Design of Smart Factory Web Services
Based on the Industrial Internet of Things

Jieun Jung
Korea Electronics Technology Institute (KETI)
jejung@keti.re.kr

Byunghun Song
Korea Electronics Technology Institute (KETI)
bhsong@keti.re.kr

Kym Watson
Fraunhofer IOSB
kym.watson@iosb.fraunhofer.de

Thomas Usländer
Fraunhofer IOSB
thomas.uslaender@iosb.fraunhofer.de

Abstract

The Industrial Internet of Things (IIoT) is cited as the latest means for making manufacturing more flexible, cost effective, and responsive to changes in customer demands. However, a major concern surrounding the IIoT is interoperability between devices and machines that function within different protocols and architectures. This paper presents the Smart Factory Web (SFW), which is based on the IIoT concept of improving factory-to-factory interoperability. The proposed SFW enables secure data and service integration in cross-site application scenarios as well as 'plug & work' functions for devices, machines, and data analytics software by applying industrial standards, Open Platform Communications Unified Architecture (OPC UA), and Automation Markup Language (AutomationML). To reach the goal, experimental factories that have heterogeneous manufacturing infrastructures are linked and the SFW is implemented in four phases. The usage scenario, called order-driven adaptive production, used to align capacity across factories, will also be validated in the real deployment.

1. Introduction

Today, Industrial Internet of Things (IIoT) is the next wave of innovation impacting the way the world connects and optimizes machines. The IIoT, through the use of sensors, advanced analytics, and intelligent decision making, will profoundly transform the way field assets (e.g., machines or robots) connect and communicate with enterprise [1]. With the applications and services of IIoT to manufacturing, many believe the fourth stage of industrialization (referred to as Industry 4.0) is approaching [2]. Sensors, machines, and Information Technology (IT) systems will be able to interact with one another using industrial internet technology. Further, they will be able to analyze data to predict failures, configure themselves, and adapt to changes.

Shifting the paradigm on the shop floor as IT creates more flexible and responsive manufacturing is not a new concept. Leading automation and software suppliers have been working to address this demand for decades. However, today's business practices have not always been successful due to the vendor's dependency on the underlying production infrastructure [3]. The high variability of systems and equipment in a factory, by line and even by manufacturing process, combined with a mix of new equipment and legacy investments, leads to challenges in interoperability and flexibility.

According to a study commissioned by Forrester Consulting [4], 67% of surveyed manufactures are concerned with lack of standard interfaces and interoperability challenges. Another survey on the perceived barriers to adaption of the IIoT, conducted by the World Economic Forum [5], revealed that almost two-thirds of respondents agree with the widely-held view that security and interoperability are the two biggest hurdles for the IIoT.

In response to these concerns, major standard organizations and industry consortiums have already started teaming up to address the standardization challenges and to promote open interoperability and the widespread usage of a common architecture. For example, International Electrotechnical Commission (IEC), Standardization Management Board (SMB) [6], established a Strategy Group, SG8, to deal with a number of tasks related to smart manufacturing in 2014. SG8 focuses on leveraging current and next-generation technologies to achieve safe and secure factory operations. The Industrial Internet Consortium (IIC) [7] was also founded to accelerate the development, adoption, and widespread use of interconnected

HICSS

machines, devices, and intelligent analytics. The IIC members are concerned with creating an ecosystem for interoperability and security via a reference architecture, security framework, and real-world implementation. Lastly, Institute of Electrical and Electronics Engineers (IEEE) Project P2413 [8] and OneM2M [9] have focused on developing an architecture framework for IoT and defining how devices and services are used in the IoT communication.

There are still open questions to be answered in terms of the industrial use of IIoT technology. Recently, industrial providers and academic researchers have initiated real-world testbeds to demonstrate how technologies from different organizations can work together and support new innovations. These test-beds for smart production technologies (referred to as experimental factories) are being actively operated with the purpose of establishing interoperability guidelines and applying new IT technologies in existing automated systems.

