Review Article
Volume S1, 2021
DOI: 10.37421/bset.2021.S1.008

Journal of Biomedical Systems & Emerging Technologies

ISSN: 2090-5092 Open Access

The Network Structure of BEMS and Cyber Security

Takeji Toyoda*

TOYODA SI PE Consultant, D-111 Yokohama Parktown, 3-76-3 Mutsukawa Minami-ku, Yokohama, Japan

Abstract

This paper describes on the recent trends of network structure of BEMS (Building and Energy Management System) and measures of BEMS against the risks of cyber-attacks. The network of BEMS consists of three networks, such as internet, main network and field networks which are work together to cooperate with each other. By having the linkage to internet, BEMS becomes to have the risks from cyber-attacks. This paper describes how to reduce the risks of cyber-attacks to BEMS.

This paper explains the network configuration of BEMS and the devices subject to cyber risk, and the contents of cyber-attacks on these devices and the basics of countermeasures (cyber security). The following three requirements as the basis of security control as a cyber-security measure of BEMS are described.

1. Connect only to trusted parties.

2. Connect only to reliable devices / devices.

3. Implementation of anti-virus measures.

The detail of specific contents of implementing these three requirements in BEMS are also explained. Cyber risk countermeasures are an indispensable technology in the digital society of the future, and effective and highly effective economic cyber risk is desired.

Keywords: BEMS • Network • BACnet • Cyber security • IEC62351 • Security control

Introduction

BEMS is an abbreviation of Building and Energy Management System and has been defined by SHASE (the Society of Heating Air Conditioning and Sanitary Engineers of JAPAN). The purpose of BEMS is to realize the most suitable environment, saving energy and carbon in the building and it's area by controlling the facilities of building such as electricity, lighting, air conditioning, sanitary and firefighting system. The functions of BEMS are same as BACS (Building Control and Automation System) which is defined in the series of ISO16484. BEMS is traditionally familiar as BAS (Building Automation System). Today, BEMS has become a powerful infrastructure in a building by utilization of various network technologies such as ICT, IoT and AI. Because BEMS is the devices centered on electronics, the countermeasure is important under the threat of noise in electromagnetic and electrostatic environments. Ensuring the security of INTERNET-connected BEMS against cyberattacks is an important issue. In this paper, requirements and countermeasures for cybersecurity in network facilities centered on BEMS are explained [1,2].

Network Structure of Bems

The outline of BEMS

(Figure 1) shows an example of the basic structure of BEMS inside and outside of the building. As shown in (Figure 1), the BEMS consists of a central device (B-OWS: BACnet Operator Work Station) including of a high-function pc server, display device, printer, and other peripheral devices, and an autonomous distributed sub controller (B-BC: BACnet Building Controller) installed in each facility or area, mainly on the core network by TCP/IP (Transmission Control Protocol /Internet Protocol) and UDP/IP (User Datagram Protocol /Internet Protocol). Each B-BC also functions as a gateway (GW) and is connected to various subordinate remote terminals (RS: Remote Station) through a field network. Each RS connects to various equipment managed by BEMS (corresponding to "things" of IoT) and executes information input / output (PI / O) and local control with the equipment. In addition, the main network connects to the Internet through GW and executes services and controls in cooperation with the outside of business establishments such as buildings. RS connects to various equipment managed by BEMS (corresponding to "things" of IoT) and executes information input / output (PI / O) and local control with the equipment. That is, the main network of BEMS connects to service providers (ASP: Application Service Provider), aggregators, BEMS and administrator PCs of other buildings, and contract consumer PCs via the Internet, and exchanges various information held by each of them via the Internet. The scope shown as IT in (Figure 1) is a part of B-OWS and the cloud side on the Internet, and performs services such as cloud communication, data management, analysis, processing, commands, and data display on the energy dashboard. It is a virtual world that can be regarded as IT (Information Technology) related processing. The range indicated by OT is for device-to-device communication, hardware interface, sensing, data collection, control, etc. It is a real world with

