Edge Computing Gateway of the Industrial Internet of Things Using Multiple Collaborative Microcontrollers

Ching-Han Chen, Ming-Yi Lin, and Chung-Chi Liu

Abstract

An Internet of Things gateway serves as a key intermediary between numerous smart things and their corresponding cloud networking servers. A typical conventional gateway system uses a high-level embedded microcontroller (MCU) as its core; that MCU performs low-level perception-layer device network management, upper-level cloud server functions, and remote mobile computation services. However, in edge computing, many factors need to be considered when designing an IoT gateway, such as minimizing the response time, the power consumption, and the bandwidth cost. Regarding system scalability, computational efficiency, and communication efficiency, solutions that use a single MCU cannot deliver IoT functionality such as big data collection, management, real-time communication, expandable peripherals, and various other services. Therefore, this article proposes an innovative multi-MCU system framework combining a field-programmable-gate-array-based hardware bridge and multiple scalable MCUs to realize an edge gateway of a smart sensor fieldbus network. Through distributed and collaborative computing, the multi-MCU edge gateway can efficiently perform fieldbus network management, embedded data collection, and networking communication, thereby considerably reducing the real-time power consumption and improving scalability compared to the existing industrial IoT solutions.

Introduction

The Internet of Things (IoT) is used in a wide range of fields such as industry, business, environmental engineering, mobile devices, and governance; in addition, it can be used to support various efforts, such as smart transport, healthcare, farming, smart energy, and environmental monitoring [1, 2].

Recently, moving service supply from the cloud to the edge has enabled the possibility of meeting application delay requirements, improves scalability and energy efficiency, and mitigates the network traffic burden [3]. With these advantages, edge computing can become a promising solution and can provide more scalable services for delay-tolerant IoT applications. In [3], Ju *et al.* first proposed a transparent-computing-based IoT architecture and clearly identify its advantages and associated challenges. Yaoxue *et al.* [4] analyzed the disadvantages of cloud computing when big data encounters IoT, and introduced different edge computing paradigms, such as transparent computing and fog computing, to support the big data services of IoT.

A typical IoT architecture comprises three layers. The core of the architecture is the IoT gateway of the network layer, which controls and manages the bottom-perception-layer smart sensors and actuators, monitors the diverse automation equipment and status of industrial devices, provides upper-application-layer data reports, and manipulates interfaces. The IoT gateway is also an information platform and serves as a key intermediary between numerous smart devices and their corresponding cloud servers or networking devices. For example, in small-scale and low-power IoT applications (e.g., smart homes), conventional gateway systems mainly use microcontrollers (MCUs) to perform bottom-perception-layer device network management, upper-level cloud server functions, and remote mobile computation services.

The Industrial IoT (IIoT) is a topic within Industry 4.0; IIoT is intensively discussed in government and academic circles [8–11]. The main difference between IoT and IIoT is the presence of diverse automation equipment and industrial devices in an IIoT environment; moreover, IIoT is often used in applications such as smart factories and smart manufacturing.

Particular constraints hold for IIoT systems that achieve IoT functionality. The IoT enables any object to be connected anytime and anywhere with anything and anyone, but because different control interfaces and communication protocols are used in the aforementioned physical devices, meeting the reliability and real-time communication requirements in the IIoT environment is difficult. Therefore, reliability and real-time communication limitations have become key IIoT research topics.

Recently, academicians and commercial practitioners have focused on developing IIoT gateway-related technologies and products for factory automation, smart industrial manufacturing, and other IIoT solutions. Studies on IIoT gateways have not considered the overall system hardware cost, power consumption, and other performance indices; moreover, they have not considered the interconnection, intercommunication, interaction, and interoperation requirements of a complex IIoT gateway system. The aforementioned factors are believed to affect the overall performance of the IIoT system. In addition, industry-related com-

Digital Object Identifier:
10.1109/MNET.2018.1700146

Ching-Han Chen and Ming-Yi Lin are with National Central University; Chung-Chi Liu is with Cavium, Inc.

0890-8044/18/$25.00 © 2018 IEEE

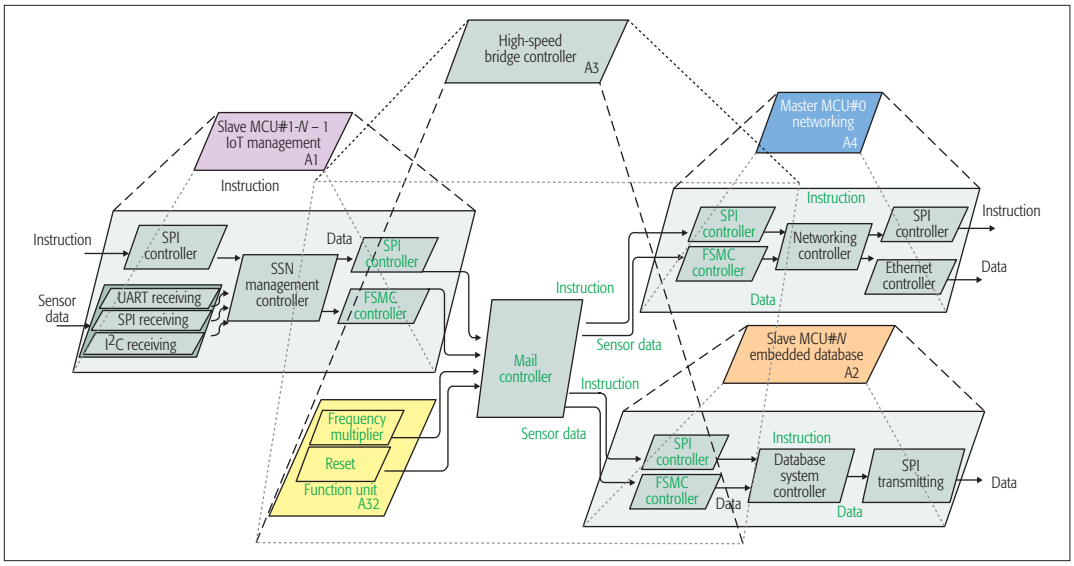


FIGURE 1. Multi-MCU IIoT gateway by IDEF0.

mercial gateway products are notably expensive; therefore, the cost of integrating all performance indices into an IIoT system will be very high.