However, there has been no attempt to interconnect the experimental factories and allow them to flexibly adapt their production capabilities based on cross-site demands. Because the experimental factories have a great deal of freedom to experiment, they can promptly react to changing requirements from an integration point of view. Thus, Korea Electronics Technology Institute (KETI) and Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB) have launched a joint testbed project called Smart Factory Web (SFW),[1] which links the heterogeneous infrastructures of each experimental factory [10]. At the moment, Fraunhofer IOSB in Karlsruhe and Lemgo, Germany, operates experimental factories to demonstrate new concepts related to Industry 4.0. KETI is establishing factories for IIoT services in Pangyo and Ansan, Korea.

The vision of SFW is to network a web of smart factories to improve order fulfillment by aligning capacity across production sites with flexible adaptation of production capabilities and sharing of resources, assets, and inventory. To realize this vision, secure data and service integration will be implemented in cross-site application scenarios as well as 'plug & work' functions for devices, machines, and data analytics software by applying industrial standards, OPC UA [11] and AutomationML [12].

We expect that researchers can test and resolve a number of issues related to factory-to-factory interoperability on the basis of the industrial standards as well as IIoT concepts by linking factories.

Additionally, the adaptability and security of cross-site production can be validated between factories.

The paper is structured as follows. Section 2 gives an overview of related work. Section 3 explains the SFW architecture and technologies to be implemented in a phased approach. Section 4 presents the core usage scenario, order-driven adaptive production, to be validated. Section 5 concludes the paper.

2. Related Work

With traditional automation architectures, devices and machines are directly connected to a control system and are poorly visible to enterprise business applications. This leads to a major bottleneck hindering increases in the ability of factories to react to customer demands and unforeseen events in the supply chain [13].

However, as IoT technologies emerge into the industrial environment, a number of assets are able to communicate, collaborate, and offer their functionality as a service. Several efforts on service oriented manufacturing systems have been explored.

Karnouskos et al. [14], [15] work intensively on Service Oriented Architecture (SOA) to enhance interoperability and cross-layer collaboration for gluing together heterogeneous industrial systems. Two prototypes that serve as a proof-of-concept were implemented. The first is a simple event-based monitoring prototype for dynamic management and enterprise control via a web service. Subsequently, an integration of heterogeneous devices using dynamic web service composition was presented in a mashup manner. Karnouskos et al. tried to demonstrate the effects of using web services on enterprise systems, networks, and the device itself.

An IoT architecture for things from the industrial environment was presented in [16]. The integration architecture, based on the OPC.NET specification, consisted of two main components: a data server and Human Machine Interface (HMI) application as a client. The integration concept can make it easy to introduce new fieldbus protocols and distribute data acquired from fieldbuses by using Internet infrastructure.

Moreover, recent research [17], [18] has focused on analysis using big data management and artificial intelligence on the cloud to feed back to the manufacturing floor. However, there are still many challenges to obtain real-time data from the manufacturing floor and integrating that data with IT data such as that from sales, logistics, and support.

The plug & work approach has also been one of the crucial topics for interfaces in industrial automation. A
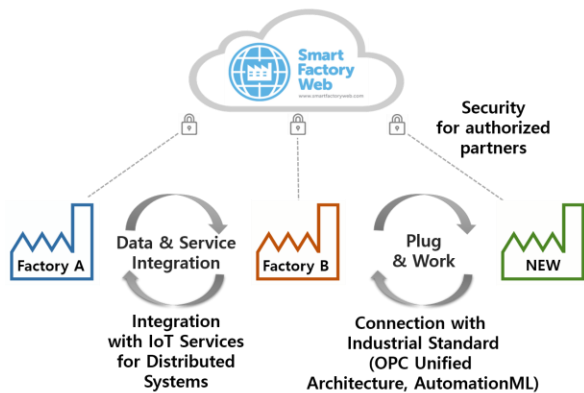
Figure 1. Objective of the Smart Factory Web

basic aspect is the identification of control relevant entities within production systems that can be plugged in or connected to the production system and start operation without requiring any changes to the control applications in the rest of the production system [19], [20]. In order to support plug & work capabilities for physical resources (e.g., devices, modules, or subsystems) within networked control systems, the following five steps are required: 1) physical connection, 2) discovery, 3) communication, 4) capability assessment, and 5) configurations, based on OPC UA and AutomationML [19].

