Field-ubiquitous Computing

Application of IPv6 to Field Instruments level network and Virtual Wiring Technology

OKABE Nobuo [*1]

The changes in social environment, such as globalization of enterprise activities, depletion of natural resources, and eco-oriented movement will affect the structure of mass production. Control systems require flexibility and scalability in both size and function to adjust to the changes. Our goal is to free the systems from the controller-centric model where all field instruments must be accessed via controllers, as well as to achieve flexibility and scalability with the latest network technologies. The author proposes a virtual wiring technology, which consists of a network security mechanism and a plug-and-play mechanism. This technology can be applied to resource-limited devices such as field instruments. This paper describes our activities toward creating the virtual wiring technology.

INTRODUCTION

The changes in social environment, such as globalization of enterprise activities, depletion of natural resources, and eco-oriented movement will affect the structure of mass production. Control systems must be prepared with flexibility and scalability in both size and function to adjust to the changes. On the other hand, the further development of computer technology and communication technology is expected to lead to the commoditization of distributed computing technology. In order to realize the flexibility and scalability required for control systems within a reasonable time and cost, commoditized technologies should be utilized effectively.

As shown in Figure 1, with existing control systems, every access to a field device is through a controller, and so the controller acts as a bottleneck to performance, functionality and cost. In this paper, we call this the "controller centric model."

In contrast, as shown in Figure 2, networks simplify the role of a controller to its intrinsic functions and make it easy to add functions. Furthermore, high-speed broadband network technologies reduce many input-output cables and enable the emergence of intelligent devices by consolidating numerous input-output ports.

In this paper, we propose a virtual wiring technology to free the system from the controller centric model and create a flat network architecture as shown in Figure 2.

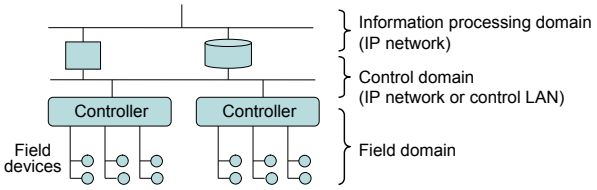

Figure 1 The architecture of existing control systems

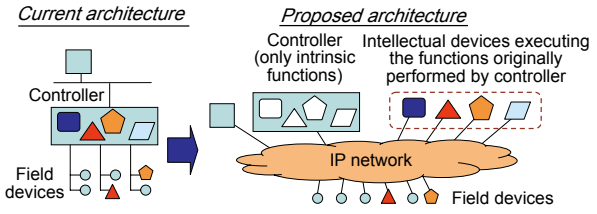

Figure 2 Proposed flat architecture

*1 Ubiquitous Field Computing Research Center, Corporate R&D Headquarters

There are several restrictions for realizing such network architecture, the most severe of which is the limited computational resources (CPU power, memory size, etc.). The power to field devices often must be supplied through signal lines. Also, with restrictions such as IEC60079, the amount of electric power consumed at hazardous locations such as where flammable gas exists must be minimized. For these reasons, the amount of electric power consumed by field devices is limited, and so computational resources are also inevitably restricted.

This paper introduces virtual wiring technology for application to devices whose computational resources are restricted.

VIRTUAL WIRING TECHNOLOGY

When configuring a network over the field domain, physical signal lines used to connect controllers and devices need to be made virtual. That is, a controller has to identify the proper one from the group of devices distributed over the network and establish a virtual wiring connection with the identified device. In this paper, we call this virtual wiring connection "virtual wiring."

We achieve this virtual wiring by combining our original network security mechanism with plug-and-play as described below. The former can be applied to devices with limited computational resources unlike usual security mechanisms, while the latter provides secure and autonomous automated configuration for devices with limited computational resources.

Network security mechanism

Currently, many types of network security for control systems rely on a firewall model. Since the model premises a specific network topology, it is difficult to apply to cases where the network topology cannot be predetermined such as in wireless and mobile communication. On the other hand, the network security mechanism proposed in this paper protects End-to-End communication with IPsec (Security Architecture for Internet Protocol) [1] as shown in Figure 3. Since IPsec ensures security independently from the application, it hardly affects existing applications and is suitable for long-lasting industrial systems.

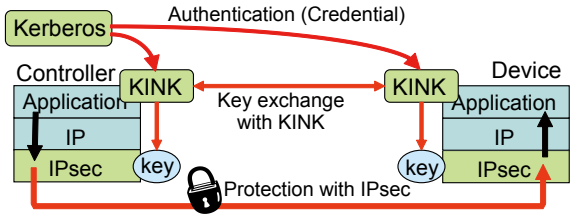

Figure 3 Network security mechanism using KINK and IPsec

IPsec requires both communicating ends to share confidential information. Since devices installed in the field do not have a powerful user interface like a PC, manual key setting is difficult and auto-setting called "key exchange protocol" is necessary. Because existing IPsec key exchange protocols such as IKE (Internet Key Exchange) [2] require public key cryptography, its application to devices with limited computational resources has been difficult. We therefore decided to adopt the IPsec key exchange protocol, KINK (Kerberized Internet Negotiation of Keys) [3], which was developed and standardized as an international standard by us. KINK is based on the Kerberos Authentication System and does not require public key cryptography.

