelligence (AI) have brought significant changes in various fields of the economic society and a reform called "the 4th industrial revolution" is occurring in the manufacturing industry also.

Until now, in the manufacturing industry, the information and knowledge intensive reforms have occurred to in the manufacturing process. Above all, in particular, in a machining process (a process starting from setting work in a machine tool up to the final process in a production line), control systems are developing at high levels by commanding the digital control technology while pursuing improvement of accuracy and efficiency. Such control systems generate and process a large volume of data with variety of types including information on the status of the work, which is the target of machining and information relating to the status of the machine tool that performs the machining.

In the context of the 4th industrial revolution, these information items become the sources of new value creation while involving synergistic effects with the information generated from other systems beyond the prime objectives, which are the improvement of accuracy and efficiency of the machining process. That is why the term indicating a discontinuous change, "revolution", is used. For instance, from a perspective of management of a supply chain from order receiving to product shipment, the information presents the machining process progress status as well as the operating status of the related facility such as machine tools, leading to the global optimization of the production plan. From a perspective of management of daily operation of a machine tool and so on, the information can be used for the identification of the health of machine tools and for the basis of predicting failure occurrence. Furthermore, a machine tool manufacturer may be able to accumulate the information about the machine tool operations in various utilization conditions in a long term, which can be used and analyzed. As a result, the machine tool manufacturer will be able to use the information for design and development of machine tools with higher performance as well as for refinement of the operational expertise to exert the functions to the maximum capability. With use of such operational expertise effectively, the manufacturer can develop a service business that supports the improvement of accuracy and efficiency of the machining process. Eventually, a

smart machining process will be able to create new industries, not to mention the increase of competitiveness of the existing industry.

In this way, the revolutionary change mentioned today provides opportunities for acquiring new added values not only for manufacturers regarded as users of industrial machineries, but also for manufacturers of industrial machineries. In particular, in the movement called a new industrial revolution, the cases where information technology is provided through open source are becoming tangible and utilization of information technology that is developing remarkably is essential for securing competitiveness. However, the obstacle for implementation of the service that adds high values by utilizing the information technology cannot be easily overcome. This is because linkage and integration, which have not been contemplated, but rather have been avoided, are necessary. Typical obstacles are vague uneasiness towards the unexpected risks associated with linkage and integration, with which the operators have no experience, concerns towards the risks associated with information leakage and security attacks that will inevitably increase as a result of linkage and integration, technical issues (interfaces, protocol, and so on) of the information system for which linkage and integration have not been assumed originally.

A promising approach for achieving significant results through the revolutionary change by overcoming these obstacles is to find specific examples of smart manufacturing that can create an added value substantially enough to overcome the difficult obstacles, share the smart manufacturing among the stakeholders, and acquire the methodology for overcoming the obstacles through the implementation.

Smart manufacturing has the following three features.

Firstly, it has the mechanism that centrally manages and integrates production engineering data of the machines in the factory, processes the data that is obtained as a result, and provides the data to upper level systems such as ERP and MES, on the production management side, as the data useful for improvements of machining efficiency of the machines, predictive maintenance, and “Kaizen” (on-site improvement activities).

Secondly, it has the mechanism that enables optimization of the entire production line without human interventions beyond the conventional approach of accumulating partial optimizations performed manually in each process, by

feeding back to the machines the production engineering data that has been digitally processed.

Thirdly, it has the mechanism that enables the visualization of the entire structure of the engineering chain, which is production engineering, and the supply chain (production control), which is production management, management in an integrated manner by utilizing AI technologies if necessary, capture the site as the cyber-physical system, and consequently, achieve improvements that lead to the global optimization.

The linkage and integration, which are the essence of smart manufacturing, require collaboration among multiple different entities under the commands of the conductor that performs the total optimization. On the other hand, a new value that is created through collaboration is spread to many stakeholders over a wide range, not attributed to specific players only. The important factors for creating such a structure as this and realizing the win-win relationship are that implementation of smart manufacturing is presented in the form that can be shared by a wide range of stakeholders, the merits, risks, and risk management techniques are correctly understood, and wide range of entities can participate. Above all else, it is important for operators that use smart manufacturing to prove to the customers their abilities to provide the solutions such as the best products and services and that many stakeholders enjoy the profits.

"Series: Toward Realization of Smart Manufacturing Systems" is the message to the world from the practitioners at the front line in Japan, who declare as the leaders of the revolution and share and implement such a concept as this.

2. Improvement of the machining process productivity based on the machine tool technology

As the primary approach to the realization of smart manufacturing, improvement of the machining process productivity is focused on and examined.

In a sense where advancement of the manufacturing industry has been realized by mechanization in production processes, industry machine manufacturers made a significant contribution to the evolution of the manufacturing industry. In the emerging countries that are aiming at adding high values to the manufacturing industry, movements for adding high values will spread in the future by installing advanced industry machines as has been done by developed

countries.

Among the production processes, in a machining process in particular, there are significant differences depending on the operating skill levels of machine tools and the productivity and added values are influenced greatly by the comprehensive expertise including setup and maintenance inspection. Therefore, there is an ample scope for machine tool manufacturers to make contributions. That is, a new market is available for machine tool manufacturers as "manufacturing service providers" that provide the effective utilization expertise of machine tools as well as supplying them.

Accordingly, this document summarizes and presents the use cases toward realization of smart manufacturing by specifying concrete services that improves the productivity of a machining process through the capitalization of the latest technologies such as IoT and AI as the precondition.

3. Examination method

An examination team was organized (see page 46) by the practitioners mainly including the users and manufacturers of the machine tool. The examination was carried out in the following procedure as the implementation that conforms to the actual businesses.

[1] Based on the customer needs relating to machining processes, team members documented the summary of the specific details of the services addressed as the implementation of smart manufacturing. After that the target service contents were specified by the team.

[2] The service that was specified in [1] was described as the information model (in this examination, SysML of OMG is used) as a common method to enable the team members to mutually compare their services implemented or examined for this implementation.

[3] Through the comparative analysis of the information models based on the examined service contents provided by the team members, the team members extract common items, which construct the basic (general) structure of the service.

[4] The forms of linkage and integration with other systems, which are necessary for implementation of the service, were verified based on the information model that was specified in [3] and the items that are to be

regulated into rules such as the items to be standardized including interfaces, security, and data control entities were specified and summarized.

4 Overview of the target services and the issues

(1) Remote maintenance service, predictive maintenance service, and production management service

To improve the productivity of machining processes, it is necessary to minimize the reduction in the operating rate caused by troubles as well as promote multitasking of machine tools to minimize work transfers and setup changes (e.g., increase of the number of controlled axes and number of machine tools used).

Of these objectives, each machine tool manufacturer has focused on the latter objective since around 2000 and has been providing services such as checking and monitoring the operating status from the service base of the manufacturer by connecting the machine tool to the network.

As the typical services such as predictive maintenance and maintenance that are provided mainly to large manufacturers, the machine tool used by the user is connected to the service base of the manufacturer via the mobile phone network or the Internet. The manufacturer collects the operating status of the machine tool at that time and past log information in remote mode. Based on the collected information, the manufacturer repairs the tool in remote mode or gives advices to the user. In comparison with the method where the manufacturer visits the site for verification of the condition from the service base after receiving the information from user, the cause of the trouble can be identified and measures can be taken more quickly. In addition, by utilizing various types of data relating to the behaviors of the machine tools that have been accumulated by the manufacturer, signs of troubles can be predicted and predictive measures can be taken. In this way, more refined measures can be taken. As a result, the user can reduce the downtime of the machining process (standalone machine) and improve the productivity.

In addition, the operating status of machine tools can be stored digitally as

data, enabling accumulation and analysis and, beyond the scope of troubleshooting, operating skills can be checked. . Manufacturers can extend the services to operation support to users, transforming the service to a high value added machining process.

If the data relating to the operating status of machine tools has been collected and organized to the degree that enables the checking in remote mode, the data can also be used for production management of the entire factory, and management and optimization of the supply chains.

The service for the productivity improvement for machining process as described above is summarized as the predictive maintenance/maintenance/operation support service in remote mode.

A variety of forms can be assumed for the procedures of the predictive maintenance service, maintenance service, and operation support service.

For instance, the following methods can be considered for the operating status monitoring mode: method that acquires various types of sensing data on the operating status in remote mode at the frequency close to real time, method that automatically acquires only the signals on the occurrence of fixed events such as abnormal termination, which require countermeasures in remote mode, method that automatically acquires, in remote mode, log information of related sensing data together with the event at its occurrence, and method where the manufacturer searches and acquires the necessary data in remote mode at the occurrence of an event.

The following maintenance methods are assumed: method where the user performs maintenance of the machine tool at the installed site, method where the manufacturer directly takes the necessary measure in remote mode via the Internet if the measure is possible within the range of general operation procedure or parameters, and method where a fix program is created in remote mode and the system version is upgraded by sending the program to solve the trouble at a program level.

In mere combinations of monitoring of operating status and possible maintenance procedures, a substantial variety of the combinations can be assumed. While the discussions subsuming such a variety of service forms as these are intended, there is still an issue regarding significant

differences depending on the service form such as information security measures. Therefore, for the design of maintenance procedure, discussions will be carried out based on the principle under which the user implements maintenance at the site where the machine tool is installed. Such a method as this is applied according to the maintenance procedure currently requested by the user. Since more diverse forms will become available as the market expands in the future, other forms will not be eliminated from the examination targets and will be handled as future issues to be examined.

(2) Issues faced on the spread of the target services

Although each machine tool manufacturer provides a part of the service that was described in (1), the service is not necessarily widely accepted by users. This means a loss of useful opportunities not only for the manufacturers intending to provide the service, but also the users who will be able to enhance the machining processes by using the new service.

The following main issues are assumed if the service becomes widespread..