OPC UA is a platform-independent standard for how industrial automation devices and systems communicate. AutomationML is a standard data format based on XML for describing production factories and factory components.

3. Proposed Architecture

3.1. Phased Approach

The objective of the proposed SFW is to demonstrate secure data and service integration in cross-site application scenarios as well as plug & work functions for devices, machines, and data analytics software, as illustrated in Figure 1.

The industrial standards AutomationML and OPC UA, complemented by the companion specification "OPC UA for AutomationML", will play a key role. Combined, these standards reduce the manual engineering effort required for the exchange of information between factories [10].

The SFW will be implemented in four phases as presented in Figure 2. In the first phase, called geospatial mapping, a geoportal will be implemented to show the location of registered factories and to
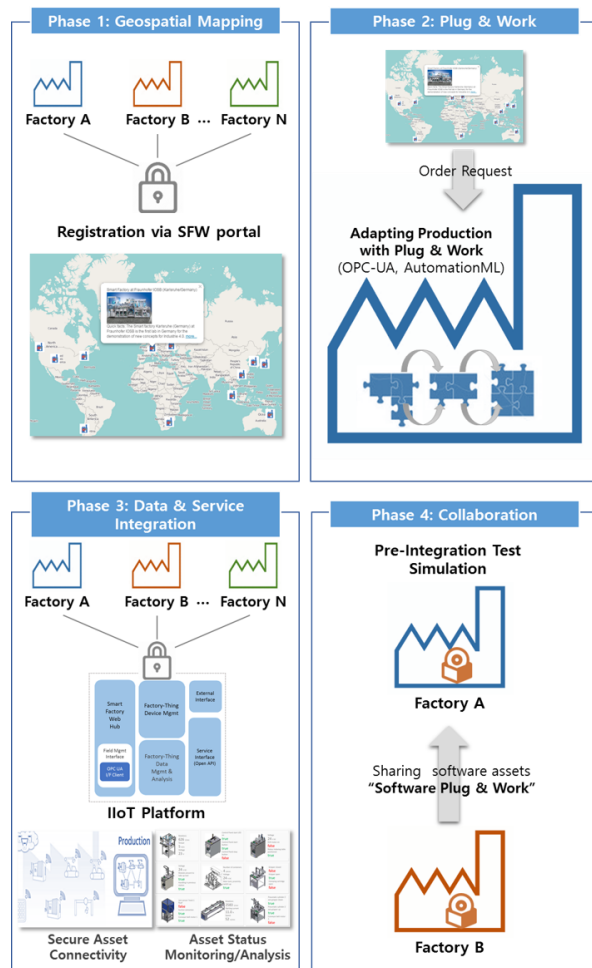

Figure 2. Four-phased approach

visualize factory information on a global map in layered views. In order to discover a smart factory with the required capabilities, detailed information such as asset status, configuration, and operation schedules by location will be provided depending on the user role and level.

The second phase will focus on plug & work functions supporting auto-connection among various types of factory devices and machines. It will validate the functionalities used to plug new components into a factory, connecting without any changes to the control applications through the usage scenario. The main idea is that the component's attributes and communication interfaces will be recognized and its application functions will then be reconfigured automatically based on OPC UA and AutomationML standards.

