# Strong Security Measures Implemented in ISA100.11a Wireless System

*Kinichi Kitano* [*1]    *Shuji Yamamoto* [*1]

***From the beginning, Yokogawa has been participating in standardization and dissemination of ISA100.11a, a wireless communication standard for industrial automation advocated by the International Society of Automation (ISA), and has been expanding its product portfolio with conformance to this standard. Although field wireless standards including ISA100.11a are being introduced into plants widely, security is still one of the major concerns. This paper introduces the security measures of ISA100.11a and Yokogawa's efforts to enhance plant security.***

## INTRODUCTION

The introduction of wireless systems into plant sites is growing. Unwiring field devices brings various merits that are not available in wired systems. They include the reduction of costs for signal and power cables, shortening of installation time, measurement at high places and isolated places where wiring is physically and economically prohibitive, measurement at rotating or moving points, and temporary measurement during maintenance shutdown. Because of these merits, wireless systems are highly anticipated in the field.

When introducing field wireless, security is often pointed out as an essential requirement, like reliability of communication. However, the inherent features of wireless communication such as invisibility and uncertain communication ranges are a concern. In addition, due to lack of technological understanding, some people are confusing it with wireless LAN and misunderstanding that it has the same vulnerabilities as wireless LAN.

The ISA100.11a wireless standard [(1)], the dissemination of which Yokogawa has been promoting, was established based on user requirements, and its specifications were drawn up with priority on reliability and security from the beginning. Not only experts in wireless and instrumentation but also those in security participated in creating its specifications, and so robust security technologies were incorporated into this field wireless protocol.

This paper introduces known threats to wireless systems in general, and then describes security measures offered by ISA100.11a and Yokogawa's efforts regarding security.

## CONFIGURATION EXAMPLE OF CONTROL SYSTEM

Figure 1 shows a configuration example of a control system based on the ISA100.11a.

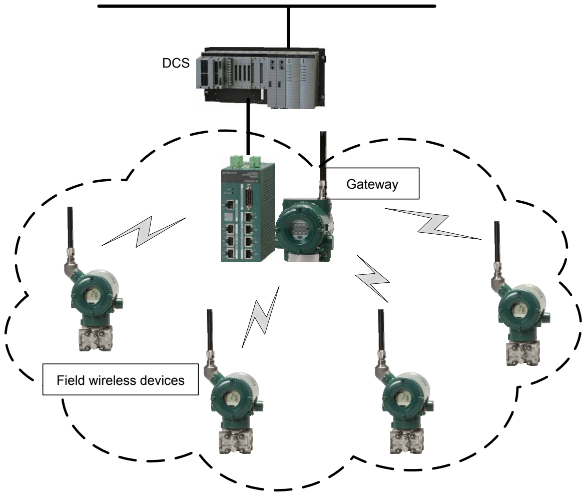

**Figure 1** Configuration example of a control system

The gateway manages the communication between ISA100.11 field wireless devices and a host system such as distributed control systems (DCS). In addition, the gateway includes a system manager that manages ISA100.11a communication, such as communication scheduling and determination of communication routes, and a security manager that is responsible for security management, such as authentication of field wireless devices and management of encryption keys.

[*1] Business Initiative Department, New Field Development Center, IA Platform Business Headquarters

## THREATS TO SECURITY OF FIELD WIRELESS SYSTEMS

The data handled in field wireless systems includes operation data such as process values and manipulating values, manufacturing data such as production volume and transaction volume, and management data of wireless systems such as communication status and system configuration information.

The following threats are generally known as those to the security of field wireless systems that deal with such important information.

- Sniffing
- Data falsification
- Spoofing
- Replay attack

### Sniffing

Sniffing involves a malicious third-party that intercepts the communication and tries to steal the contents of the communication.

If a malicious person steals data from the communication in some way, manufacturing know-how, production volume, and other business-related data are likely to leak out. In addition, leaked administrative data for a wireless system may give the person a hint as to how to illegally access the system.

Even if the data itself have no value, the disclosure through the Internet and other media about the leakage may make both system providers and users lose social credibility.

### Data falsification

Data falsification involves a malicious third-party that monitors communication and intentionally changes its contents.

If process values or manipulating values are used without knowing that they have been maliciously falsified, it can deteriorate the quality of products, cause damage to manufacturing facilities, and even endanger human life due to abnormal outputs

### Spoofing

Spoofing involves a non-authenticated device that behaves in the network as if it is authenticated.

Wireless field devices and gateways can be targets of spoofing. If a malicious device mimics a proper wireless field device, it can send wrong process values to a host system. If a malicious device mimics a proper gateway, it can send wrong manipulating values to field devices such as valves and actuators.

### Replay attack

A replay attack is a special type of spoofing in which communication packets are recorded, and later the recorded packets are sent. A replay attack is characterized in that it can make an attack without cryptanalysis.

Some field wireless standards do not offer a defense mechanism against this attack. In such case, a possible attack and its results are supposed as follows:

A wireless gateway sends an open command to an actuator of a valve. The actuator opens the valve because the command is from the valid gateway. An adversary intercepts and records the communication and later replays the communication. Because the actuator cannot distinguish whether this communication is from the gateway or the adversary, the actuator opens the valve. That is how an adversary can operate a valve at an unexpected time.