From the viewpoint of performance, system scalability, and computation and communication efficiency, solutions that use a single MCU cannot fulfill the requirements of IoT with respect to heterogeneous network communication, management, big data collection, and various other services. Therefore, this study considers a multi-MCU architecture for an IIoT gateway because of the advantages of MCUs, which include small size, low cost, low power consumption, simple interface, and high reliability; moreover, an MCU does not require an additional operating system. However, in the multi-MCU architecture, short-distance synchronous serial communications between the serial peripheral interface (SPI), RS232, and RS485 suffer from a bottleneck.

Because of this communication bandwidth problem, in this study, we incorporate a high-speed parallel bridge controller using a reconfigurable field programmable gate array (FPGA) into the multi-MCU gateway architecture. By using the reconfigurable FPGA for high-speed parallel computing to enhance the efficiency of data transmission and increasing the gateway expansibility, in this study, we divide the communication interface into two subsets for data transmission and command state control.

In the design and integration of heterogeneous network systems, each type of IoT system exhibits a unique network interface and a distinct protocol. The processes of protocol conversion and system integration are very difficult; moreover, the proposed system designs are wasteful and complicated because of the interconnection, intercommunication, interaction, and interoperation features in the IIoT architecture. Therefore, appropriate solutions and integration methods must be applied to fulfill the requirements of heterogeneous networks for complex IIoT systems. In conclusion, having a strong and effective design methodology is necessary. In this study, we propose an innovative multi-MCU gateway system architecture by using a coherent and systematic

The proposed system features distributed processing, high-speed communication between MCUs, and compatibility with a wide range of peripheral devices. Furthermore, the multi-MCU gateway architecture enables seamless roaming in a single logical overlay network comprising many heterogeneous physical networks and provides high communication performance for these networks.

design methodology as the core design concept to overcome the problem of complex heterogeneous network integration [12–14]. A multi-MCU smart gateway is designed to solve the following problems:

1. High flexibility and scalability solved the problem of resource insufficiency in applying a single MCU.
2. High integration solved the hardware and software design problems of the decentralized real-time system.
3. Low-cost, high-efficiency parallel structures solved the problem of the limited performance of a single MCU.

In the proposed multi-MCU system framework, a reconfigurable FPGA-based hardware bridge and multiple MCUs were combined to construct a master–slave architecture for a high-performance multi-MCU IIoT gateway. The proposed system features distributed processing, high-speed communication between MCUs, and compatibility with a wide range of peripheral devices. Furthermore, the multi-MCU gateway architecture enables seamless roaming in a single logical overlay network comprising many heterogeneous physical networks and provides high communication performance for these networks. To understand the development of a gateway system in IoT, this article summarizes the foundational technologies of IoT systems and their communication protocol conversion and key system integration challenges, and identifies research constraints and system requirements. The significance and contributions of this article are summarized as follows:

1. Dynamic adaptation of an FPGA is a generic solution to heterogeneity.
2. With a cross-layer design for system integration, diverse devices can roam among het-

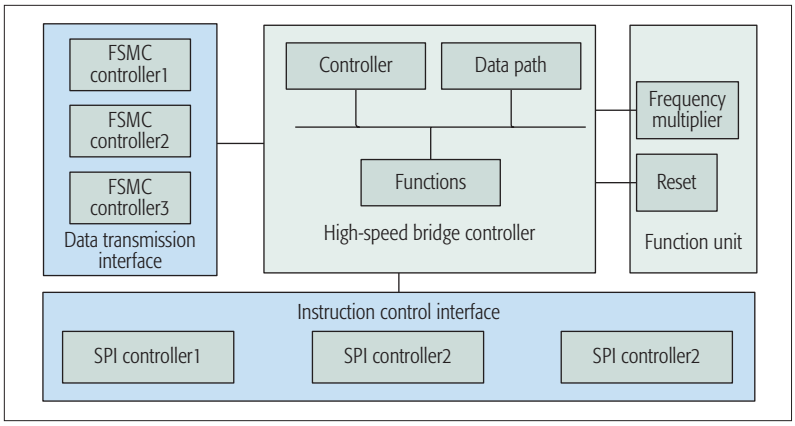


FIGURE 2. High-speed bridge controller hardware architecture.

erogeneous networks and retain ongoing sessions.

3. The use of a gateway in the infrastructure can solve the problems related to heterogeneous network protocol stacks.
4. The use of this gateway offers advantages such as simplicity, flexibility, scalability, low cost, high efficiency, and high integration.

The remainder of this article is organized as follows. Am overview of the heterogeneous sensor network is provided. The overall multi-MCU architecture of the proposed IIoT gateway system is introduced. We present the implementation of and applications for an IoT-based smart manufacturing system in detail. Finally, the conclusions are summarized.

Overview of Heterogeneous Sensor Networks

The IoT system is an intensively discussed topic in industry, government, and academia, and has gained much attention in practice and research in recent years. The ideal goal of IoT is to enable any object to be connected anytime and anywhere with anything and anyone. Consolidating a variety of IoT devices to compose the application for smart things has been applied in many fields recently. Proposals exist for several technical applications within the IoT (e.g., smart home, smart factory, and smart city).

The IoT's characteristics, including an ultra-large-scale network of things (devices); network-level heterogeneity and large numbers of events generated spontaneously by these things; and the gateway being connected to multiple smart functional sensors in the network layer through the physical medium and wired or wireless protocol. The above will make the development of the diverse applications and services an important issue [2, 12].