[1] Apprehension towards the risks attributed to network connection

Many users assume serious risks due to the connection of their information systems such as machine tools that are used by machining processes with the network that connects internally and externally. Such risks can be long-term suspension of the production lines caused by malicious hackers or computer virus infection and malfunctions causing fatal accidents. The data relating to the operating status of machine tools about machining processes are considered highly confidential as such data directly indicates the performance of the machining processes. Possibilities of serious economic loss caused by information leakage are often apprehended.

Information network technology is the largest technological factor that leads to the 4th industrial revolution. Thus, proper management of network connection is necessary considering the aforementioned risks due to the network connection as the precondition. Due to the lack of the understanding of the service structure based on the network connection as

the precondition and the absence of the sharing of a definite view on the risk management techniques, many users seem to hesitate to utilize the service that capitalizes IoT. The handling of information security that removes the uneasiness of users is necessary.

[2] Difficulty in providing the service through the machines of different manufacturers

In general, machines of multiple manufacturers are installed in users' production sites (production lines). To take the full advantages of the service based on the network connection as the precondition, it is desirable to be able to collectively check the behaviors of machine tools of various manufacturers that configure the production line. Even if the maintenance service or predictive maintenance service can be provided by each manufacturer individually, there is a limit to the effects of optimization of the entire factory if there are significant differences among the service contents and the measures for risk management as indicated in [1], and as a result, the merits to users become low.

Currently, no linkage structure is available for manufacturers to collectively implement the service in a unified manner. For the realization of such a structure, it is necessary to define the coordination area among the manufacturers such as the quality and volume of data, data linkage frequency, grading, and communication protocol.

[3] Difficulty in service deployment based on the data accumulation and analysis

Currently, each manufacturer provides their service within the scope requested by the user for solving troubles such as troubleshooting for a standalone machine tool and so on by intermittently obtaining data relating to the operating status or log data. As outlined in (1), one of the services assumed for realization of smart manufacturing systems is the operation support for further enhancement of machining process of users by studying more data in more detail regarding the behaviors of the machines that run at the users' sites.

To materialize such a service, it is necessary to organize the concept of

data such as the agreement on the utilization range of the data relating to machine tools and organization of responsibilities for data accumulation and management to enable the stakeholders to collaborate widely under the common recognition. However, such details have not been organized.

[4] Uncertainty of service merits in return on investment

It is difficult for the manager (user) to predict the effects that lead to the investment judgment such as other actual services enabled by the introduction of the service and the effects of these enabled services. Thus, it is necessary to provide the materials as the guidelines for the management decision-making process and clearly promote the service that can be effectively utilized. In addition, through the implementation of smart manufacturing, creation and proposal of effective services are necessary.

[5] Shortage of engineers for network and security

Up to now, systems such as machine tools and robots have been integrated by machine tool manufacturers and line builders. In the implementation of smart manufacturing, system integration including IT equipment and network is necessary as well. However, the shortage of engineers for network and security in the machine tool manufacturers makes it difficult to provide technical advice to enhance the understanding of the service to the users and remove the uneasiness relating to security at the proposal of a solution. It is necessary to train engineers for network and security and create a guideline for clearly explaining the service to the users by describing the form of the system linkage and specifying the sections for which rules are to be established.

The common points on the issues that were described in 4. (2) can be summarized as the absence of the common recognition regarding the basic characteristics of the service that utilizes network and data and the absence of rules specific to the service. As the preconditions of actions to verify and solve these issues, a service information model is presented as described in 5. (1). Based on the information model, verification of the form of linkage and integration with other systems, sections that are to be standardized such as interfaces, and sections for which rules are to be

established such as security and data control entities are to be identified and organized.

5. Information modeling associated with remote maintenance service, predictive maintenance service, and production management service

(1) Organization of information modeling for machine tools

The function for monitoring the states ”Mieruka(visualization)" of the machine tools that form the production line is an valuable factor to apply remote maintenance and predictive maintenance services. In particular, to realize ”Mieruka" of various machine tools manufactured by different providers with same manner, it is important to clarify their hardware configurations and internal statuses and to be prepare for information models for designing and implementing the information system of productive activities. Machine tools that configure the current production lines vary in the structures and dynamic behaviors according to the machining spindles and number of pivots of the machining table, installation location, and the drive mode of each axis. These differences make it difficult to define a common model that indicates all the functions. Even if a common model for the current machine tools is defined and machine tools are designed and manufactured based on the model, it means that a model is determined for machine tools corresponding to the future manufacturing of all the products, impairing the development of machine tools.

However, for the users of a production line with multiple machine tools, "Mieruka" of the entire production line at the uniform level is also important in terms of production management. Therefore, we attempt to create models that enable the recognition of the hardware configurations and machine operating status of the target machine tools at a uniform level. In this project, models were created in terms of the block definition diagram (static structure) and the state machine diagram (dynamic structure) of an NC cutting machine based on the information collected from machine tool manufacturers.

[Block definition diagram of an NC cutting machine]

Hardware configurations of NC cutting machines vary depending on the degree of operation freedom of the machining equipment and the number of tool units. The basic configuration comprises the "CNC unit (referred to as "NC" in the diagram) that controls the machining equipment, the “PLC unit” (referred to as “PLC” in the diagram) that controls the sensors and the auxiliary tool units, the "industrial PC (referred to as "IPC" in the diagram)" that functions as the user interface and the network interface with the office floor, and the "machining unit" (referred to as “Motor” and “Cutting tool unit” in the diagram). The block definition diagram in Figure 5.1 shows the relationship among these components.

When sensor information within the NC cutting machine is distributed to the Internet (EtherNet), the information is transmitted to the Internet by using the industrial PC that functions as the gateway of the information and the bus-connected PLC unit as the source of the information. The other devices of the production line that are connected to the field network (FA-Net) are controlled via the PLC unit only. Regarding the common issues such as the securement of operation safety of the production line, the model help to examine the problem such as how the information system that distributes information to the Internet and the control system that controls the production line can co-exist without any problem. Such modeling also clarifies the control information at operation of each machine tool that forms the production line, design information, the sections that handle sensor information, and the connection relationship/access range. This is effective for identification of failure factors at the occurrence of machine failures, impact relationship with other machines, and designing of the information system that handles the relationship between various types of information and the interfaces.

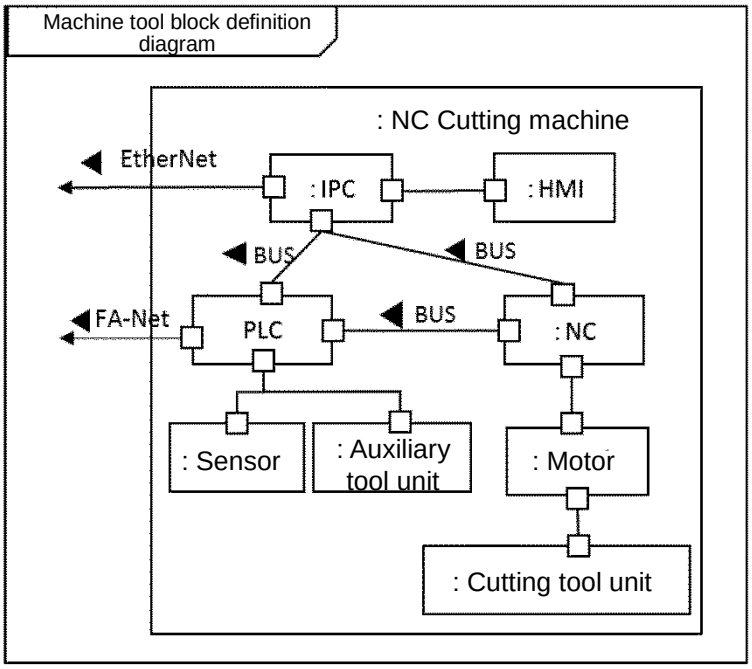

Figure 5.1 Block definition diagram of an NC cutting machine

[State machine diagram at normal operation of an NC cutting machine]

By using the block definition diagram of an NC cutting machine showing in Figure 5.1, the relationship among the internal units of the NC cutting machine, various functions, and information that is handled can be described. However, since the information generation at NC cutting machine operation and the flow are not described, the information is not sufficient for developing an information system for "Mieruka" of the statuses of NC cutting machines. Therefore, we modeled an inside state transition of an NC cutting machine at normal operation as the state machine diagram.

For the state machine diagram at NC cutting machine operation also, the details vary depending on the functions of each machine and configuration of internal units in the same way as the block definition diagram that is described above. As a result of the information collected from the manufacturers, the common state machine diagram can be presented as shown in Figure 5.2.

The status transition indicated here refers to the flow of operation and the timing of status transition when an NC cutting machine is operated in a

factory.

An NC cutting machine often has multiple machining preparation states for prevention of accidents during machining operation, requested accuracy of products (machining targets), and preparation of peripheral devices and auxiliary devices of the working machines. To realize "Mieruka" of production at the factory configured by multiple machine tools, production line, and production cell, design and installation of an information system at the level that commands the entire operation are necessary. Modeling of common sections as this are effective for its realization. If detailed models (individual models) corresponding to individual machine tools can be provided by the manufacturers, an information system capable of "Mieruka" of various levels can be easily designed and installed by combining common model and individual models. By presenting the operation of each working machine as a common model, an important guiding principle can be made available for standardization of manufacturer’s specific ID that indicates warning information and failure information.