The third phase, concerning secure data and service integration, will feature asset-monitoring and data analysis applications for the SFW. The IIoT platform will provide secure functions to aggregate and process
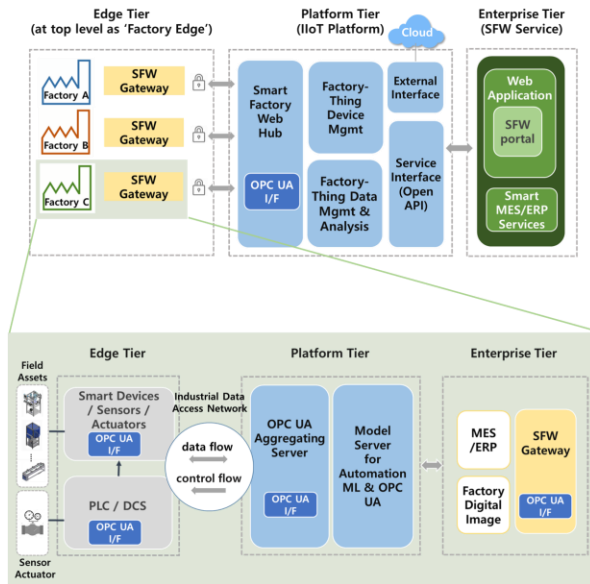
Figure 3. Three-tier deployment architecture of smart factory web, experimental factory

massive amounts of factory data and integrate with business systems. Services will be implemented for asset status monitoring, as well as material and information logistics.

The goal of the fourth phase, collaboration, is to design and implement methods for cross-site engineering, including simulation and pre-integration testing between multiple components. The plug & work scenarios will be extended to the deployment of software algorithms and data analytics. Further details regarding this phase are explained in Section 4, which gives an example of a use case.

3.2. Deployment Architecture

The deployment architecture depicted in Figure 3 represents the different components and various tiers of the SFW and the experimental factory, respectively, which is based on the three-tier Industrial Internet Reference Architecture (IIRA) [21]. The upper layer shows the SFW itself, whereas the lower level describes a single factory. The two levels are linked by a SFW gateway.

Each factory instance is connected to the SFW gateway for data communication between the IIoT platform tiers. The main role of the SFW gateway is to collect necessary data from the factory and send collected or preprocessed data to the IIoT platform. It also performs a syntactical and semantic data conversion to a uniform information model for upstream and downstream communication.

The IIoT platform is designed to manage a variety of factory instances. It consists of four major components: (i) SFW Hub, which has an OPC UA client module to interface with OPC UA servers in the SFW gateways; (ii) Factory-Thing Device Mgmt., which provides Factory-Thing registration, deletion, connection, and search functions; (iii) Factory-Thing Data Mgmt. & Analysis, which is responsible for data collection, storage, analysis, and transmission; and (iv) Service Interface, which provides an open Application Programming Interface (API) for the SFW portal as well as for Enterprise Information System (EIS) applications.

At the enterprise tier, the SFW portal will visualize the deployment of factory assets and their locations through geospatial mapping services. Access to factory information will be controlled by an assigned security mechanism. If necessary, smart EIS, such as the Manufacturing Execution System (MES) or Enterprise Resource Planning (ERP) system, can be involved in SFW.

The architecture of the experimental factory is also illustrated in detail in Figure 3. The physical platform of the edge tier consists of various field assets, including devices, sensors, actuators, control systems such as Programmable logic controllers (PLC), and Distributed Control Systems (DCS).

At the edge tier, two classes of sensors and actuators can be installed: classical sensors/actuators and smart sensors/actuators with OPC UA interface. The classical sensors/actuators must be connected using the PLC to the OPC UA server implementing a security profile, because OPC UA specifies security profiles for authentication, authorization, and encryption. However, smart sensors, actuators, and devices with OPC UA interfaces can choose their connectivity type to connect with an OPC UA server. The data and command at the edge tier are collected and processed by the OPC UA aggregating server as well as the model server.