A. Smart Home

Smart homes are designed to interconnect all things from daily life to the Internet. The ideal goal of a smart home is to enable any object to be connected anytime and anywhere with anything and anyone. Smart home designers envisage a future in which things or objects (e.g., security systems, intelligent lighting systems, smart leak detectors, and heating, ventilation, and air conditioning) can be connected by using suitable information and communication technologies to enable a range of convenient applications and services. Smart sensor networks (SSNs) typically collect information from the physical world and present promising IoT and machine-to-machine solutions for a wide variety of smart household applications. Some examples of such applications include automation control, energy management, homeland security, environmental monitoring, calamity detection, remote monitoring, and healthcare.

Smart Factory

Because of their high usability, adaptability, and scalability, SSNs are also used in industry; this is termed smart manufacturing [1, 2]. Smart manufacturing offers considerable innovation potential for industries; thus, application of IIoT for smart manufacturing is important to improve the efficiency of industrial production and services.

SSNs can be used to develop smart factories in the future. Given the rapidly evolving safety and efficiency requirements of the IIoT, smart sensors and various related devices are widely used in industrial environments. Smart manufacturing enables the collection of large amounts of data between the sensor network and various industrial devices or automated machines.

Smart City

Designers of smart cities envisage a future in which suitable information and communication technologies connect humans and devices to enable a range of convenient services. Smart cities will result in life with a variety of smart objects and a new lifestyle. Smart city solutions are designed to enable high-quality urban living over many generations while contributing to a comfortable and ecofriendly environment [7].

Wireless technologies are being widely used in smart cities around the world. The transmission range and bandwidth of existing wireless technologies cannot meet the requirements of the numerous services in smart cities. Therefore, a type of next-generation wireless network (i.e., the long-range wide area network) was developed to transform smart city networks from single to heterogeneous networks.

Most of the aforementioned applications in industrial environments include the use of numerous smart sensors, actuators, management gateways, and physical/electronic equipment connected to the Internet or a cloud server. Figure 2 illustrates the existing technologies and applications of IIoT. The difficulties in integrating a heterogeneous network make the development of IoT a very challenging task.

Heterogeneous Sensor Network Architecture

The network layer of IoT indicates that things automatically coordinate and exchange information, resulting in heavy real-time demand for network resources. Requests for network bandwidth also come from numerous smart devices. In this study, we consider the transformation of an IIoT network from a single network into a large-scale system of heterogeneous networks. We can predict some potential developments in IoT.

Several types of smart devices and traditional network devices coexist in IIoT networks. However, traditional network standards cannot meet the requirements of numerous IIoT services; traditional protocols cannot unify the diverse types

of industrial equipment that must be connected to the IIoT. Therefore, reliable real-time communications between diverse industrial machines and industrial devices are necessary. Furthermore, scalability for large-scale deployment of sensors is necessary.

Moreover, communication between heterogeneous multinetworks has some challenges [8]. Over the past few decades, machine learning has been exploited for intelligent control in sensor networks. In [5], Zubair *et al.* surveyed a lot of related works to indicate the evolution of deep learning from conventional machine intelligence and machine learning paradigms, and further discussed applications of deep learning in sensor networks. Moreover, Nei *et al.* [6] indicated appropriate input and output characterizations of heterogeneous network traffic, and proposed a deep learning system based on a supervised deep neural network to improve heterogeneous network control.

In particular, the wide deployment of multilayer heterogeneous networks requires improved intracell interference coordination, handoff, protocol conversion, and system integration. Moreover, scale, connection technology, and deployment locations can vary considerably depending on the IIoT application. Thus, integrating various applications into a single IIoT system is a challenging task. Heterogeneity results in problems related to interactions. In general, a gateway can ease a development process by integrating heterogeneous computing and communication devices and supporting interoperability of the diverse applications and services. Developing an IoT gateway system for various applications is a challenging task.

Architecture

In this study, we used a high-level design methodology [15–17] for the hardware–software codesign of a complex multi-MCU gateway system. By using a hierarchical modeling tool, ICOM DEFinition0 (IDEF0), a complex IIoT gateway system was decomposed into a set of distributed functional modules. The behavior of each module can be represented as a sequential–concurrent hybrid discrete-event system. We applied high-level synthesis rules to produce VHSIC hardware description language (VHDL)-based efficient hardware for the bridge controller and to develop embedded software in C for the MCU. Finally, the bridge controllers and embedded software framework were generated automatically to integrate all intelligent functional modules into a complex embedded system.

Overall Architecture of the Multi-MCU IIoT Gateway

The system hardware architecture of the IIoT multi-MCU gateway comprises three major modules: a master MCU controller networking for the cloud, a high-speed bridge controller backbone for data and instruction exchange, and slave MCU controllers for IoT management and database operations. This architecture is based on the functional hierarchy of automation and control gateway systems (Fig. 1). The master MCU controller, which is the networking module at the management level, remotely monitor and supervise all of the control and environment information.

The high-speed bridge controller, which is at the automation level, executes real-time instruction control functions to exchange information in a heterogeneous network environment. The slave MCU controllers, which are at the field level, contain sensors and storage devices (e.g., a memory card). In this system, the IIoT gateway was implemented as a versatile heterogeneous network interface for system integration and a heterogeneous network management subsystem for the network-layer conversion protocol.