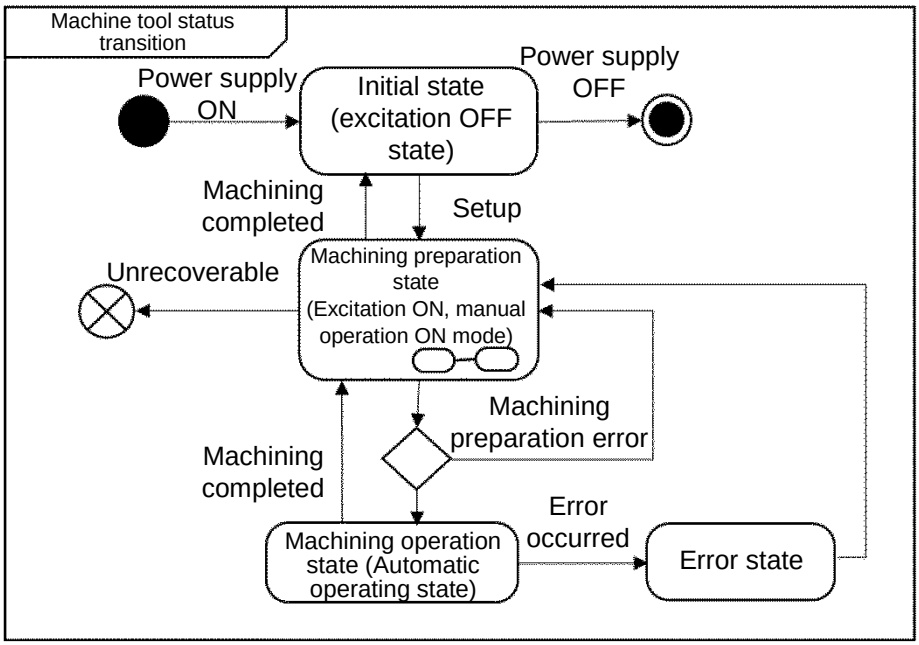

Figure 5.2 State machine diagram at NC cutting machine operation

(2) Organization of information modeling for the target services

[1] Modeling maintenance service

Important points for realization of high-efficiency production activities by enhancing the existing production technology by introducing IoT for machine tools are minimization of down time due to various failures in the existing production line and elimination of waste such as occurrence of manufacturing defects. Efficiency improvement and enhancement of maintenance work of machine tools that comprise the production line are one of the important techniques for the elimination of waste.

Currently, in many factories, maintenance work of production lines is carried out in various methods. However, most of the "Kaizen" of maintenance work are individually handled based on the tacit knowledge of the operators (production engineers of the factory and site administrators). "Kaizen" of production activities through individual handling based on the tacit knowledge as the core will soon reach the limit due to the bottleneck attributed to human resources. It is difficult to utilize advanced systems and technologies such as machine tools equipped with IoT technologies, various information system, and AI technologies.

For the maintenance work in the current production sites to overcome such limit and continue to evolve by introducing IoT and AI, the conditions that require human intervention for various maintenance work must be changed. Initially, it is important to clarify a current maintenance work by modeling. Therefore, modeling of maintenance work at the current production sites was attempted by collecting information from machine tool manufacturers and users of production lines.

Figure 5.3 shows the block definition diagram relating to maintenance work. This model shows that there are delay of dissemination, underdevelopment of the technologies, and ambiguous relationship between maintenance work and workers (persons in charge in users and manufacturers) in remote/preventative maintenance.

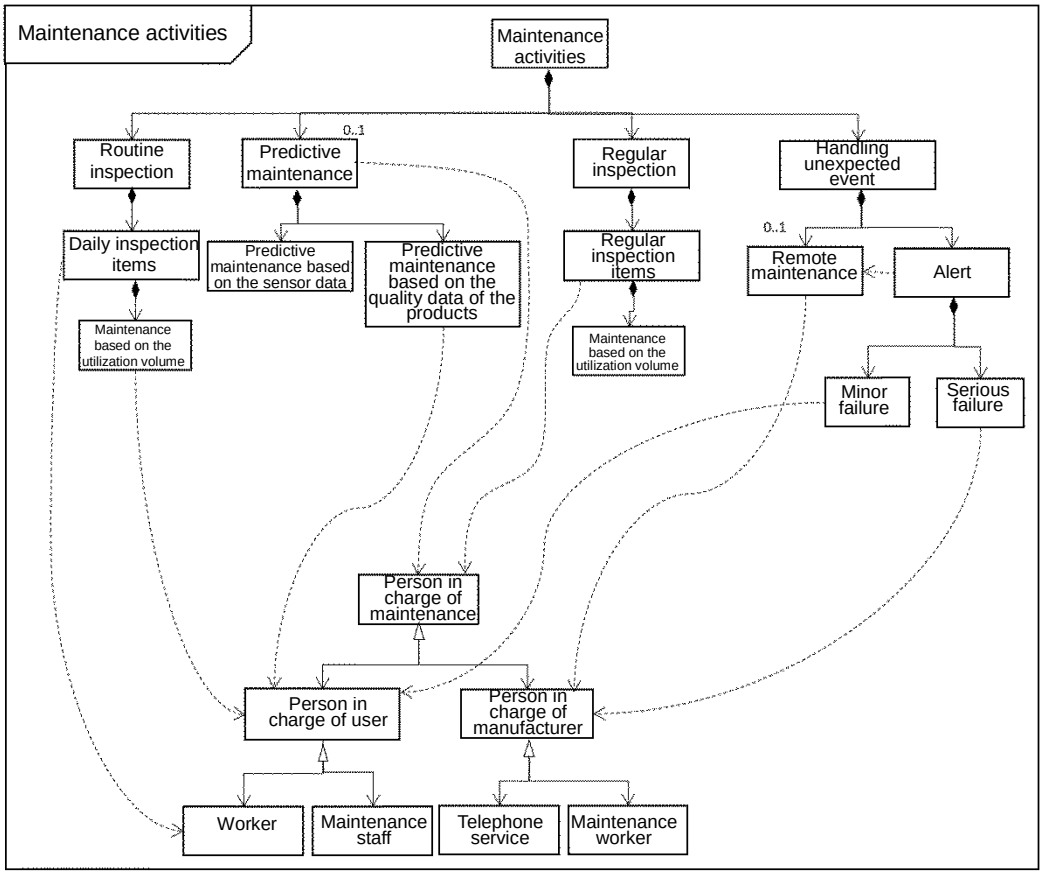

Figure 5.3 Block definition diagram of maintenance work at current factories

Maintenance priority items in the current production line vary depending on the product and production system. For instance, in case of single breed mass production/small lot production of many products in 24-hour system such as factories in the automobile industry, it is most important for maintenance work to realize of the zero downtime maintenance. On the contrary, in the make-to-order mode that is applied in production lines of infrastructure facilities as units that form a large power generation system, maintenance work is performed to prevent a failure of machine tools or product failure during the production period. Most of the factories in large companies have the sections that can implement most maintenance and repair without the need for the support of each manufacturer regardless of the particular machine as long as the machine tool forms the production line. On the other hand, small to medium companies cannot afford to have such sections.

In creating the information model, we believe that it is necessary to classify into two viewpoints, "viewpoint on the presence/absence of the section of maintenance work" and "viewpoint of the production system (mass production, small lot production of many products, and make-to-order production)". In addition, we need to create individual models and analyze the requirements while noting the clear indication of the contents of maintenance work and functions that require human interventions.

[2] Modeling remote maintenance and predictive maintenance services

While referencing the information models that indicate the current maintenance work as described above in [1], we attempt to model both remote and predictive maintenance systems that are currently realized by related companies.

[Remote maintenance system]

Currently, Internet connection via cabled or wireless LAN is seldom introduced in factories due to the reason of inadequate information security measures. Therefore, for most of the machine tools that support remote maintenance, the maintenance service is implemented by using the public line network through the mobile phone network dedicated to data communication. Figure 5.4 shows the typical block definition diagram of the remote maintenance system that is currently implemented by machine tool manufacturers.

Since there are problems in terms of the capacity restriction and communication cost of communication lines under the current remote maintenance service, data monitoring in real time through constant connection is difficult. Therefore, information on the operation time in the machining process by machine tools and information obtained from internal sensors are stored in the storage unit that is installed inside of the machine tools such as hard disks and the data is regularly uploaded to the database that is managed by the manufacturer. Normally, when an alarm is issued due to the occurrence of a fault, relating information such as the alarm type is automatically transmitted to the manufacturer and the manufacturer

performs the initial analysis of the faulty section corresponding to the alarm by using the data such as the operation history that is uploaded regularly.

In this case, the data such as operation history that has been accumulated in the server regularly is often used only for the initial analysis of the faulty section at the occurrence of an alarm. This is because information such as machine tool operation history is the production engineering expertise itself for users as mentioned in 4.(2). This hinders the deployment of services of machine tool manufacturers, where "a large volume of data is collected from various users, and is analyzed and high-value added remote services are developed by using the analysis results". However, in fact, the operation data that is accumulated handles the movements of machine tools only as has been clarified by this modeling and it is impossible to restore the entire machining process by the data only. Even if the data acquired for remote maintenance is leaked, the risk for the leakage to cause the flow-out of the production technology of the user is low.

The modeling of the system is effective for clarifying the sections where faults are likely to occur by a new service as remote maintenance. It is also effective for assessing the risks by the introduction of a new technology. Therefore, in popularization of IoT equipment and improvement of the Internet environment within factories in the future, the model of remote maintenance system can be useful to realize a service expansion with adequate security measures by updating it with the change of the configuration.