Plug-and-play mechanism

A control system consists of many controllers and devices. Conventionally, each of them has to be configured and connected with an input-output cable, which takes time and effort. Although a network can reduce such work, controllers have to deal with input-output cable virtually. That is, a controller has to identify the proper one from the group of devices distributed over the network, and establish a virtual wiring connection with the identified device. In this paper, we propose a method of establishing virtual wiring utilizing the plug-and-play mechanism [4], [5] which we have proposed. From the perspective of security, it is difficult to apply existing plug-and-play technology, such as Jini [6] and UPnP (Universal Plug and Play) [7], to devices with limited computational resources. On the other hand, since the proposed plug-and-play technology is based on the network security mechanism described above, it can be applied to such devices. The sequence called "Chain of Trust" indicated in Figure 4 enables virtual wiring.

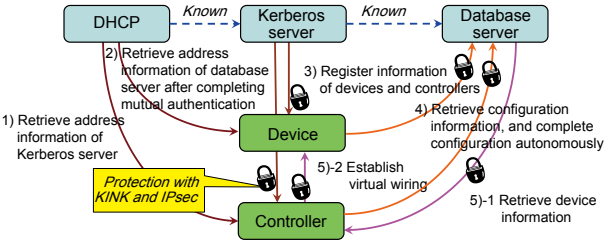

Figure 4 Virtual wiring sequence with chain of trust

1) DHCP (Dynamic Host Configuration Protocol) broadcasts address information of Kerberos server.
2) Devices and controllers confirm whether they belong to the broadcast Kerberos server or not. When confirmed, mutual authentication between Kerberos server and devices/controllers is completed. Devices and controllers then obtain the address information of the database server from the trusted Kerberos server.
3) Devices and controllers register their own information to the trusted database server.
4) Devices and controllers trust the configuration information provided by the trusted database server. With this configuration information, devices and controllers autonomously complete the configuration.

5) Based on the information provided by the database server, controllers establish virtual wirings with the devices to be controlled.

Even though controllers and database servers are assigned to different entities, controllers can find the database server which they trust by the sequence 1) and 2) above. Usually, a control system consists of multiple controllers distributed over a network, but with the sequence 3) and 4), controllers can configure themselves autonomously.

Evaluation by prototype

We have evaluated the feasibility through the prototype of the proposed mechanism. We implemented functions including HSE (High Speed Ethernet) of FOUNDATION Fieldbus (hereinafter referred to as FF) in the prototype. Table 1 shows the configuration of the prototype and the object code sizes of implemented modules. The total object code size of the initial version partly utilizing open source was more than one megabyte, but with optimization of specifications and implementation, it was reduced to 270 Kbytes. Especially, we successfully reduced the size of the KINK part to one fifth of the original one.[8] To reduce the code size further and increase the speed, we are now investigating using hardware to cover the IP/IPsec part which accounts for almost half of the entire code.

Table 2 shows the processing time of the prototype. Because the overhead for virtual wiring processing is required only at the time of system start up, the penalty for automating the configuration of each device is considered to be sufficiently small. On the other hand, the key exchange processing is required not only at the time of system start up, but also at the time when the shared confidential information expires. However, since the amount of communications between controllers and devices is not so much, the influence caused by the key exchange processing can be suppressed by extending the valid time limit (for example, for a few weeks) or in other ways.

Table 1 Component and object code size of the prototype

Classification	Component	Source	Object code size (Kbyte)
Hardware	CPU	H8/3029	-
Software	RTOS	iTRON	-
	IPv4/IPv6	Original	132
	IPsec	Original	15
	KINK	Original	45
	FF HSE	Original	80
	Total		272

Table 2 Processing time of the prototype

Processing	Processing time (msec)
Virtual wiring processing	511
KINK key exchange processing	65

SUPPLYING POWER TO DEVICES AND INSTALLING THEM AT HAZARDOUS LOCATIONS

The last one hop is always a challenge for the network. A part of the field domain environment susceptible to fire is called a “hazardous location.” Since communication traffic increases along with networking of the field domain, the performance of the data link in hazardous locations must be improved. However, Ethernet itself cannot satisfy the regulation for hazardous locations. Also, it is impossible to supply power to field devices through standard Ethernet.

Table 3 shows the characteristics of FF H1, the data link which can be used in hazardous locations and can supply power, and Ethernet. If FF H1 is to be expanded to improve the performance of the data link, the improvements of FF H1 in bandwidth, maximum transmission unit and full/half duplex are required in order to transmit relatively large packets as IP does. At the same time, the features of supplying power through a cable, maximum cable length and low power consumption conforming to the regulation for hazardous locations, must still be provided.

Figure 5 indicates the current data link and the topology proposed in this paper. To improve the performance of the data link, it is effective to exclude the bus configuration and restrict to a P2P (Point-to-Point) configuration like Ethernet. The simplified topology helps to simplify the wiring design. Even though the topology of the data link is restricted to P2P, an Ethernet switch provides the capability equivalent to the existing multi-drop data link.