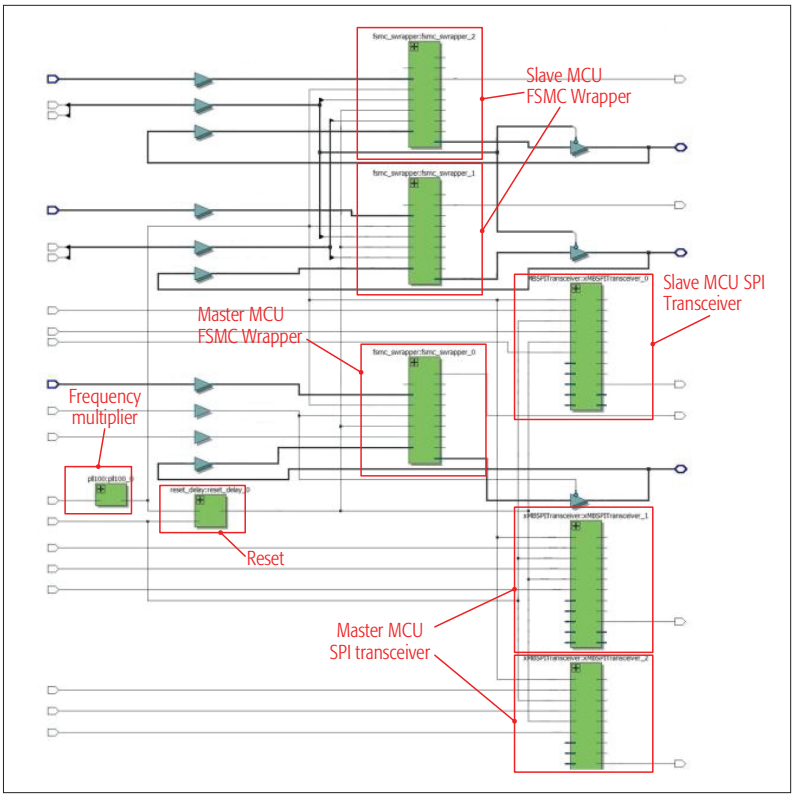


FIGURE 3. VLSI hardware circuit for the high-speed bridge controller.

As shown in Fig. 1, the IIoT gateway was integrated with a networking module, an SSN management module, an embedded database module, and a high-speed bridge controller module.

The main function of the networking module was remote monitoring and supervision of the entire system as well as providing a graphical user interface (GUI) to enable users to capture data, analyze information, and make prompt decisions. The proposed networking module comprised four submodules: the main networking controller, Ethernet controller, flexible static-memory controller (FSMC), and SPI controller.

The SSN management module was responsible for managing the SSN tasks, controlling the actuator, exchanging data and instructions with other heterogeneous network modules that included the main smart sensor network controller submodule, fieldbus communication submodules, FSMC controller submodule, and SPI controller submodule. The fieldbus communication submodule was responsible for transmitting and receiving signals from heterogeneous IoT network interfaces and activating the main management submodule for data processing. The FSMC controller submodule processed the received sensor data at the field level and transmitted it to the high-

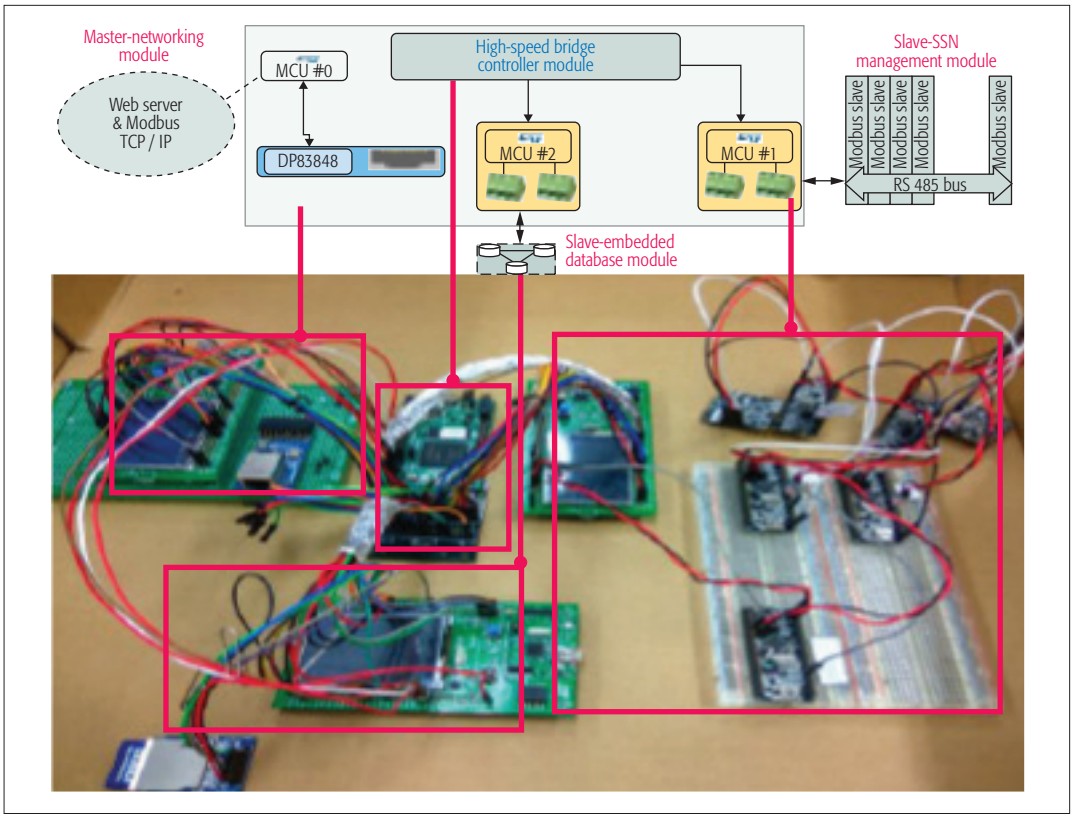


FIGURE 4. Prototype of the IIoT gateway.

The high-speed bridge controller module is the core of the multi-MCU IIoT gateway system and is responsible for packaging processing tasks and controlling communication with the other modules, including the functional unit that assists the main control module in completing specific tasks.

speed bridge controller. The bridge controller, in turn, transmitted instructions to the SPI controller submodule.

In an SSN system, whenever a relevant event occurs in the physical world, sensors gather information about that event and forward it to the actuators, which are responsible for making prompt decisions and taking appropriate actions in response to the sensed environmental data. An SSN controller submodule embedded in a smart management engine integrates functions such as signal extraction, system mode translation, sensor addition, insertion, removal, fault detection, error report generation, and automatic ID configuration, thereby satisfying the definition of SSN systems.

The embedded database module comprises the main database system controller, FSMC controller, and SPI controller submodule. The embedded database module enables the storage, collection, and analysis of valuable information gathered in various industrial environments.