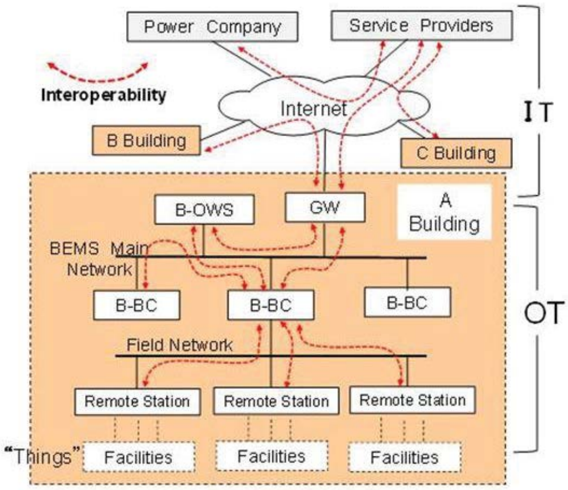

Figure 1. Basic structure of BEMS with internet.

**Address for Correspondence:* *Takeji Toyoda, TOYODA SI PE Consultant, D-111 Yokohama Parktown, 3-76-3 Mutsukawa Minami-ku, Yokohama, Japan, E-mail: Toyoda.si.tt@gmail.com*

Received 15 September 2021; **Accepted** 30 September 2021; **Published** 07 October 2021

OT (Operation Technology) related processing. It can be considered that a digital twin is composed by the fusion of OT and IT in BACS.

Open System of BEMS

In information processing systems such as computer systems, openness is a system that allows products from different vendors to be freely combined by using software and hardware that comply with the published specifications. In BEMS, each device made by different vendors such as B-OWS, B-BC, and remote terminals (RS) connected to each network in (Figure 1) are based on a common communication protocol, and interoperability between devices is established. Interoperability has been established to share information and work together. In the BEMS, a multi-vendor environment is realized by using open communication protocol such as TCP / IP and BACnet, and it is possible to economically select the best vendor for the required functions of each device and equipment. The following effects can be expected.

1. To reduce of meetings and communication discussions for connection and information exchange with other vendor systems, etc.
2. To build a system that does not depend on a specific company.
3. To select the best devices and equipment with appropriate competition, improving economic efficiency and technology, and ensuring transparency.
4. To execute effectively cooperative control between devices of different vendor using standard objects and services
5. To display and store the obtained information in an easy-to-understand format, build an effective BMS (Building Management System), and to contribute to building operation and management.

Network and Communication Protocol

Internet Area

ANSI / ASHRAE Standard135-2020 (abbreviated as BACnet2020: latest version) [3] that can support the REST (Representation State Transfer) model that is mainstream in the IT industry. BACnet / WS RESTful of ANNEX W will be the center of introduction in BEMS.

Main network

Within the main network, BACnet / IP of ISO16484-5 and ANSI / ASHRAE Standard 135-2020 ANNEX J are mostly applied both in Japanese and international BEMS. According to the BACnet2020 standard, a BACnet / IP network is a collection of one or more IP subnetworks shown in the BACnet internetwork in (Figure 2) that can communicate with each other. BACnet / SC (BACnet / Secure Connect) [4] was standardized in BACnet2020. LTS (Transport Layer Security) can be applied to BACnet / SC, and security functions such as encrypted communication and device authentication have been improved.

Field Network

For the field network connected to the B-BC with the gateway function in (Figure 1), select the appropriate methods from the open communication methods described in (Table 1) and build on interoperability between field network and main network. BACnet MS / TP (Master-Slave / Token Passing) of BACnet standard 135-2020 is widely applied internationally, and its introduction is increasing in Japan as well. In addition, the application of the method using LonTalks communication (ISO / IEC14908-1-4) of Echelon Inc. of the United States has a lot of achievements worldwide including Japan. In Europe, KNX of ISO / IEC 14543-3 is often applied. Modbus and CC Link are often applied in PLC systems. In lighting control, it is expected that the DALI communication protocol of IEC62386 will be applied from the multiplex transmission remote control method.