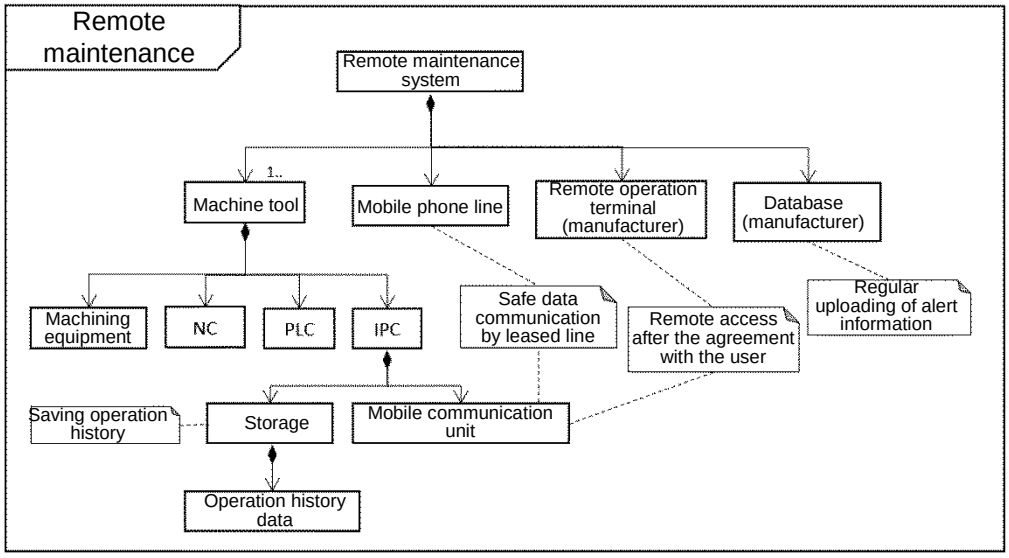

Figure 5.4 Block definition diagram of the remote maintenance system

[Predictive maintenance system]

Predictive maintenance can be said that it is conservation activities to achieve efficient operation of the production line by predicting failures of the machine tools configured the production line by using various information of their inside or outside sensors. Under the present condition, the technology for measuring the correlation between the sensor data associated with such predictive maintenance and defects is being developed and the predictive maintenance service for machine tools is restricted to the limited function units only. In this section, modeling was implemented as the block definition diagram of the system configuration (Figure 5.5) relating to the predictive maintenance system that is currently tackled by each manufacturer by assuming multiple machine tools based on the results of interviews.

Figure 5.5 shows the configuration of the predictive maintenance system in the production line configured by multiple machine tools. This model is based on the factory where conditions surrounding the production line can be measured by external environment sensors and so on. Regarding predictive maintenance, more accurate signs can be detected by using the data on the environment where machine tools are used, as well as sensors of stand-alone machine tools. For foretaste detection, machine tool installation locations and data that indicates shapes and materials of metals may be useful and the data accumulated relating to production lines including such data can be used as the user-specific production technology or expertise. Therefore, when compared with remote maintenance, a system must be configured considering the risks of information security. In the model that is shown in this document, the use of the database of the production site and the cloud system is assumed. Classification and ranking of the types of the information to be uploaded to the cloud system is found to be effective in information security risk assessment.

For the predictive maintenance system also, the service provider and the user can have common recognition more easily through the prior deliberations on the risks and the countermeasures for the service that is to be created in the future by modeling the entire factory including the external systems,

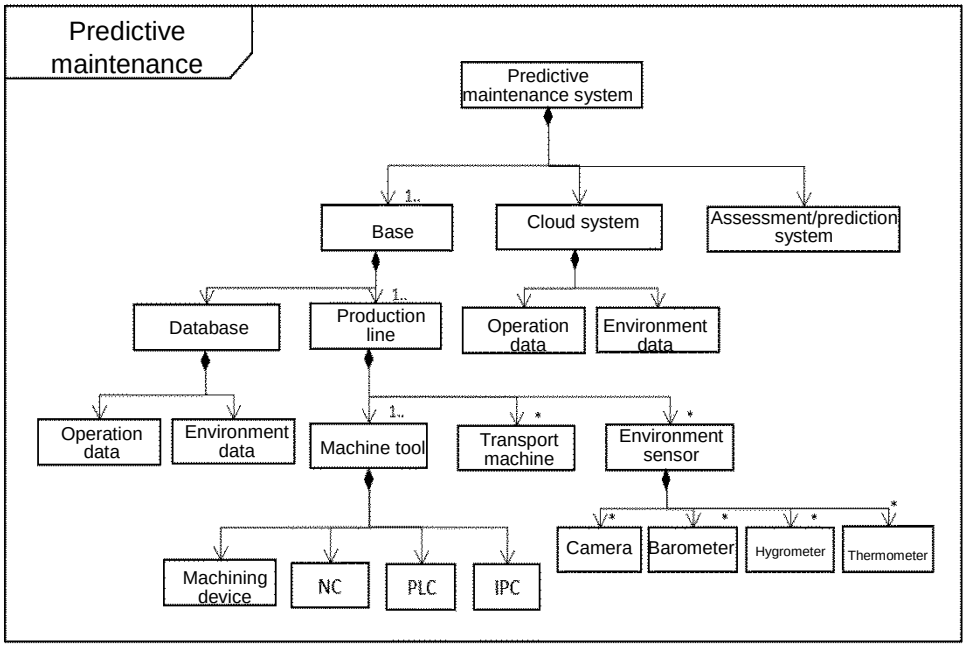

Figure 5.5 Block definition diagram of a predictive maintenance system

6. Draft of the guidelines for the deployment of the target services extracted from the information model

(1) The guidelines/interfaces relating to the definitions of the basic states of machine tools and methods for extracting information on the states

The machine tool information model has been discussed in Section 5. (1) [1]. The state machine diagram of Figure 5.2 presents the sufficient state definitions for comprehensively checking the operation status of the production line or the entire factory for the user that operates the production line, detecting any defects of the production line, and implementing maintenance activities. As the basic states of machine tools, the following four states can be defined.

[1] Initial state

The machine tool is set to this state immediately after the power is turned on and before the machine is stopped safely after termination of machining. Since termination of the power supply due to an error or some other defect may cause some fault in the machine tool, the machine tool must be returned to this state for normal termination of the power supply.

[2] Machining preparation state

The machine tool is set to the machining preparation state to shift to the machining operation state and this state can be subdivided to multiple states such as the warmup state at machine tool replacement for maintaining machining precision and preparation state for automated setup. The machine is to return to this state at the returning to the normal state from the error state that is set due to the alarm that is occurred during the machining operation. When the machine cannot be returned to the normal state (machining enabled state) from this state, the machine is to be stopped as an unrecoverable error and is to be set to the mode that requires maintenance.

[3] Machining operation state

In this state, the machine is processing a work after normal completion of setup and the machine is set to this state from the machining preparation state. When an alarm is occurred during machine tool operation, the machine is set to an error state.

[4] Error state

The machine is set to this state from the machine operation state when a warning or fault alarm is occurred during machine operation. To return the machine to the power supply disconnected state or machining state, the machine must be set to the machining preparation state.

Since these basic states of machine tools are defined for improving the efficiency of production management through "Mieruka" of the operating state of the entire factory or the production line, the states need to be notified to the information system that performs production management via the internal IPC. Currently the information acquisition specifications in the NC and PLC that form a machine tool vary according to the manufacturer. Therefore, to acquire the information on the state of a machine tool, IPC acquires the state of the machine in the production line through the interface (API: Application Programing Interface) according to the manufacturer of the NC and PLC and the external information system acquires the information of the state of each machine through IPC. Since a specific interface is defined for each machine tool manufacturer and the production line control system must be constructed according to the interface, it may be necessary to reinstall the production line control system whenever the production facility is updated.

To realize a "smart factory" for the total optimization of the supply chains and engineering chains, and construction of an efficient platform and improvements of production efficiencies of various machine tools, the necessary information should be able to be acquired by applying the open platform technology as much as possible to reduce the adjustment costs associated with differences among the manufacturers.

Based on such a concept as this, standardization is planned for the

following two interfaces for the acquisition of machine tool states and other information.

[Interface among NC, PLC, and IPC]

In the conventional method, API specific to the manufacturer is used for acquiring information from NC and PLC that control the jigs of machine tools and peripheral auxiliary tool units. This causes an extra development load to the manufacturer of the machine tools and consequently, less convenient for the users of machine tools. Therefore, an open standard specification is applied in principle for acquisition of the information that satisfy the configuration that is expressed in the shared model. Specifically, an interface that complies with the MT-Connect Standard, which is becoming a de facto standard or the Dejure Standard such as ORiN is recommended.

[Interface between IPC and an external information system]

The target of control for machine tool users is the production line, not individual machine tools. The approach for improving the production efficiency by monitoring the operating state of the production line from the office or an external base is developing. Therefore, the interface for linking the information system that completely grasps the state of the production line including the behaviors of individual machine tools with the external information system that performs production control is important. Currently, installation of API specific to each manufacturer is necessary, requiring major reconstruction whenever the facility is updated. To avoid such a load, the use of the common interface including the linkage function section with MES and ERP is recommended. For the common interface, middleware that complies with the international standard such as ISO20242 can be assumed as the future global open strategy.

(2) Basic concept relating to information security measures at connection of machine tools with the Internet

- Technical background

  For a long time, manufacturers have assumed that devices in the factory are to be connected to a closed-area network that does not involve in any way with external networks such as the Internet. Consequently, many factory devices available today became significantly “insecure” when compared to the devices used in the other field, and many security vulnerabilities of PLC and other factory devices are reported publicly. Further worse, today’s closed-area network is not really “closed” in practice; there is so many possible intrusion paths available for security attackers, and is becoming a major risks to the real systems. Many real successful invasions are reported, such as destruction of factory equipment and loss of control/explosion in factories. Under these circumstances, there seems to be great difficulty of applying the concepts on IoT and big-data application via Internet to the current factory-area network.

  In the area of control systems (such as critical infrastructure systems), separation between the control system network and information system network/external Internet using multi-level firewall configurations has already been exercised (Figure 6.1). In these configurations, the machines connected to (or “bridges between”) two or more network is the critical point of the network security. We cannot avoid such machines to exist, since information distribution is necessary among the different layers in such configurations. In addition, from the view point of security, commonly-used USB storage media used for the distribution of information such as design data from the information network to the control network, can also be regarded as "devices that are connected to two or more networks" in a broad sense. When a malware (computer virus) infects a device connecting two or more networks, it can infect into the control network and the many insecure devices in the control network (including PCs without proper security updates applied) fall into a serious condition (Figure 6.2).