The high-speed bridge controller module is the core of the multi-MCU IIoT gateway system and is responsible for packaging processing tasks and controlling communication with the other modules, including the functional unit that assists the main control module in completing specific tasks.

High-Speed Multi-MCU Bridge Controller

As depicted in Fig. 2, the high-speed bridge controller architecture includes the FSMC controller modules, SPI controller modules, functional unit, and high-speed bridge controller module, including the main controller submodules, data processing submodules, and functional submodules.

Compared to the traditional multi-MCU systems that adopt the serial communication interface, this system uses a hardware bridge controller and an FSMC memory interface as the communication interface between the MCU and the bridge controller to achieve a high degree of parallelism and communication performance, higher than that of a serial interface.

An FPGA was used to implement the bridge controller. However, the main purpose of using the bridge controller was to perform the system high-speed bridge management tasks of the master controller. As a result, the master controller can be used for handling the transmission of control signals and data between the master and slave controllers; in addition, the master controller can be used as a buffer area for the common memory to control the slave controllers' states with automated management, specify the address of an MCU, and allocate memory blocks.

Finally, this article presents the entire very large-scale integration (VLSI) hardware circuit of the high-speed bridge controller according to our methodology (Fig. 3).

Smart Sensor Network through Modbus

This section presents the design of a Modbus-based SSN architecture with superior management performance. This system comprises

smart sensor nodes and a fieldbus master, both of which were realized using hardware; furthermore, the system involves a client monitoring program. In the system, Modbus protocol modules were used as the sensor network communication infrastructure.

In addition, an IIoT gateway was developed to integrate different protocols of the network layer and different interfaces of the device physical layer. It was adopted to improve the reliability of real-time communication. The function modules in the architecture were integrated into the design of a fieldbus master and an embedded database; an Internet access port is provided to a sensor.

SSN devices include multiple slave MCUs as subgateways and a set of field smart sensor nodes. A slave MCU is managed by a centralized network manager. It is responsible for the management, scheduling, and route creation of distributed network node devices with wired or wireless communication.

Implementation

The system architecture of the multi-MCU IIoT gateway comprises four major modules that are introduced below. The IIoT gateway architecture was developed and implemented for an IoT-based smart manufacturing application. The hardware prototype of the IIoT gateway is shown in Fig. 4.

As illustrated in Fig. 4, the prototype of the IIoT gateway system constructed in this study includes a reconfigurable FPGA bridge controller using a high-speed parallel architecture, a master networking for cloud module, a slave embedded lightweight database subsystem, and a slave SSN management subsystem including Modbus sensor networks.

The high-speed FPGA bridge controller forms the core, and controls and manages the interconnection and interaction with the bottom-perception-layer slaves as well as intercommunication and interoperation with the upper-application-layer master and slave MCUs; furthermore, it provides the data report and manipulates interfaces. In this study, the prototype of the FPGA bridge controller is implemented using the resources mentioned in Table 1. The slave IoT management subsystem was connected to multiple smart sensor array networks in the perception layer.

	High-speed bridge controller
System clock (max)	143.43 MHz
Device	10M08DAF484C8GES
Total logic element	2,942/24,624 (12%)
Total register	2188
Total pins	10/157 (6%)
Total PLLs	1/4 (25%)

TABLE 1. Resources used for implementing the high-speed bridge controller of the IIoT gateway. The numbers in brackets indicate device utilization.

The high-speed FPGA bridge controller forms the core, and controls and manages the interconnection and interaction with the bottom-perception-layer slaves as well as intercommunication and interoperation with the upper-application-layer master and slave MCUs; furthermore, it provides the data report and manipulates interfaces.

The Innovative Advantages Analysis of the Multi-MCU Gateway for the Smart Manufacturing System

This section presents a smart manufacturing system for Industry 4.0. In the era of IIoT, it is inevitable that smart manufacturing will transform current industrial manufacturing into Industry 4.0. This will reduce production and maintenance costs, improve production efficiency, and meet the requirements of flexible production. The establishment of a smart factory with high adaptability, high resource efficiency, and high automation without any production barriers can considerably improve the functionality, reliability, and safety of industrial manufacturing.

In this study, we integrated Modbus sensor networks with the multi-MCU gateway architecture to implement a smart manufacturing system with a cyber-physical system as its core. This cyber-physical system was combined with heterogeneous communication technology, distributed computing, sensors, and actuators.

As illustrated in Fig. 4, the controllers based on local computing use the received information (e.g., digital inputs and outputs; DI/DO, devices, sensors, actuators, and other diverse automation equipment) to change the behavior of the environment or physical systems.

Based on the above-mentioned objective of a smart manufacturing system of industrial IoT, the innovative advantages of the multi-MCU edge gateway improved technology proposed by this study have been analyzed as shown in Table 2.

Performance Evaluation

We validated the improvement in multi-MCU performance by comparing the performance with those of other industry-related Modbus gateway products (EKI-1224 [18], MB3480 [19]); in this study, we benchmarked the communication interfaces by transferring 256 bytes of data from the low-level perception layer through the gateway to the web server of the upper application layer.

In addition, we measured several performance indices, such as baud rate, power consumption, and response time of the multi-MCU system, so as to verify whether the proposed solution can meet the technology innovation indices described in Table 2. The results are shown in Table 3.

As shown in Table 2, the performance indices of the proposal solution are superior to those of other competing products in the market. This is because our study adopted three MCU serial communication high-speed bridge controllers and designed the multi-MCU gateway hardware, using the FSMC interface for communication between different MCUs, so the baud rated can be increased to 82.41 Mb/s.