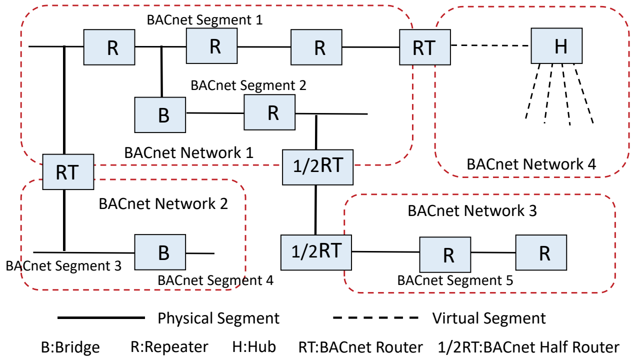

Figure 2. BACnet Internetwork.

Table 1. Open communication methods of field network.

No.	Communication	Note
1	BACnet/IP ISO16484-5	ANSI/ASHRAE Standard BACnet 2020 ANNEX J
2	MS/TP ISO16484-5	ANSI/ASHRAE Standard BACnet 2020 Chapter 9
3	P2P ISO16484-5	ANSI/ASHRAE Standard BACnet 2020Chapter 10
4	LonTalk	ISO/IEC14908-1～4
5	KNX	ISO/IEC14543-3
6	Dedicated Communication Protocol	DALI Protocol for Lighting, Buil-Multi Protocol for PACs, Communication Protocol for PLCs
7	Direct Interface	Direct Inputs and Outputs from Process
8	Wireless Interface	Wireless method by using Wi-Fi, ZigBee, EnOcean, LTE, etc. at access point (AP)
9	Internet Intetface	Communicate via the Internet using GW, VPN, Firewall

The Syberattacks Threats of Bems

IoT Trends and Recent Threats of Cyber attacks

In the previous BEMS, it was an independent system as a buildi.ng unit, not related to the Internet. Therefore, it was unrelated to cyber-attacks from outside the building and did not require countermeasures for them. It also provides a communication protocol for the network in the system. A vendor-specific protocol was adopted. In recent years, the BAS (Building Automation System) has evolved into BEMS due to the development of ICT and IoT related technologies. As shown in (Figure 1), it has become possible to execute a wide range of functions and services by connecting to the Internet, open system technology, and connecting it to ASPs, aggregators, other buildings, etc. by exchanging information and sharing functions. In 2010, a cyber-attack by malware targeting the control system of Iran's nuclear fuel equipment caused great damage. In 2015 and 2016, there was a cyber-attack on the control system of a power plant in Ukraine, and since then, a cyber-attack on the control system has become apparent. In addition, many cyber-attacks on building systems are occurring overseas. These events have begun to recognize the importance and necessity of cyber-security in BEMS in recent years.

The Characteristics of IoT and BEMS Devices

According to the "IoT Security Guidelines (published in 2016)" [5] by the IoT Promotion Consortium, the Ministry of Internal Affairs and Communications, and the Ministry of Economy, Trade and Industry, the general IoT-specific properties for cyber-attack risk are as follows.

(Characteristic 1) The range and degree of impact of the threat are large,

(Characteristic 2) The life cycle of IoT devices is long,

(Characteristic 3) Difficult to monitor IoT devices,

(Characteristic 4) Insufficient mutual understanding of environment and characteristics on the IoT device side and network side, (Characteristic 5) The functions and performance of IoT devices are limited and, (Characteristic 6) There is a possibility that a connection that was not expected by the developer will be made.

These six characteristics indicate that IoT devices are at risk of cyber-attacks. It is fully applicable to BEMS that is connected to the Internet and performs various functions, and BEMS components are subject to cyber-attack risk.

BEMS cyber-attack risk target equipment

In BACnet 2020 Annex L, the BACnet components shown in (Figure 1) are classified into the contents shown in (Table 2). These devices are the IoT components of the Internet in Section III A, the main network in Section III B, and the field network in Section III C, to which they belong. These have communication functions and have the characteristics of the above-mentioned IoT devices. Therefore, it is necessary to take measures against the risk of cyber-attacks on each network.

Table 2. BACnet components defined by BACnet2020.