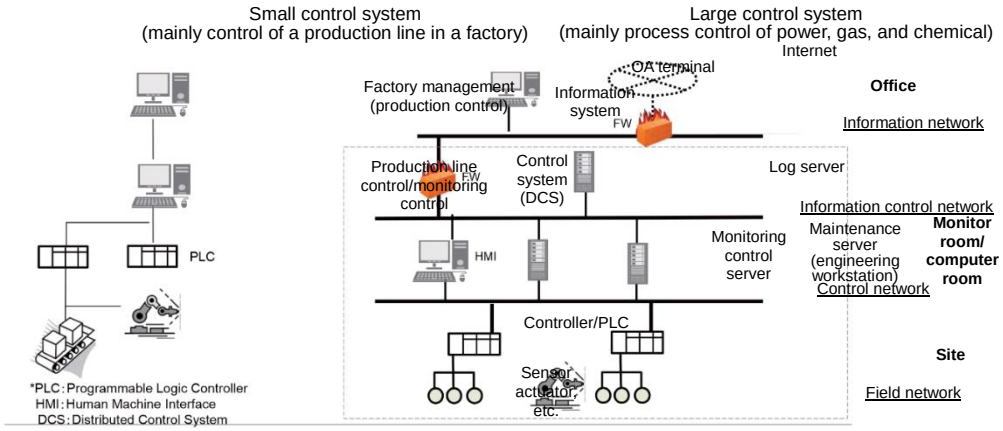

Figure 6.1 Example of conceptual configuraiton of the control system including factories

(Source: page 15, "Security risk of control systems as a serious management issue", by Information-tecnology Promotion Agency Japan; translated by authors)

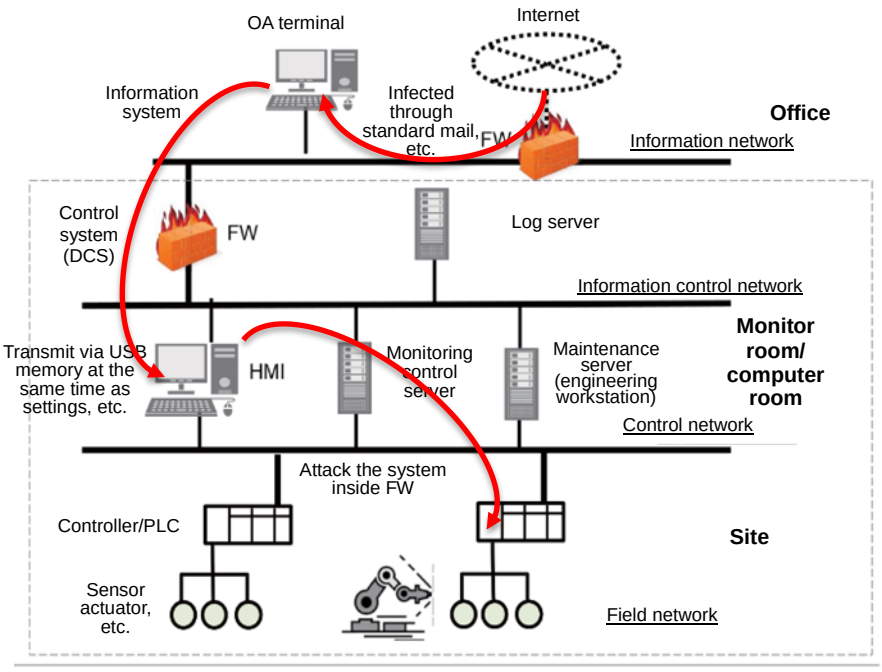

Figure 6.2 Example of the route of malware infection bypassing the firewall

(Source: the same as Figure 6.1, with alternation by authors)

On the other hand, many manufacturers are providing an optional communication module that connects a machine in the factory to the manufacturers' network directly, through an externally provided network services (such as 3G/4G mobile phone networks) (Figure 6.3). The possible reasons for using such a "bypassing" feature are twofold: for small-scale users it is not always realistic to prepare a network environment specifically to applications for the 4th industrial revolution; for larger entities, it is not practical to reconfigure the already-existing closed-area control network to allow external communications for remote maintenance purpose. Such connection becomes more and more practical under the current trend of low-cost wireless communication environment. From the viewpoint of the network security, only if such external connection is the only connection to the machine (and when the manufacturer is absolutely trusted), it is a practical solution. However, if a local-area IP network is existing, or it is to be installed in the near future, the solution is quite unacceptable, because all of such devices will become "the machine connected to two or more networks" as described above (Figure 6.4), causing a vulnerable situation. In particular, the presence of multiple external connections under differently administrations is a serious situation for network management and operation. If devices inevitably need to accommodate both the in-house and external connections, such connections must be completely controlled by the firewall managed by the factory and an unnecessary increase of the number of connection points must be strictly avoided.

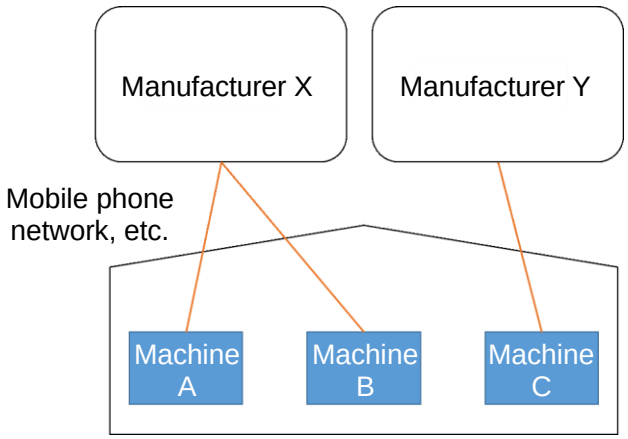

Figure 6.3 Direct connection via the mobile phone network, etc.

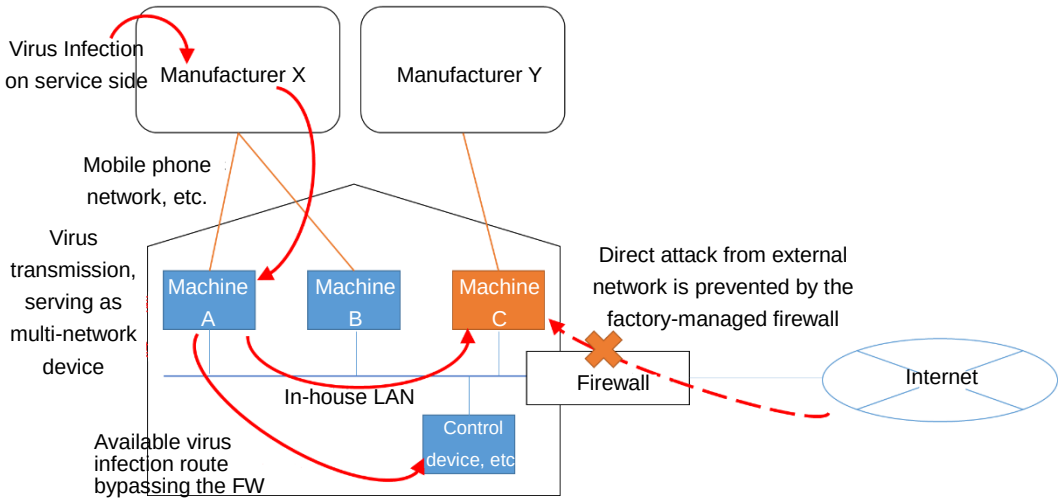

Figure 6.4: Risk of possible virus intrusion caused by the dual connection of the mobile phone network and in-house LAN

Considering the perspective and the current situation indicated above, for the time being, we propose that the security model for the remote maintenance services for industrial machineries shall be examined as two separate use cases: whether in-factory inter-device communication is required or not.

As the first case, if in-house inter-device communication is *not required*, we can consider the use of the direct logical connection of machines to the network on the manufacturer side by using dedicated connection such as a mobile phone network. In this case, such machines should be considered as belonging to the manufacturer's network in terms of the information security, regardless of the actual ownership and the installation location. We show the two example configurations of the use case, "standalone device connection case," and "simple connection configuration case using VPN."

In contrast, if inter-device communication within in-house LAN is *required*, we propose that we should focus and invest to the design and construction of the properly managed, externally connected in-house network, including the development of required technologies. We summarizes this use case as an "in-house LAN case" and examines some specific requirements for security measures.

In any case, security protection of devices is considered strictly essential today, even in the closed and stand-alone environments. The security measures independent of the connection figuration will be summarized separately as the information management system.

- Examples of use cases

[Standalone device connection case]

This use case involves direct connection of in-factory devices to the manufacturer's network using external network services (such as 3G/4G mobile phone network). The case assumes that 1) there is no in-house information exchange with other systems through LAN, USB storage device etc., and 2) security violation risks from the manufacturer's side can be ignored (the factory side decides to trust the security management of the manufacturer). In this case, the machine connected to the manufacturer system must be considered as belonging to the manufacturer's network. Factory-side users should verify the following points as security assessment.

[1] The machine that is connected to the manufacturer's system must not be connected to the in-house LAN in principle (Figure 6.4).
[2] When any data is exchanged between the machine and the factory-side computer system using a USB storage etc., such a carrier device must be considered as one outside of the factory environment. For example, virus checking should be performed each time it is used.

In addition, it is important to verify that the connection network (communication network service) satisfies the following criteria.

(a) The connection network must be isolated from the Internet.
(b) The manufacturer-side systems that accommodate the connection network must either disconnected from the Internet, or have its security strictly managed and protected as if it were the critical factory-side infrastructure.
(c) If either the connection network or the manufacturer-side network accommodates multiple devices, direct communication between

devices should be isolated; at least, devices from different factories or different sections/lines must not be able to communicate to each other.

(d) The devices from different factories must be network-separated on the logical link layer (Layer 2) or below. If necessary, a virtual network (VLAN) must be used.

(e) The communication network should provide protection against tampering/eavesdropping of the traffic. If such function is not provided as a network service, alternatively, the device manufacturer must implement the encryption and mutual authentication between the device and system, using the widely accepted standard technologies.