In addition, this study adopted gateway hardware constructed with three MCUs of the same specification (max clock in 180 MHz; power consumption: STM32 F429 power support: ((5 V × 0.1 mA) × 3 = 1.5 W), which is without the extra operating system to prevent the piling up and switching of software stacks, as well as significant-

	Existing gateway technology	Proposed gateway	Advantages
IIoT gateway hardware solution	Adopts high-level embedded microcontroller system (MPU + embedded Linux). • e.g., Intel Quark X1020D (System clock: 400 MHz, Power consumption: 2.2W,) As a gateway solution, the cost is US$50. • Advantech EKI-1224 1-port Modbus Gateway [18] (Power consumption :5.2W)	Adopts gateway constructed with three MCU of the same specification (Max Clock:180Mhz, Power consumption: 0.9 × 3 = 2.7W) The costs will be reduced to below US$20.	High flexibility, scalability Low cost, power consumption
Fieldbus	Must be written by the developer basing on the demands.	With built-in Modbus; additional high level software function is not required.	High usability, adaptability, availability
Wireless Modbus Fieldbus	No	Realizes wireless Modbus master, and the device node implemented Modbus slave. The gateway has the management functions for both wireless and wired Fieldbus heterogeneous network.	High adaptability, availability
Smart management engine	No	Smart management engine with the Fieldbus device.	High adaptability, availability
Embedded Web server	Supports IPv4; requires operating system.	Supports IPv4 and IPv6, and operating system is not required. Can be run in MCU of low hardware resources such as one with 2MB Flash+ 256 KB SRAM inside.	High usability, adaptability Low cost, power consumption
Intelligent networking	Supports remote monitoring	Supports remote developing, deploying, and monitoring	High usability, adaptability

TABLE 2. Comparative analysis of proposed multi-MCU gateway technology.

Indices	Proposal solution	[18]	[19]
Baud rate	82.41 Mb/s	921.6 kb/s	921.6 kb/s
Power consumption	1.5W	5.2 W	4.6 W
Response time	10.8ms	30 ms	30 ms

TABLE 3. Comparison of performance indices with similar gateway products.

Communication interfaces	Time (ms)	Execution	Response time (ms)
FSMC	0.02485	6	0.1491
SPI	0.835	6	5.01
Modbus RS-485	2.68	1	2.68
Modbus RF 2.4 G	3	1	3
Total response time			10.8391

TABLE 4. Computation cost of total response time.

ly reducing the power consumption by adopting distributed computing. Furthermore, in terms of performance index for response time, a complete communication process involves polling by using the high-speed bridge controller to three MCUs and the reception of response messages returned from the DI/DO slave.

This study conducted the design of Modbus protocol based on the goal of performance optimization, reducing the response time of the Modbus slave node from the mainstream 30 ms to 10 ms (Table 4). The above-mentioned improvement of performance indices indicates that the multi-MCU gateway proposed by this study can achieve high reliability, real-time industrial communications, and task control of industrial IoT.

Implementation for the Smart Manufacturing System

The computer numerical control lathe is the most common machine tool for industrial manufacturing and precision machining. The stability of the lathe must be maintained to obtain high- precision processing and systematic manufacturing, which are key factors for achieving high-quality product manufacturing. This section introduces a combination of a machine tool and an SSN using various sensors to monitor the temperature variation of a lathe machine spindle, reduce the thermal error and vibration effects, and provide a protection mechanism for the machine.

Machine tools usually work in harsh industrial environments; thus, noise, electromagnetic interference, and other problems need to be considered. Therefore, the SSN must be designed and deployed carefully to ensure accurate interpretation by the sensors when monitoring the signal feedback for system abnormality.

Research conducted at the Precision Machinery Research and Development Center (PMC) reveals that because of the thermal expansion and contraction characteristics of metals, any lathe spindle temperature variation can cause shape or size deviations or surface roughness anomalies on the workpiece. Therefore, to ensure precision of the machine tool during long-duration processing, finding a method to monitor the spindle temperature variation is important; it can allow the machine to self-compensate for temperature deviations (Fig. 5).

To overcome the problem of lathe spindle temperature variation, as illustrated in Fig. 6, we