Category	Abb.	BACnet Device
L1 Opelator Interfaces	B-OWS	Operator Workstation B-AWS Advanced Operator Workstation B-OD Operator Display
L4 Controller L4.1	B-BC	Building Controller
L4.2	B-AAC	Advanced Application Controller
L4.3	B-ASC	Application Specific Controller
L4.4	B-SA	Smart Actuator
L4.5	B-SS	Smart Sensor

Cyber Security Measures of Bems

Basic requires the Internet to link with external unspecified network users.

This may pose a threat or risk of unauthorized access by a malicious third party (eavesdropping of internal data, falsification, attack, malware infection, etc.). BEMS needs to consider cyber security measures against these threats. The basics of cyber security measures are to secure the following [6].

1. Confidentiality of information (securing the scope of information disclosure)

2. Integrity (information is not tampered with or erased)

3. Availability (accessible by users when needed)

Details of cyber-attacks

The BEMS components shown in (Figure 1) are required to ensure specific security against the following cyber-attack threats.

1. A cyber attacker sends malicious data to BEMS components and sensors over the GW via a network, causing malfunctions, outages, and data acquisition impossible.
2. Falsification or theft of internal data of energy equipment and sensors of the target equipment (thing level) occurs.
3. Unauthorized access to energy equipment or sensors may cause equipment malfunction or stop functioning.
4. The processing load is increased by transmitting unauthorized data from unauthorized access sensors and energy devices to the servers that make up BEMS, and as a result, the entire BEMS service is reduced or stopped.
5. A cyber attacker hijacks an energy device or sensor by unauthorized access and makes it involved in its DoS (Denial of Service Attack) attack on an external system via GW.
6. As a result of the destruction or suspension of equipment due to the above, the suspension of BEMS service and malfunctions related to the safety of the building are induced.

IEC62351 Security Level and BEMS

The IEC62351 [7] series is international standards for information security for communication protocols of power system monitoring and control systems. IEC62351-10 classifies domains for security management of electric power systems into four types: public, enterprise, important business, and important system operation. The above public supports communication on public networks. The security level is "low". Enterprises support office-level networks. The security level is "medium". Support the operation of electric power systems in important businesses. The security level is "high". Important system operation is related to the reliability and availability of power generation and distribution infrastructure. Therefore, the security level is set to "extremely high". BEMS is an important facility related to the operation of building facilities, including the control of power facilities in the building, and falls under the category of important business. Therefore, a high security level is required.

Security Controls

In addition, the IEC62351 series stipulates physical control, procedural control, technical control, operational control, legal regulation and compliance control shown in (Table 3) as security controls. In BEMS, security controls are classified as shown in Table 3 in order to avoid, take measures, and minimize security risks. BEMS implements the following security controls centered on No. 1 physical control and No. 3 technical control [8].

1. Physical control: The installation location of BEMS components such as the central monitoring room, disaster prevention center, electrical / mechanical room where BEMS components are installed is always locked, and entry is limited to authorized persons.

2. Technical control: Mainly user authentication and logical access control, installation of anti-virus software, introduction of secure protocols, and installation of firewalls. The basics of these controls are the following three items.

(a) Connect only to trusted parties.

(b) Connect only to reliable devices.

(c) Implementation of anti-virus measures.

Support network segmentation by installing a VPN for (a) above and ensure the confidentiality of information. There are two types of VPN: Internet VPN via the Internet and closed VPN (IP-VPN) for leased lines by communication service providers. Closed VPN unrelated to the Internet has higher security. (Figure 3) shows an application example of BEMS firewall and VPN. A login password is set for operator access. For (b) above, the main tasks are authentication, authorization, and encryption of information between network devices. In BACnet, user authentication, CA certificate, and encryption by TLS (Transport Layer Security) of Web Socket communication are introduced in the communication protocol by BACnet / SC. The main countermeasure against (c) above is to install anti-virus software from virus infection from an external storage media such as a USB memory. In addition, the version will be updated as appropriate for the PC manufacturer support deadline.