The use of the “public network” services without the dedicated communication control/separation functionality is not recommended within this use case. If such connection is to be used, we recommend to consider the network connection as the public Internet, and to take adequate security measures as provided in the “simple connection use case using VPN” below.

[Simple connection case using VPN]

If in-house LAN is to be used as a communication channel to the manufacturer’s network, but the full-brown control system network (as shown in Figure 6.1) has not been deployed, we may consider some simplified configuration. This use case requires slightly more management cost compared to the previous use case, and it still does not support inter-device linkage within the factory well. However, it can be considered, for today’s small-scale deployments, as an intermediate, transitional step to the future full-scale controlled environment supporting full use cases.

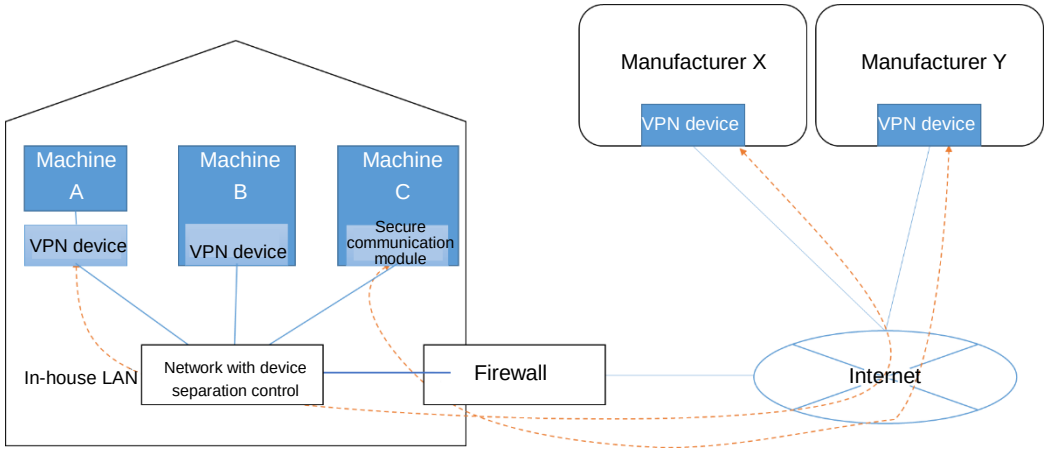

Figure 6.5 Communication control by combination of VPN and communication control switch

In detail, this case uses the virtual private network (VPN) functionality to realize the functionality of the dedicated network on the Internet (Figure 6.5). In terms of security, it does not rely on the security of the in-house network compared to the Internet, still it provides virtually the same level of security to individual devices, compared to the previous “dedicated network” case. However, since the VPN device is itself a high-risk device due to its vulnerability caused from complex functionality, cautions are necessary. To mitigate this risk, we propose to introduce additional security control to the network level in this use case.

In detail, this use case requires the same cautions and provisions as the “standalone device connection case” above. In addition to that, the following settings are deployed on VPN devices and network equipment.

(a) In VPN devices on both ends, the whole traffic from the internal side is transferred to the virtual network and not to the in-house LAN. (Cautions are required when generic-purpose VPN devices are used, because the VPN client devices usually forward general traffic to the in-house LAN by default). All incoming traffic from in-house LAN are discarded (except the traffic for the VPN communication itself).
(b) Strict management is required for mutual authentication and encryptions of VPN devices.
(c) The manufacturer (possibly with other third-parties), should provide

up-to-date management on the vulnerabilities of VPN devices and others.

(d) Network switches should be configured so that only the communication between each VPN device and the external firewall is permitted. Direct communication between devices is discarded by default (Figure 6.6).

(e) Firewall is configure to allow the outbound communication from the in-house LAN to the Internet only, and incoming communication from the Internet is discarded (technically, except the responses to the outgoing communication) (Figure 6.6). This means that VPN connection is to be established from the factory side. If possible, configurations will only allow individual communications from the in-house VPN devices to the manufacturer's counterpart.

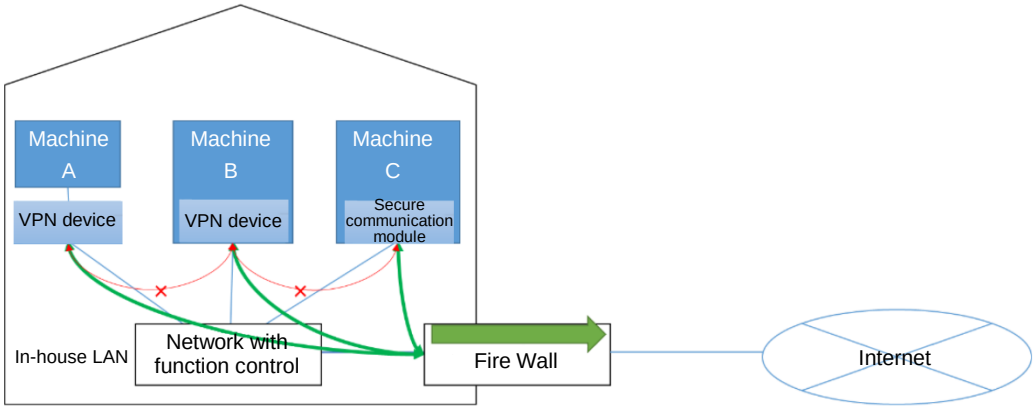

Figure 6.6 Setting of enabling/disabling communication by a communication control switch and so on

The switches that perform such control is available from many vendors, primarily designed for separation of customers in the shared network such as in a residential complex. Many wireless LAN devices are also equipped with such a separation function in the infrastructure mode.

Actual deployment of this case can have some variations; one base case is to use separate VPN device (machine A in the diagram). VPN facility can also be integrated with the equipment as a part of the communication module of the equipment (machine B). Furthermore, full VPN facility can be replaced by some simple, secure, dedicated communication protocol (machine C).

Management of the VPN devices in this use case is better served by the

manufacture's side for two reasons; it should be configured tightly related to the manufacture's counterpart; and also it is infeasible to perform management operations (b) and (c) described above by the client side. Such maintenance operations may be included to the (possibly paid) maintenance service provided by the manufacturer. On the opposite, the management of in-house LAN and the firewall should be performed on the client side, as a measure for the self-management of the factory security.

[In-house LAN connection method]

If a full-scale inter-device communication within the factory is required, it is necessary to manage both external and internal communication at the local network level. Without that, we cannot restrict the external security border of the in-factory network to the single point of management. Consequently, the network configuration becomes similar to those shown in Figure 6.1, and the all external communications pass through the factory's single external connection point.

One of the most major risks for such configuration is that the infection of every single device within the LAN affects broadly many other (possibly vulnerable) devices within the same LAN. Leakage of internal information abusing the permitted route of communication for external services is also a major risk. To mitigate or reduce such risks, it is desirable to control as detailed as possible the permission of both external communications to services and internal communication between devices. At the same time, if complicated network operation such as VLAN is employed, it will impose both high costs and high risks of operation errors even if professional engineers are involved. To solve such problems, the following measures should be examined. Unfortunately, some of measures suggested here cannot be implemented easily today, due to the high cost of implementation and management. We propose to develop such technologies/products soon to reduce the operation cost and make it realistic.

(a) To prevent device spoofing, describe and manage all connections of the in-house devices to the network at the physical level or logical level, e.g. which device is connected to which connection port and which IP

address is used for communication. It can be achieved, for example, by the use of individual encryption keys or the use of WPA2-Enterprise in the wireless LAN. For wired LAN, the use of fixed IP addresses along with the ARP and IP filter setting in physical port level on switches can be used (Layer 2 configuration). Alternative method is to separate each wired devices to the individual logical network by using the L3 switch or VLAN (Layer 3 configuration).

(b) Manage and control the all mutual communication among the in-house devices and communication between local devices and the Internet. Such control should be employed by the communication type and protocol level. Assuming the provisions described in (a), it can be realized by using packet filtering on the switch in the Layer 2 configuration and by setting IP filter of the L3 switch or the router in the Layer 3 configuration.

(c) Above managements should put into the central control at the factory or manufacturing line level. Information Management Chief of the factory/line should be able to comprehensively check the configuration status of all the devices.

(d) Operational management must be provided to monitor the state of the unpermitted communication in (b) and decide whether to update the rules or to isolate the malfunctioning devices.

(e) For any externally outgoing traffics, take appropriate traffic-securing measures such as encryption for protection from eavesdropping and interferences. The technologies used for such securing should be the general-purpose ones that has been widely used and verified for the communication via the Internet. As the examples, authentication using the TLS server certificate and client certificate or establishment of VPN communication such as L2TP can be considered. Whenever possible, it is desirable to have an end-to-end encryption between the devices and the external servers. However, if the communication have to be relayed by some internal management systems, end-to-end encryption must be applied to the communication between the device and the relay system and the relay system and the external system, respectively. If encryption is not applied in the terminal devices side, take enough measures (such as (a) and (b)) so that the communication is not affected in the IP network before encryption is applied.

As a partial measure compared to the full-featured method above, having a separate local network for each device manufacturer may mitigate some risks influenced by the mixture of different security management by some extent. However, as long as logical network is shared at least partially, or as long as having a device that connects two or more logical networks, we consider that the above-mentioned measures will be required in the near future.

- Information security management establishment on the factories and manufacturers

In the above use cases, fundamental requirements for the information security management of these systems are similar to that of the closed-network control systems (for instance, IEC 62443-2-1 CSMS for IACS). Additionally, these systems need more strict management for the risks of vulnerabilities and intrusion incidents, as existence of allowed external communications raises the risks of the security intrusion and information leakage.