When considering the latest Ethernet physical layer (PHY), high bandwidth is not a major factor of power consumption as shown in Table 3. However, it is clear that just applying Ethernet technology is not enough to achieve the maximum cable length equivalent to FF H1.

Table 3 Comparison between FF H1 and Ethernet

Items	FF H1	100B-T Ethernet
Topology	Bus	Bus, P2P
Bandwidth	32 Kbps	100 Mbps
Maximum Transmission Unit (MTU)	256 byte	1500 byte
Full / half duplex	half duplex	full duplex
Maximum cable length	1.9 km	100 m
Power consumption at physical layer	100 mW	150 mW

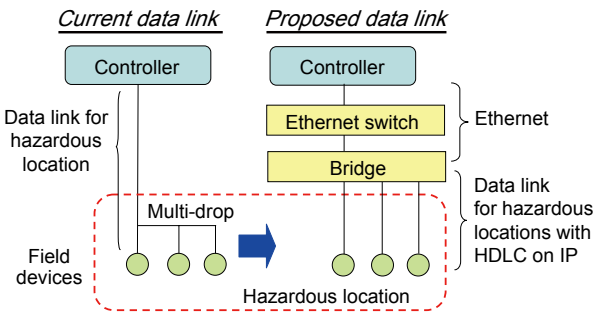

Figure 5 Data link topology at hazardous locations

Figure 6 shows the evaluating system including the prototype bridge for the data link layer to verify the function described above and the prototype device described in the "Evaluation by prototype" section. This evaluating system has the following features.

1) By improving encoding and other technologies, the communication bandwidth has been widened to about 8 times that of the original one (from half duplex 32 kbps to full duplex 128 kbps) while maintaining the equivalent electrical characteristic and maximum cable length of existing FF H1. This means that it can be used at hazardous locations under the constraint of the FISCO (Fieldbus Intrinsically Safe Concept) model based on IEC60079-27.[9]
2) Direct transfer of IP packets is enabled using HDLC (High-Level Data Link Control).
3) Power supply capability is provided like FF H1.

With this bridge, controllers and devices located at hazardous locations can directly exchange IP packets. We are now investigating ways to increase the performance and the reliability.

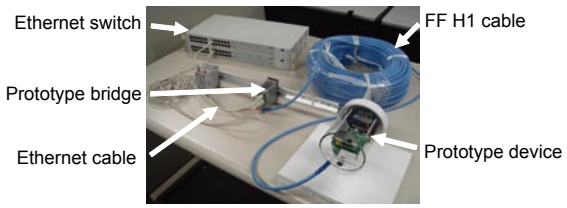

Figure 6 Evaluation system including prototype bridge and device

CONCLUSION

To prepare for major changes in production systems in the future, it is necessary to move control systems away from the controller centric model and to provide them with flexibility and scalability in both size and function. As a basic technology to realize this, we proposed virtual wiring technology in this paper, which offers the following advantages.

- Secure networking in the field domain
- Freeing controllers from a bottleneck to performance, functionality and cost
- Reduction in number of ports and wires in the field domain
- Reduction of engineering works for the field domain

An evaluation using the prototypes showed that these advantages can be realized within feasible code size and performance.

In order to extend networking into the field domain, it is necessary to improve the performance of the data link used in hazardous locations. In this paper, we described an initial prototype of a new data link for solving such issues and indicated that the performance can indeed be improved.

REFERENCE

(1) S. Kent, K. Seo, "Security Architecture for the Internet Protocol," IETF RFC4301, 2005, pp. 101
(2) D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)," IETF RFC2409, 1998, pp. 41
(3) S. Sakane, K. Kamada, et al., "Kerberized Internet Negotiation of Keys (KINK)," IETF RFC4430, 2006, pp. 40
(4) N. Okabe, S. Sakane, et al., "Secure Plug and Play Architecture for Field Devices," Proceedings of 5th IEEE International Conference on Industrial Informatics (INDIN2007), 2007, pp. 873-878
(5) N. Okabe, S. Sakane, et al., "Implementing a Secure Autonomous Bootstrap Mechanism for Control Networks," The IEICE Transactions on Information and Systems, Vol. E89-D, No. 12, 2006, pp. 2822-2830
(6) Sun Microsystems, "Jini Specifications Archive - v2.1," Sun Microsystems, Inc., 2005, http://www.jini.org/
(7) UPnP Forum, "UPnP Device Architecture 1.0, Version 1.0.1," UPnP Forum, 2003, http://www.upnp.org/
(8) Kazunori Miyazawa, Shouichi Sakane, et al., "Designing and Implementing of Kerberos Version 5 for Embedded Devices," Proceedings of Embedded Systems Symposium (ESS2007), No. 2007-8, IPSJ Symposium Series, 2007, pp. 168-175, in Japanese
(9) Kaoru Onodera, "FOUNDATION Fieldbus Explosion Protection Systems in Japan," Yokogawa Technical Report, Vol. 51, No. 2, 2007, pp. 69-70 in Japanese

* "FOUNDATION Fieldbus" is the registered trademark of Fieldbus FOUNDATION.