## SECURITY FUNCTIONS OF ISA100.11A

To prepare for those threats described above, the security functions of the ISA100.11a are designed so that they satisfy the following requirements.

- Message authentication ensures that messages received are originated by a valid device and have not been modified by an outside, rogue entity.
- Guaranteed data confidentiality through state-of-the-art encryption
- Offer protection means against replay attacks.

To satisfy these requirements, the following security technologies are incorporated into the ISA100.11a.

- Device authentication
- Encryption
- Message authentication
- Freshness of communication messages

Some papers have reported that the ISA100.11a offers more robust security than other field wireless protocols. [(2), (3)]

### Device Authentication

Preventing a spoofing device from joining a network is the linchpin of a secure wireless network. The security of ISA100.11a is based on the assumption that  an authenticated gateway shares a secret key only with a valid device. Encryption and data encryption and falsification-prevention depends only on an authenticated gateway and devices that share a secret key. In case an adversary gets a secret key, a gateway cannot distinguish between data from a valid device and data from a false device.

As counter-measures for a false device and a false gateway, ISA100.11a introduces a provisioning, which is a mechanism for sharing an authentication key, and necessitates mutual authentication between a gateway and a device using an authentication key. When a gateway and a device succeed in mutual authentication, both sides generate a secret key.

This authentication key is called a joining key. Infrared communication is used for a device provisioning. The limited transmission range of infrared communication offers secure data transfer. Figure 2 shows a provisioning; an infrared adapter is placed less than 30 cm from a device.

A join key in a device cannot be read back. A different join key is generated for each provisioning; every device has a different join key. The join keys are stored in a file and this file is downloaded into a gateway.

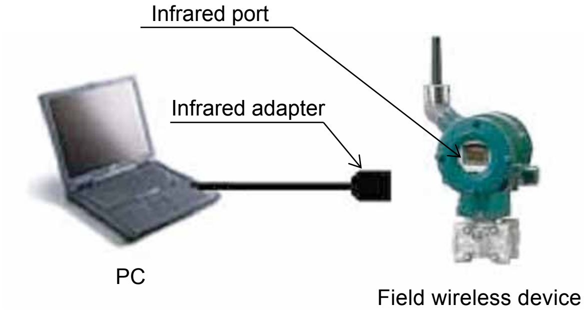

**Figure 2** Example of provisioning of a device

Authentication during the joining process uses an authentication mechanism called challenge-response. Challenge-response authentication offers good security because an authentication key is not sent over the network. In challenge-response authentication, one party presents a question (“challenge”) and another party must provide a valid answer (“response”) to be authenticated. A challenge-sender calculates a response by itself and compares a response from another party. If the responses match, the sender determines that another party shares the authentication key and is a valid one. In ISA100.11a protocol, a join key is an authentication key.

Figure 3 shows the mutual challenge-response authentication of ISA100.11a. The device generates a challenge $C_A$ from a pseudo random number and a join key. The gateway generates a response $R_A$ corresponding to the challenge. The device generates a response by itself and compares it with the response from the gateway. If the responses match, the device determines the gateway is valid. The device generates a challenge $R_B$ from $R_A$. The gateway generates a response by itself and compares it with the response from the device. If the responses match, the gateway determines the device is valid. That is how a device and a gateway mutually authenticate in ISA100.11a.

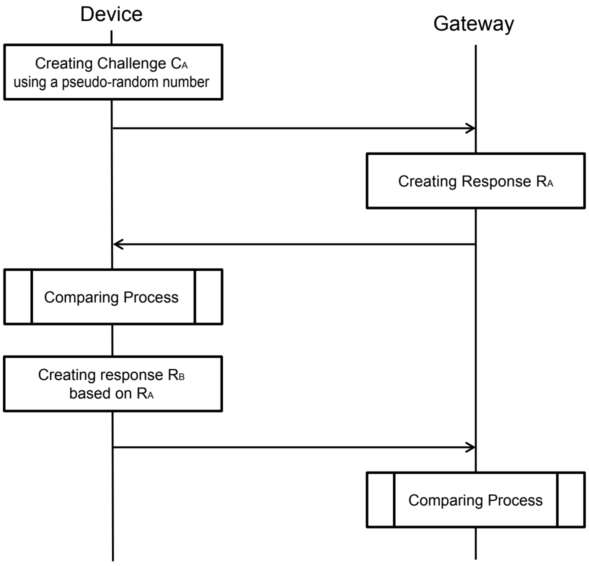
Device
Gateway
Creating Challenge CA using a pseudo-random number
Creating Response RA
Comparing Process
Creating response RB based on RA
Comparing Process

**Figure 3** Mutual authentication by challenge response authentication

**Encryption**

Encryption is an effective countermeasure against sniffing. Even if wireless communication is monitored, it is impossible to extract effective data from encrypted messages.