Depending of the system designs described earlier in this section, the entity that should primarily manage the information security of these systems will vary. The basic principle is that the entity who holds actual control of the information flow should take the primary role on the information security management. In the first “direct connection use case,” the manufacturers (service providers) must take the primary role, since only the manufacturers’ system engages the primarily control of the devices communications. In this case, the terminal device on the manufacturers’ side that is connected to the factory-side machine should be thought as “a part of factory networks that have been extended to the distant manufacturer’s facility", and the manufacturer’s side network should be conceptually considered as the network of a virtual factory with multiple independent lines (corresponding to multiple customers). Existing guidelines for the control systems should be applied, after appropriately modified based on this virtual aspect of view. Of course, the fundamental diversity between the actual owner of the machines and the manager of the information systems should be carefully understood, and both customers

and manufacturers must have tight communications with each other regarding security policies, risks and countermeasures. The second "simple connection use cases using VPN" can also be considered in the same manner, at least in this moment.

Oppositely, in the "In-house network use case," the factory side should take the primary role of control, and the information flow from factory machines to the manufacturer's network shall be considered as data provision to the external entity with a different security management policies. These external communications should be put under strict and careful management.

In any cases, users and manufacturers should have adequate sharing of information on the contents of communications and its security risks. To enable the factory-side managers to employ reliable management on their information property, it is desirable for the manufacturers to provide the following information to the factory-side in a systematically organized ways.

- *Detailed information of communication required for each device to operate as an information device*:
  Such information includes the following: communication destinations and traffic volume to occur under normal operation, and those relating to alerts that occur at error/abnormal states; the communication destinations and its volumes required to perform software updates, and so on. Without those information, local communication control policy will become either unnecessarily tolerant or inappropriately tightened, causing either failed detection of malware behavior or interference of alert transmissions.
- *Guaranteed/agreed provision period for the maintenance of third-party software platform (operating systems etc.) used in the devices, procedure for applying security updates, and manufacturers' provision period for security vulnerabilities handling of their products*:
  In these days, almost all OS and software cannot be used securely without proper maintenance updates. Accurate information on the period of software maintenance provisions, along with the cost required on such provisions, must be shared between customers and providers, to prevent old devices without being maintained from being used continually without proper maintenance. In other words, "when the old devices

become unuseful” should be mutually understood and agreed.

(3) Guideline for access control for digital data generated by machine tools

The information security measures described in (2) are those for preventing unexpected situations for the parties concerned. The guideline of access control for digital data described in (3) is the summary of "(should be) expected state" for the parties concerned.

For instance, machine tool users can easily assume that information relating to machine tools is supplied to the service provider to some extent. However, it is rare that common understanding regarding the use of digital data and management state (e.g., “which digital data is used in what way under whose management" and "how related digital data is processed after the immediate objective has been accomplished”) are established by the user and the service provider. Focusing on such an aspect of digital data management as the background for users, particularly machine tool users become cautious about sharing of digital data under the environment connected to the Internet, the guideline summarizes a means to the development of common understanding by the parties concerned.

In this case, even if the contents are restricted to the service such as maintenance management assumed in this implementation, the contents vary according to the original idea of the provider so that a caution is necessary in terms its strong nature as the competitive area. Since the manner of using digital data also varies depending on the service contents, it is necessary to allow such diverse ways and foster innovation in organizing the commonly understood items relating to access control for digital data.

Based on such problems involved, the actual concepts are summarized as follows.

[1] Principle

(a) Parties concerned must have the clear common recognition on the digital data handled in terms of following aspects.

- Range of the digital data that is handled

- Purpose of using the digital data that is handled
- Collection, storage, processing, and disposal methods of the digital data that is handled
- Range of the persons who can collect, store, process, and disposed of the digital data that is handled
- Range of the persons who can access the digital data that is handled

(b) The digital data that is handled must be collected within the necessary and adequate range for the use purpose.

(c) For the new knowledge obtained as a result of processing the digital data that is handled, the guideline must be clarified in advance among the parties concerned, under the principle that such knowledge is attributed to the person engaged in the processing.

[2] General summary of the remote maintenance and predictive maintenance services

For the contents described in the principle of [1], it is desirable to maintain certain rules among the parties concerned through a contract and so on within the necessary range according to the individual services.

Ultimately, various handlings must be permitted based on the agreement among the parties concerned. However, when the main service is based on the use of the open network such as the Internet as the precondition, the range of the parties concerned becomes wide in both the service providers and the service receivers, and consequently, related parties may not be able to be specified in advance. Therefore, regarding the typical service type, topical concepts are summarized and the result is utilized for the smooth agreement for individual services.

[Handling of digital data relating to the remote maintenance service]

As shown in the block definition diagram for maintenance work in Figure 5.3, remote maintenance is one of the measures taken for unexpected events. In the main service of the current remote maintenance is identification of the cause of the fault and maintenance parts to be replaced by referencing the histories at the occurrence of a fault in the machine tool. The handling of digital data can be summarized as follows based on the

block definition diagram of the remote maintenance system that is shown in Figure 5.4.

- Range of digital data:
  - Operation information of the machine tool for a certain period up to the occurrence of a fault (Information of sensors installed in the machine tool and alarm information, excluding the manufacturing program and information on work regarding the product manufacturing by the user)
  - Operation history of the worker (operations of power supply/operation switches, operations of auxiliary tool units, etc.)
  - Past maintenance record for a certain period of time
- Use purpose of the digital data:
  To resolve the fault of the machine tool, recover the machine tool to enable normal operation, and identify the relationship between the fault and maintenance parts
- Collection, storing, processing, and disposal methods of the digital data:
  Operation information of machine tools and operation history of workers are collected from the sensors installed in the machine and are stored in the machine tool or the server maintained by the manufacturer based on the remote maintenance contract, which is concluded between the user and manufacturer. In principle, past maintenance record refer to the records of the maintenance work performed by the manufacturer and when the user implements maintenance work individually, the record is collected and stored in the server maintained by the manufacturer based on the remote maintenance contract.
  The digital data described above is processed only by the computer with adequate security measures and is disposed when the fault is resolved, the relationship between the cause of the fault and the operation history is clarified, or based on the remote maintenance contract.

- Range of the persons who can collect, store, process, and disposed of the digital data:
  Digital data can be handled only by the production manager in the user side, person in charge of maintenance and person responsible in the manufacturer side, and persons designated in the remote maintenance contract.

- Range of the persons who can access the data:
  In principle, access to digital data is restricted to only those who can collect, store, process, and disposed of the data.

[Handling of digital data relating to the predictive maintenance service]

As shown in the block definition diagram of maintenance work in Figure 5.3, the predictive maintenance service is to inspect data at a certain cycle in the same way as regular inspection and daily inspection and notify the sections to be repaired in advance. Currently, the service used for detection of the foretaste of the fault in the part that causes the stopping (alarm stop) of the production line for a long period of time. Access control of the data that is handled can be summarized as follows.

- Range of the digital data:
  - Maintenance and replacement records of the parts that cause alarms
  - Operation information (insulation resistance, spot welding pressure, chip wearing degree, voltage and current of arc welding, etc.)
  - A reasoning model for the termination of alarms (a model that causes alarm stop)

- Purpose of using the digital data:
  Detection of abnormality prior to the alarm stop of machine tool

- Collection, saving, processing, and disposal methods of the data:
  During the operation of a machine tool, operation information is collected from the sensor that is installed in the machine and is stored in the server maintained by the user or manufacturer. Past

maintenance records (e.g., part replacement records) are collected from maintenance records of the user based on the predictive maintenance contract and is stored in the same server as for the operation information. A reasoning model is generated and managed by the manufacturer that provides the predictive maintenance, and is stored in the server that performs detection tasks. Digital data are transmitted to the server that performs detection tasks, processed, and disposed of.

- Range of the persons who can collect, store, process, and disposed of the digital data:
  Digital data can be handled only by the production manager in the user side, person in charge of maintenance and person responsible in the manufacturer side, and persons designated in the predictive maintenance contract.
- Range of the persons who can access the data:
  In principle, access to digital data is restricted to only those who can collect, store, process, and disposed of the data.

The handling of digital data of the predictive maintenance service has been summarized. However, the current predictive maintenance service has not reached the level of detecting all the foretastes of machine tool defects and various technical developments are required in this field. In particular, the technology relating to the models of reasoning the sings that lead to alarm stop and the technology for processing data are the basis of the predictive maintenance service and are currently in the process of development. Therefore, to promote the research and development of such technology, consideration should be given to permission of access of the digital data to third parties that exchanged the confidential contract.

7. Proposal of a smart factory by utilizing the information model relating to the target services

The information model organized in 5. comprehensively represents the behaviors of machine tools and describes their various statuses. Accordingly, this model can also be utilized for production management of the entire factory or management of our supply chains as discussed in 4. (1). Recently, remarkable progress of AI technologies represents an opportunity to establish a useful environment for factories to collect and organize machine tool generated digital data in a state that allows great cost savings with significant gains in efficiently.

The keys for implementing mass customization targeted by a smart factory are the cycle for controlling the system and complete optimization. Important to note is that smart customization refers to the strategy of manufacturing customized products at the similar cost and price as those of mass-produced products.

Production data is manageable by personal judgment if data is processed daily. However, creating optimum production instructions is a challenge to be done by personal judgment for data processed by the hour or by the minute. Flexible approaches are important for situations involving a level of difficulty causing a short-term suspension of machine operation which cannot be handled by inflexible production instructions. Various software tools are necessary to support performing complete control analysis, and measures in real time by connecting facilities of production sites, machine tools, and states of various processes. Despite this need for such software tools, connecting extremely diverse hardware and software cannot be done easily. Therefore, constructing a factory to develop this connection mechanism is a great challenge for the customer.

The manufacturing industry has strength in its “Kaizen”, meaning the ability to improve on-site improvement capability, and maintenance and reinforcement measures are important elements of this strength. Conventional improvements by manufacturers result in favor partial optimization. “Kaizen” is implemented for human-oriented activities so that the range is often within the visual reach or arms’ reach so that such activities are effective for the problems in a narrow range such as those between facilities, between a facility and a worker, between a facility and a part, and between parts. However, such an approach cannot

achieve the entire optimization even if partial optimizations are gathered. The following points are to be examined in order to realize a smart factory while ensuring the strength of the domestic manufacturers.