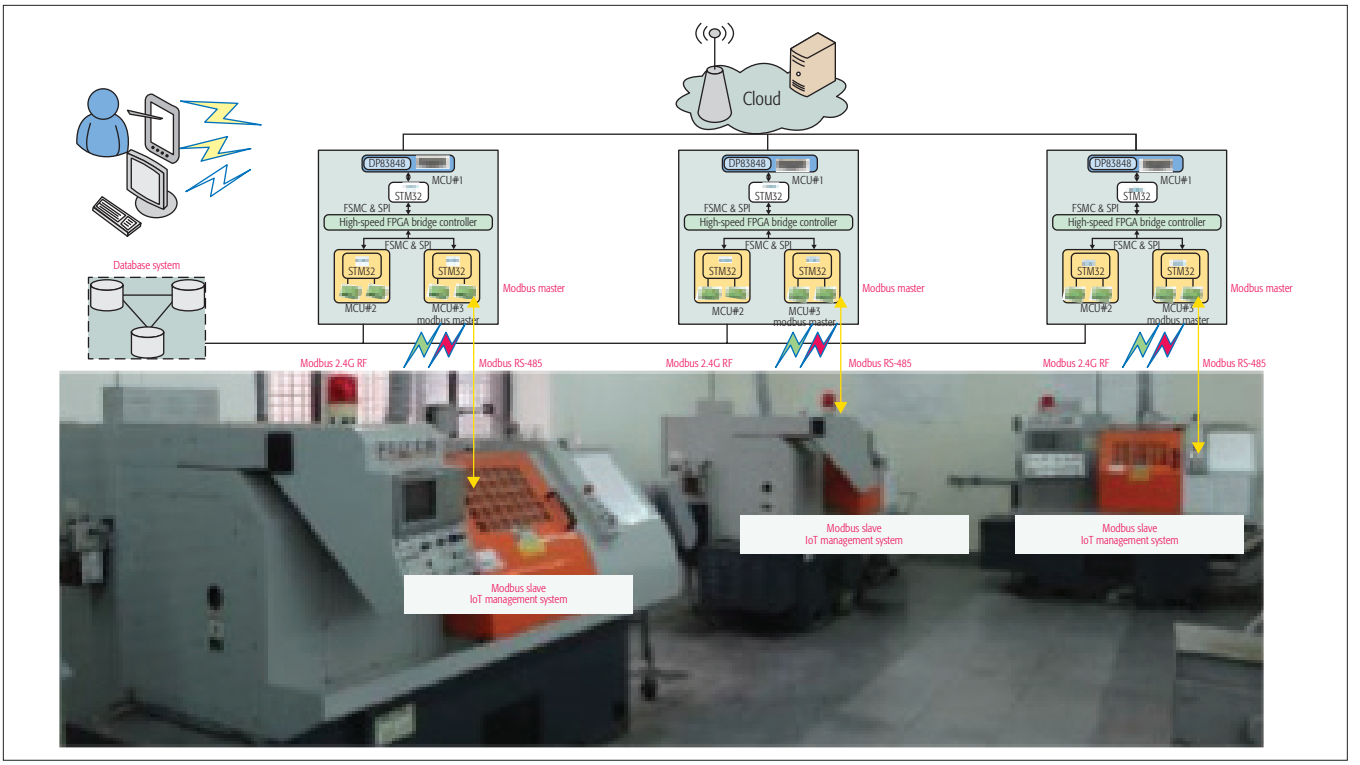


FIGURE 5. Application in smart manufacturing.

integrate 10 digital temperature sensors (SHT10) into a temperature sensor array to be installed on the inside and the outside of a machine tool to transmit temperature data through an RS-485 cable. Subsequently, we can study the relationship between temperature and thermal error from the data and use the self-compensation method to minimize the impact of thermal error on the workpiece through controlling a cutting fluid system for cooling and lubrication.

We can study the vibrations of the lathe spindle and machining chatter by using a 3-axis accelerometer (LSM303DLH) while measuring the vibration signals transmitted through the RF module to monitor the abnormal spindle vibration. By using a 10-bit high-resolution embedded software and a high-performance MCU, the sensor network can obtain the voltage sensitivity through calibration, and the measured vibration signals considerably improve the system's monitoring capabilities. In terms of mechanical interference, this study will integrate a MEMS audio sensor (MP45DT01) into the sensor to design an anti-collision and protection mechanism.

The IIoT gateway architecture was developed and implemented in an IoT-based smart machining system for industrial manufacturing. The hardware specifications of the IIoT gateway are described in detail in Table 5.

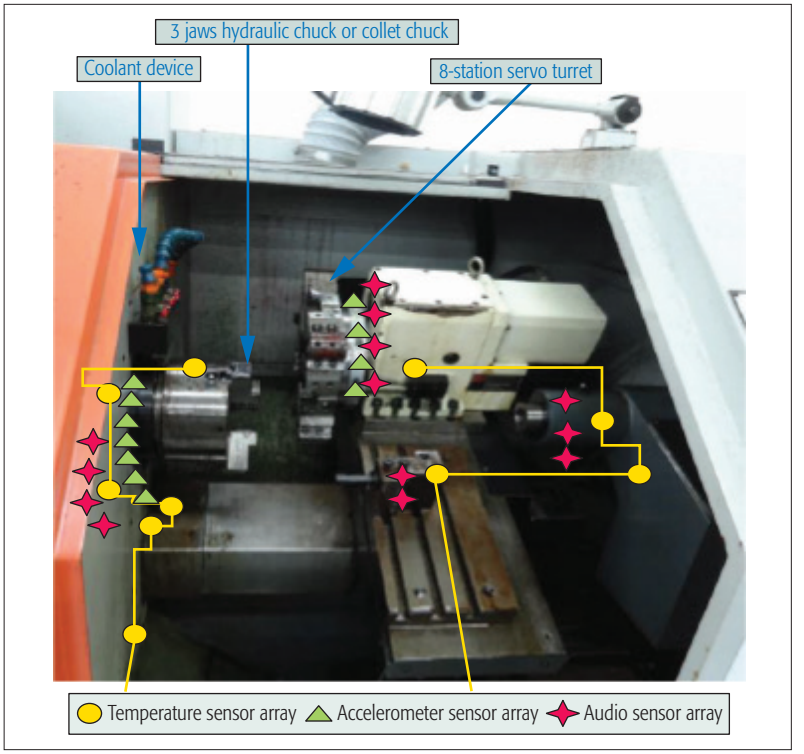


FIGURE 6. SSNs in the machine tool of a smart manufacturing system.

Application Analysis

The IIoT gateway comprises various smart sensor arrays. In addition to enhancing the operation of the machine tool, integrating the SSN into the machine tool prevents thermal error, machining chatter, and mechanical interference; moreover, by doing so, we can adjust the processing parameters automatically according to machine learning in the back-end system to improve the efficiency of machining, and make fault diagnosis and maintenance of the machine easier.

Because mechanical interference can easily cause a collision during the operation of the machine tool, the thermal error and machining chatter affect the yield rate during production, and the repair costs for the damage caused by collisions are very high, SSN monitoring can help

Through the local computing of the gateway, the IIoT system saves the bandwidth costs of transfer the data to the remote cloud servers and database systems, and its further feedback is to shorten the response time of M2M.

Hardware	Specification
Machine tool	Polygim PLG-42 CNC lathe
High-speed bridge controller	10M08DAF484C8GES
Master MCU	STM32F429ZI
Slave MCU	STM32F429ZI
Smart sensor node	ARM Cortex M4
3-axis accelerometer	LSM303DLH
3-axis magnetometer	LSM303DLH
3-axis digital output gyroscope	L3G4200D
Ambient light sensor	MAX44009
Barometer Pressure sensor	MPL115A
Temperature sensor	SHT10
Humidity sensor	SHT10
MEMS audio sensor	MP45DT01
RF module	nRF24L01
Ethernet controller	DP83848
Database	Secure Digital Card

TABLE 5. The hardware specifications of the IIoT gateway system.

overcome the safety problems of personnel and the machine tool. Moreover, it can save personnel and material resources indirectly and imperceptibly. The users can analyze and control the real-time data from the smart machining system to improve the power efficiency, performance, machine tool life, and mode control of the system.