The OPC UA aggregating server consolidates the data space of individual OPC UA servers installed in the field assets to ensure the consistency of configuration and online data. Information about the assets, configuration, topology, and data context (the metadata) is exposed in the collective address space of the individual OPC UA servers. The model server receives asset descriptions in AutomationML format and integrates various individual models of devices and machines to form an overall model. The AutomationML models can be exchanged via OPC UA communication. The companion specification for AutomationML consists of an object model including many specific semantics which can be used online with multiple involved parties/tools by OPC UA.
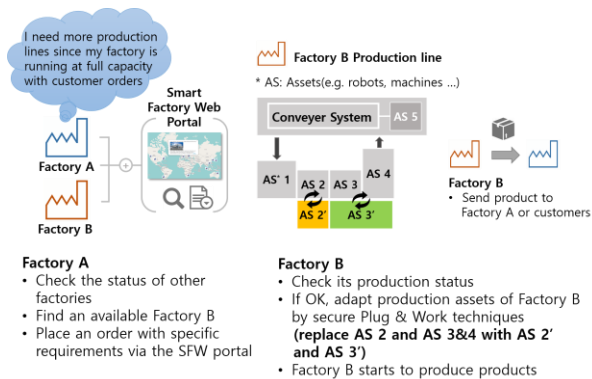
Figure 4. Usage scenario: order-driven, flexible adaption of production value

At the enterprise tier, the access to factory data by external parties is strictly restricted for reasons of security and performance. The SFW gateway can only access data in the factory digital image mapping of the part of the factory data approved for release. As a result, applications in the SFW platform tier will not access machines and devices of the factory directly.

4. Usage Scenario

An order-driven adaptive production scenario was designed from the factory integration perspective. This scenario provides a pictures of all the factory interactions within the SFW, as illustrated in Figure 4.

Suppose that a single factory, A, is not able to meet a customer order due to a lack of product capacity. In this case, with the aid of a discovery service provided by the SFW portal, the manager of factory A can identify a factory B as having the required conditions and can send an order request. Factory B then checks its production status and adapts its production process flexibly to meet the order, reconstructing a production line, such as by replacing or extending assets. These replacements use the plug & work method to ensure adaptive and secure production operation. With an information model that contains properties and characteristics of new production components, newly plugged in components are integrated into the running production process without manual efforts or changes. Finally, the business application, such as MES in factory B, is adapted automatically and executes an order.

To implement the entire usage scenario, sub-scenarios that include overall patterns as follows will be developed:

- Publish: registration of smart factories
- Find: discovering smart factories
- Order: management and execution of orders
- Adapt: adapting the factory production
- Bind: asset connectivity and monitoring
- Collaborate: collaborative engineering

5. Conclusion

The IIoT and its potential to transform operations is currently one of the hottest topics in manufacturing. As a reflection of its increasing significance as well as growing customer demand, several experimental factories have been established to validate interoperable interfaces and common architectures.

This paper proposed the Smart Factory Web (SFW), which links an individual experimental factory with heterogeneous infrastructures based on the IIoT concept. Our main goal for connecting factories in a network is to improve order fulfillment, which may be best accomplished by aligning production capacity across sites and adapting flexibly to share resources. To realize this goal, the SFW will be implemented in four phases: (i) geospatial mapping, (ii) plug & work, (iii) data and service integration, and (iv) collaboration.

The coherent usage scenarios related to asset adaptation will also be employed to validate diverse issues in the real factory environment. As seen in the usage scenario, the engineering effort of adapting and deploying the asset will be minimized by using common interfaces between smart factories. Registered factories in the SFW will also have a great opportunity to optimize manufacturing, resulting in reductions in unnecessary labor and waste of resourced, as well as enlarging their market by being responsive to order requests.

For future work, security profiles will be explored to ensure secure cross-site communication with managed user roles. Furthermore, an appropriate matching procedure to identify a factory as having the required conditions needs to be investigated. These efforts should address architectural and security issues at the level of the Smart Factory Web based on the IIoT concept as well as within a factory.