The ISA100.11a uses the Advanced Encryption Standard(AES) as an encryption algorithm. AES is the encryption standard in the U.S. and is adopted as a standard in the EU. This robust algorithm is proven in financial institutions and electronic commerce.

At the moment, no cryptanalysis is found other than brute force attack for AES. An effective countermeasure against brute force attack is to use a long key. Thus, the ISA100.11a uses a 128-bit key. Its combination is $3.4 \times 10^{38}$, and it takes a billion years for a billion sets of the up-to-date fastest supercomputers to break the code [4].

In 2011, several news sites reported that AES was cracked, but actually the attack just makes a brute force attack four times easier than before [5]. According to the calculation above, it still takes two hundred and fifty million years with a billion sets of the fastest supercomputers.

Furthermore, encryption keys are periodically updated by the security manager. Therefore, even if an encryption key is decoded by a brute force attack, the encryption key is no longer used at that time. In addition, encryption keys differ for each device. Decoding efforts by a brute force attack for several hundreds of millions of years can obtain only the content of the communication of a specific device for several days.

**Message Authentication**

Message authentication is a mechanism for checking that messages are from proper partners and not falsified. This is achieved by message authentication codes that only the device knowing the encryption key can create and that is embedded in messages. That is, if the code in a message differs from that created by the receiver, the receiver judges that the message is from those who do not know the encryption key or falsified, and discards it.

Early wireless LAN systems used checksums for detecting communication errors. Because the checksum is calculated based only on the content of the message, it is impossible to detect falsification if both the message and checksum are altered. The message authentication code introduced into the ISA100.11a is greatly effective for preventing falsification.

**Freshness of Communication Messages**

An effective countermeasure against replay attacks is to introduce the concept of freshness into communication messages. In this concept, only messages received within a certain period of time after their transmission are accepted.

Each device in an ISA100.11a wireless network synchronizes time with each other in the order of milliseconds, and adds current time information to transmitting messages. Receivers judge the appropriateness of the transmission time by seeing the added time information.

## EFFECTS OF SECURITY FUNCTIONS

Table 1 below shows which function provided by the ISA100.11a is effective to known threats to security of field wireless systems in general.

**Table 1** Effect of security functions of ISA100.11a

| Functions / Threats | Device authentication | Encryption | Message authentication | Freshness of communication messages |
|---|---|---|---|---|
| Sniffing | ✓ | ✓ | ✓ | — |
| Data falsification | ✓ | — | ✓ | — |
| Spoofing | ✓ | — | ✓ | — |
| Replay attack | — | — | ✓ | ✓ |

Device authentication, message encryption, message authentication, and message freshness in combination achieve tight security. If any of them are missing, a protocol would offer weaker security. For example, if a message is encrypted without message authentication, a receiver cannot distinguish if a message is valid. If a network doesn't use device authentication, an encrypted message without device authentication cannot guarantee that the message is from a valid party. If a message is without freshness, a receiver cannot distinguish whether it is a valid message or an old valid message replayed by an adversary.

## YOKOGAWA'S EFFORTS TOWARDS SECURITY

Adopting a secure communication protocol alone does not always ensure a robust wireless system. Developing a security-conscious product and ensuring that the product is implemented as intended are also required.

Yokogawa conducts the following measures during product development

- Assessing security risks of products during design.
- Training programmers on coding not to introduce vulnerabilities
- Verifying source codes by using analysis tools to detect problems in security

Even with these measures, vulnerabilities from implementation errors or false assumption may still be introduced. We collaborate with subject matter experts within and outside Yokogawa for detecting vulnerabilities by assessing our finished product.

To show the security requirements of the IEC62443 have been satisfied, Yokogawa considers that acquisition of the ISASecure Embedded Device Security Assurance (EDSA) certification is important.

## CONCLUSION

This paper has introduced security threats to Yokogawa field wireless systems and countermeasures against these threats. ISA100.11a has implemented security measures based on lessons learned from early wireless LAN. This means that devices conforming to the ISA100.11a are inherently immune to those known security vulnerabilities.

Although security technology and tools against security threats are steadily progressing, technology and tools of attackers are also progressing. Advancements in technology may suddenly make the attacks, which had been considered impossible from viewpoints of cost and processing time, realistic. Yokogawa never stands still and strives to enhance its system security.

## REFERENCES

(1) ISA-100.11a-2011, Wireless system for industrial automation: Process control and related applications

(2) Gengyun Wang, Comparison and Evaluation of Industrial Wireless Sensor Network Standards ISA100.11a and WirelessHART, Master of Science Thesis, Communication Engineering, 2011

(3) Cristina Alcaraz, Javier Lopez, "A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, Vol. 40, Issue 4, 2010, pp. 419-428

(4) Mohit Arora, "How secure is AES against brute force attacks?," EE Times, 2012, http://www.eetimes.com/document.asp?doc_id=1279619

(5) Andrey Bogdanov, Dmitry Khovratovich, Christian Rechberger, "Biclique Cryptanalysis of the Full AES," Advances in Cryptology – ASIACRYPT 2011, Vol. 7073, 2011, pp. 344-371