Conclusion

This article presents the design of a novel multi-MCU IIoT gateway architecture. In this gateway, a high-speed parallel bridge controller was integrated into a multi-MCU hardware architecture, providing collaborative and local computation advantages. Through the local computing of the gateway, the IIoT system saves the bandwidth costs of transferring the data to the remote cloud servers and database systems, and its further feedback shortens the response time of machine-to-machine communication. In addition, the multi-MCU gateway architecture uses low-cost and low-clock MCUs to perform distributed and collaborative computing, reducing the power consumption of IoT systems. The designed IIoT gateway solves the high flexibility, scalability, and expandable peripherals services issues that a single MCU cannot achieve. Finally, an application of this solution to monitor an IoT-based smart machining system is presented.

References

[1] L Leurs, BR AG "Conversion of Fieldbusses Regarding Industrial Internet of Things" *ODVA, 2015 Industry Conference & 17th Annual Meeting*,

[2] I. Ungurean "Industrial Internet of Things with Data Distribution Service for Real Time Systems" *Int'l. Research J. Engineering and Technology*, vol. 02 no. 05 Aug 2015.

[3] J. Ren *et al.*, "Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing," *IEEE Network*, 2017. DOI: 10.1109/MNET.2017.1700030.

[4] Y. Zhang *et al.*, "A Survey on Emerging Computing Paradigms for Big Data," *Chinese J. Electronics*, vol. 26, no. 1, 2017, pp. 1–12.

[5] Z. Fadlullah *et al.*, "State-of-the-Art Deep Learning: Evolving Machine Intelligence Toward Tomorrow's Intelligent Network Traffic Control Systems," *IEEE Commun. Surveys & Tutorials*. DOI : 10.1109/COMST.2017.2707140.

[6] N. Kato *et al.*, "The Deep Learning Vision for Heterogeneous Network Traffic Control — Proposal, Challenges, and Future Perspective," *IEEE Wireless Commun*. DOI : 10.1109/MWC.2016.1600317WC.

[7] N. Bui *et al.*, "The Internet of Energy: A Web-Enabled Smart Grid System" *IEEE Network*, 2012, vol. 26, no 4, pp. 39–45.

[8] K. Xu, Y. Qu, and K. Yang, "A Tutorial on the Internet of Things: From a Heterogeneous Network Integration Perspective," *IEEE Network*, vol. 30, no. 2, Mar./Apr. 2016, pp. 102–08.

[9] F. Ernst, "Industry 4.0/Industrial Internet of Things-Related Technologies and Requirements for a Successful Digital Transformation: An Investigation of Manufacturing Businesses Worldwide"; SSRN 2698137, 2015.

[10] Y. Chen *et al.*, "Industrial Internet of Things-Based Collaborative Sensing Intelligence: Framework and Research Challenges," *Sensors* vol. 16, no. 2, 2016, pp. 1–19.

[11] M. Hartmann and B. Halecker, *Management of Innovation in the Industrial Internet of Things*, Budapest, 2015.

[12] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Comp. Net.*, vol. 54, no. 15, 2010, pp. 2787–2805.

[13] H.-D. Ma, "Internet of Things: Objectives and Scientific Challenges," *J. Comp. Science and Tech.*, vol. 26, no. 6, 2011, pp. 919–24.

[14] M. Jo *et al.*, "Device-to-Device (D2D) Based Heterogeneous Radio Access Network Architecture for Mobile Cloud Computing," *IEEE Wireless Commun.*, vol. 12, no. 3, June 2015, pp. 54–62.

[15] C.-H. Chen, M.-Y. Lin, and X.-C. Guo "High-Level Modeling and Synthesis of Smart Sensor Networks for Industrial Internet of Things," *J. Computers and Electrical Engineering*. DOI: 10.1016/j.compeleceng.2017.06.005.

[16] C.-H. Chen, M.-Y. Lin, and W.-H. Lin, "Designing and Implementing a Lightweight WSN MAC Protocol for Smart Home Networking Applications," *J. Circuits, Systems and Computers*, vol. 26, no. 3, Mar. 2017. DOI:10.1142/S0218126617500438.

[17] C.-H. Chen, M.-Y. Lin, and X.-C. Guo "High-Performance Fieldbus Application-Specific Integrated Circuit Design for Industrial Smart Sensor Networks," *J. Supercomputing*, Mar. 2017. DOI:10.1007/s11227-017-2010-1.

[18] Advantech Co., Ltd., Advantech EKI-122X Series Modbus Gateway User Manual, July 2010; http://www.bb-elec.com/Products/Manuals/ADAM-4572_EKI-1221122212241221D1222D-Manua-(1).pdf.

[19] Moxa Co., Ltd., Moxa MB3480 4-port standard serial-to-Ethernet Modbus gateways, June 22, 2017; https://www.moxa.com/doc/specs/MGate_MB3180328034 80.pdf.

Biographies

Ching-Han Chen received his D.E.A and Ph.D. degrees in 1992 and 1995 from Franche-Comte University, France. He was an associate professor in the Department of Electrical Engineering, I-Shou University from 1995 to 2006. Since 2006, he has been an associate professor in the Department of CSIE, National Central University, Taiwan. His research interests include embedded systems, machine vision, and robotics.

Ming-Yi Lin received his M.S. degree from the Department of Computer Science and Engineering, Yuan-Ze University, Taiwan, R.O.C., in 2011. He is currently pursuing a Ph.D. degree in the Department of Computer Science and Information Engineering at National Central University. His research interests include embedded systems, wireless sensor networks, and the Internet of Things. He received his Ph.D. degree in computer science from National Central University in 2016. He is now a research

assistant in the Department of CCE, Army Academy, Taiwan.

CHAO-TSU LIU received his B.S. degree from National Yunlin University of Electronic Engineering and his Master's degree in computer science from National Central University in 2000 and 2012 , respectively. He is now a technical marketing engineer at Cavium, Inc. His research interests include embedded systems, RF protocol, and image processing.