(1) Cyber-physical on-site improvement activity (Cyber-physical “Kaizen”)

This refers to an improvement for a work area at a distance even if it is in the same factory, remote improvement that enables improvements in an overseas factory, and production innovation for improvement.

By visualizing a range that is actually invisible by utilizing the IoT information collection capability, create a virtual environment and construct a cyber-physical improvement site that runs PDCA cycles with predictive techniques, and an improvement site of quick PDCA cycles.

(2) Providing an emergent infrastructure that takes advantage of the strength of the manufacturing industry

From the cyber-physical “Kaizen”, emerge services and methodology for a new manufacturing concept.

In Japan, there are software vendors and integrators relating to machine tools production facilities, peripheral devices, MES, and SCADA. An infrastructure that can integrate the expertise of software vendors and integrators with those in the manufacturing industry exists here.

What is important here is to construct a cyber-physical factory that allows the flow of feeding back the improvement results on the production engineering side to the production management side. At utilization in production management and analysis by AI technologies, it is not necessarily reasonable to use the entire data generated in real time from the machine tool as it is. Although the trend of technological progress that determines the speed of information processing and communication is to be taken into consideration, at least, based on the trend of technological progress that is assumed for the time being as the precondition, the mechanism for using generated information effectively by selecting such information is the reasonable method. This enables improvements of the process design as well as the manufacturing planning.

On one hand, the engineering chain (production engineering)determines specifications of advanced real time control derived from the machine tools, FA, and robots for the realization of high quality and efficiency. On the other hand, the supply chain (production management) determines how many products are to be produced by when and where. Regarding a linking between two chains at the information level, it is significant to arrange specific linkage measures as the interfaces (information contents, granularity, frequency, method, communication protocol, etc.), with the emphasis on the differences of quality and volume of the information required for each chain to enhance the functions by fully utilizing the result of the new technology such as IoT.

The structure of a conceptual smart factory is presented by utilizing the information model that is summarized in 5. The skeletal frame of the interface draft is also presented. The primary proposal of the interfaces will be announced in this year.

- Data (A) in the machine tool that is represented by NC of the diagram below are utilized in both the production management and production engineering areas and specifically, a wide range of services can be provided by the following data flow. The conventional service such as operation condition visualization is directly integrated into the production management data from each machine tool (B). In the proposed smart factory, the production engineering data is integrated, processed, and then provided to the production management side.
- Various types of data that indicate the operating state in (A) extracted in the various units (i.e., second, minute, hour, and day), are integrated and stored as production engineering data (C). The data are used to promote more detailed site visualization of operating states and on -site improvement activities (i.e., “Kaizen”).
- Various types of data that indicate the operating states in (A) in the time units of the *μs* and *ms* levels are integrated and stored as production engineering data at the production site and are used for improvement of machining conditions.
- Production engineering data (C) are primarily processed (system construction options such as remote mode and cloud are available) by the intelligent judgment module (D) installed in a machine production

site, are fed back to (A), and are used by the service such as machining efficiency improvements.

- The intelligent judgment module (D) promotes improvements on the production engineering side. By sending the information from (D) to the production management side (B), a cyber-physical factory with an improvement scenario of total optimization can be constructed.

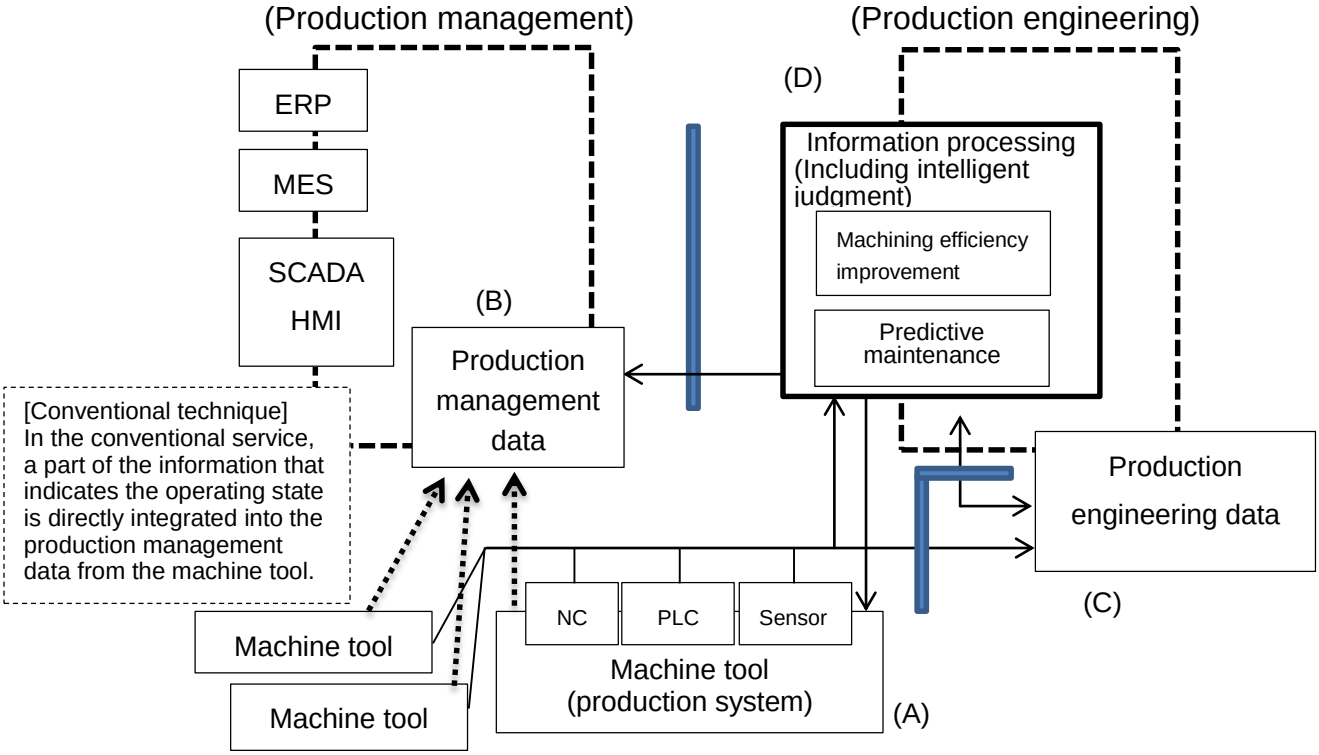

Figure 7.1 Smart factory conceptual diagram

To fully utilize the strength of the production engineering in the manufacturing industry, it is important to provide the interfaces to be standardized for distribution of data by modeling the data flow based on the improvement cycle in each service as described above.

[Skeletal frame of interfaces]

In the examination of this system, standardization of interfaces is important due to the involvement of a variety of components of (A) such as CNC and sensors, and of a variety of their manufacturers.

At this point, examples of the necessary data types that are critical to the interfaces are listed. In addition, further examination regarding the standardization of meaning of these specific data types is necessary.

- Interfaces among (A), (C), and (D)
  - Machine tool state signals (initial, machining preparation, machining, alarm, communication disconnection, and so on)
  - Machine tool machining state (machining program, machining mode, start of machining, and stop)
  - Machine tool motion state (position, speed, acceleration, and so on)
  - Spindle/feed motor state of machine tool (position, speed, acceleration, torque, temperature, etc.)
  - Machine tool alarm state (alarm type and related information)
  - Machine tool mechanical state (operation management and volume of states required for predictive maintenance)
  - Information from sensors

- Interfaces between (D) and (B)
  - Operating status of machining cell (initial, machining preparation, machining, alarm, communication disconnection, etc.)
  - Machine operation state of machining cell (machining part type, machining quantity, machining time, stop period, etc.)
  - Machine power consumption of machining cell
  - Machine alarm state of machining cell and its assumed cause
  - Machine warning state of machining cell and predictive maintenance target parts
  - Information relating to the quality of machining cell parts (accuracy, surface quality, etc.)

(Attachment)

Members of the committee

(Chairman)	Waseda University, Professor	Akiyoshi Kabe
(Vice-Chair)	National Institute of Advanced Industrial Science and Technology Information Technology Research Institute, Cyber Physical System Research Group Group Leader	Hiroshi Oiwa

[Syllabary order]

Okuma Co.	Member of the Board Executive Director Technology Division General Manager	Atsushi Ieki
JTEKT Corp.	Member of the Board Executive Vice-President	Masakazu Isaka
	Senior Fellow	Shirou Nakano
DMG Mori Co.,Ltd.	Senior Executive Officer Manufacturing and Development Head Office in charge of Electrical circuit/ control	Makoto Fujishima
Hitachi, Ltd.	MONOZUKURI Strategy Division Production Engineering Promotion Department Chief Engineer	Akio Hamaoka
FANUC Co.	Member of the Board Executive Vice President Research & Development Administration Division General Manager	Shunsuke Matsubara
Fujitsu, Ltd.	Industry Business Development Unit Principal Consultant	Hiroyuki Kumagai
Mitsubishi Electric Co.	Factory Automation Systems Group Industrial Automation Machinery Division Senior Chief Engineer	Koji Yasui
Yamazaki Mazak Co.	Managing Officer Production Headquarters	Yasuhiko Ohno
	Administration Headquarters BEST Promotion Department Corporate Officer General Manager	Isamu Inazuru

National Institute of Advanced Industrial Science and Technology
Robot Innovation Research Center
Robot Software Research Laboratory
Research Laboratory Leader Isao Hara

(WG1 Chief examiner)
Hitachi, Ltd. Power and Infrastructure Systems Group
Power & Infrastructure Systems Strategic Planning Division
Business Development & External Relations Department
Department Manager
Kiyoshi Mizukami