6. Acknowledgements

7. References

[1] S. Wang, J. Wan, D. Li, and C. Zhang, "Implementing smart factory of Industries 4.0: An outlook," Int. J. Distrib. Sensor Networks, Apr. 2015.

[2] M. Rüßmann, M. Lorenz, P. Gerbert, M. Waldner, J. Justus, P. Engel, and M. Harnisch, "Industry 4.0: The future of productivity and growth in manufacturing industries," Boston Consulting Group, Apr. 2015.

[3] ARC Advisory Group, "Process automation and the IoT: Yokogawa's vigilant plant approach to the connected industrial enterprise," ARC White Paper, Feb. 2015.

[4] Forrester Research, "Connect and protect: The importance of security and identity access management for connected devices," Forrester Consulting Thought Leadership Paper, Aug. 2015.

[5] World Economic Forum, "Industrial internet of things: Unleashing the potential of connected products and services", Industry Agenda, Jan. 2015.

[6] IEC SMB SG 8, Industry 4.0 Smart Manufacturing, http://www.iec.ch/dyn/www/f?p=103:85:0::::FSP_ORG_ID, FSP_LANG_ID:11072,25

[7] Industrial Internet Consortium, http://www.iiconsortium.org/

[8] IEEE Project, P2413, "Standard for an architectural framework for the internet of things (IoT)," http://standards.ieee.org/develop/project/2413.html

[9] OneM2M global initiative, http://www.onem2m.org/

[10] K. Watson, "Smart factory web: A testbed for IIC", Fraunhofer IOSB magazine visIT on Industrie 4.0, Apr. 2016.

[11] OPC Foundation, OPC Unified Architecture, http://www.opcfoundation.org/

[12] IEC 62714, "Engineering data exchange format for use in industrial systems engineering – Automation Markup Language AML," [white paper] available at http://www.automationml.org/

[13] D. Gerwin, "Manufacturing flexibility: A strategic perspective," Manage. Sci., vol. 39, no. 4, pp. 395–410, 1993.

[14] S. Karnouskos, O. Baecker, L. M. S. de Souza, and P. Spiess, "Integration of SOA-ready networked embedded devices in enterprise systems via a cross-layered web service infrastructure," in Proc. ETFA Emerging Technologies & Factory Automation IEEE Conf., 2007, Patras, Greece.

[15] S. Karnouskos, D. Guinard, D. Savio, P. Spiess, O. Baecker, V. Trifa, and L. M. S. de Souza, "Towards the real-time enterprise: Service-based integration of heterogeneous SOA-ready industrial devices with enterprise applications," Lecture Notes Comp. Sci. (LNCS), vol. 4952, pp. 50–67, 2008.

[16] I. Ungurean, N.-C. Gaitan, and V. G. Gaitan, "An IoT architecture for things from industrial environment," Int. Conf. Communications (COMM), pp. 1–4, 2014.

[17] J. Lee, E. Lapira, B. Bagheri, and H.-a. Kao, "Recent advances and trends in predictive manufacturing systems in big data environment", Manufacturing Letters, vol. 1, no. 1, pp. 38–41, 2013.

[18] O. Niggemann, C. Frey, "Data-driven anomaly detection in cyber-physical production systems," Automatisierungstechnik, vol. 63, no. 10, 2015.

[19] M. Schleipen, A. Lüder, O. Sauer, H. Flatt, and J. Jasperneite, "Requirements and concept for plug-and-work," Automatisierungstechnik, vol. 63, no. 10, 2015.

[20] M. Schleipen, E. Selyansky, R. Henssen, and T. Bischoff, "Multi-level user and role concept for a secure plug-and-work based on OPC UA and AutomationML", in 20th IEEE Conf. Emerging Technologies Factory Automation, ETFA, 2015.

[21] Industrial Internet Consortium, "Industrial Internet Reference Architecture (version 1.7)", http://www.iiconsortium.org/IIRA-1-7-ajs.pdf, 2015.