Equipment Disposal and Anti-theft measures

When disposing of the BEMS IoT device, completely erase the data on the

Table 3. Basic security controls in BEMS.

No.	Category	Countermeasure examples
1	Physical control	Fences, doors and locks
2	Procedural control	Incident management, raising security awareness
3	Technical control	User authentication and logical access control, anti-virus software, security protocol, firewall
4	Operational control	Situation analysis, emergency / accident analysis
5	Laws and regulations, compliance Control	Personal Information Protection Law, Laws and Regulations

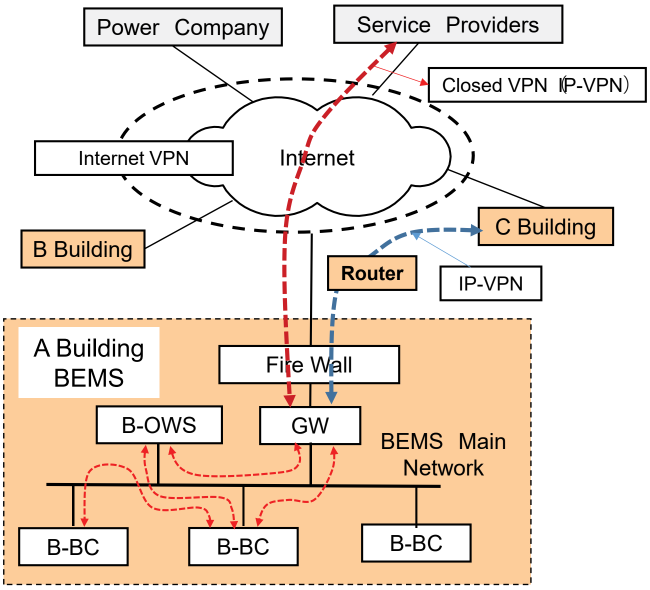

Figure 3. Sample of adaption of fire wall and VPN in BEMS network.

hard disk or storage device. Because SIM (Subscriber Identification Module) cards contain confidential information about lines and sharing, devices with SIM cards require strict control over theft and storage.

Discussion & Conclusion

By linking BEMS with the Internet, the application of BEMS and the range of services have expanded dramatically. That is, visualization service on energy dashboard by cloud, power supply and demand adjustment of consumer power resources by demand responses in smart grid [9], role of edge system of digital data infrastructure of Society 5.0 based smart city, digital transformation (DX) and digital twin, BEMS has become more involved in dealing with such issues. Therefore, the risk of cyber-attacks is high, and cyber security measures are an essential technology. Although 100% countermeasures are difficult, it is important to implement feasible countermeasures against possible risks. For that purpose, risk countermeasures that are easy to introduce, economical, common, effective, and highly practicable are desired.

References

1. Toyoda. ”The Transition of Open BACS and Trends of Internationalization of BACS.” *J Inst Elect Installation Eng JPN* 40 (2020).
2. The Institute of Electrical Engineering of Japan. “Creation of structure and services for BACS for Coming IoT Technology.” (2019): 4.
3. ANSI/ASHRAE Standard. “A Data Communication Protocol for building Automation and Control system.” (2020).
4. Fisher D, Isler B, and Osborn M. “BACnet Secure Connect”. *ASHRAE SSPC* (2019).
5. IoT Promotion Council. “Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry.” Guideline on IoT Securities (2016).
6. Agency for Natural Resources and Energy Information-technology Promotion Agency [IPA]. “Cybersecurity Guideline (Ver2.0) on Business of Energy resource and Aggregation.” (2017).
7. International Electrotechnical Commission. “IEC62351: Power Systems Management and Associated Information e8 Change Data and Communication Security.” (2018).
8. Mizuno. “Cyber Security Measures for Building System.” *J Inst Elect Inst Eng JPN* 39.
9. Toyoda. “Demand Response and Adjustment of Electricity and Demand.” *J Inst Elect Instal Eng JPN* 40 (2020).

How to cite this article: Takeji Toyoda. "The Network Structure of BEMS and Cyber security." *J Biomed Syst Emerg Technol* S1 (2021): 008.