IEICE TRANS. COMMUN., VOL.E101–B, NO.8 AUGUST 2018

INVITED PAPER Special Section on Autonomous Decentralized Systems Technologies and Approaches Innovation through Structure Change of Society and Life

Safety Technologies in Autonomous Decentralized Railway Control System and its Future Studies

Shinichi RYOKI[†,††a)], ***Nonmember***, **Takashi KUNIFUJI**[††], ***Member***, ***and*** **Toshihiro ITOH**[†], ***Nonmember***

SUMMARY Along with the sophistication of society, the requirements for infrastructure systems are also becoming more sophisticated. Conventionally, infrastructure systems have been accepted if they were safe and stable, but nowadays they are required for serviceability as a matter of course. For this reason, not only the expansion of the scope of the control system but also the integration with the information service system has been frequently carried out. In this paper, we describe safety technology based on autonomous decentralized technology as one of the measures to secure safety in a control system integrating such information service functions. And we propose its future studies.

key words: *railway, signalling system, network, autonomous decentralized technology, safety, wirelessization*

1. Introduction

Railway control systems have significant roles in the safe and stable train operations. It consists three functions, intelligent information management, soft real-time control, and safety control as one of a hard real-time system. These systems are still developing to satisfy a lot of demands such as changes of transportation capacity or revisions of train schedules. The railway control system has been digitalized from the viewpoint of automating the train traffic operation which had been previously performed by personnel, that is labour saving. Regarding digitization of safety related systems, establishment of safety technology in computer control system is necessary, and in 1985 the first electronic interlocking equipment was introduced in Japan.

Conventional safety related system was realized by hard-wired logic such as relay circuits. It required specific electric wiring. Manual jobs of the wiring tasks built up the relay circuits that was individually designed, but the jobs sometimes caused human errors which result in significant transportation disorders. Moreover, demands for high operating rate required a duplex structure of the systems, but it was difficult to complete the duplex system by the relay logics. Recently, computer technologies are much progressed. We have applied the technology to the railway signalling equipment to overcome these issues. For example, electric interlocking equipment, which is a computerized interlocking system, has computerized logics and achieves duplex structures. Other signalling equipment, such as a train detector system, an automatic-train-stop (ATS) system, have been computerized and installed. However, a huge amount of wiring remains from the control equipment of the machine room to the field signalling device, and further improvement in design and construction efficiency due to the advance of digitization is required.

In this paper, firstly we describe issues of the present railway control system. Secondly, we introduce a novel system as an autonomous decentralized control system. Thirdly we discuss the safety technologies of general autonomous decentralized railway control system and specific safety technologies of our system. Finally we present the future studies for wirelessization of the optical network and its issues and measures.

2. Autonomous Decentralized Railway Control System

2.1 Issues in Conventional Railway Control System

Railway control system generally consists of three hierarchies of traffic control, route control, and signal control (Fig. 1). Therefore, when a higher-level system becomes inoperative due to failure, maintenance, or construction, it affects a wide range of the lower-level. Especially in Tokyo metropolitan area, the system should be often expanded to meet the customer requirements. However it is difficult to expand the system to follow changing of social environment with conventional hierarchical system. Due to this reason, railway control systems which operates heavy traffic should have properties such as online expansion, online maintenance and fault tolerance. Hence the ATOS (Autonomous decentralized Transport Operation control System) for Tokyo Metropolitan Area and COSMOS (Computerized Safety, Maintenance and Operation Systems of Shinkansen) are introduced as an autonomous decentralized traffic and route control system [1]–[3], [5], [6].

On the other hand, the online expansion and online maintenance have not been realized in signal control system. And it is caused by its system architecture. Concretely as shown in Fig. 1, since the control logic is centralized to the computer which is set up in the machine room of a station and the signalling devices such as actuator are installed at the wayside. They are connected by enormous number of metal cables and control commands are transmitted through

Manuscript received November 8, 2017.
Manuscript revised December 28, 2017.
Manuscript publicized February 22, 2018.

[†]The authors are with Department of Human and Engineered Environmental Studies Graduate School of Frontier Sciences, The University of Tokyo, Chiba-shi, 277-8563 Japan.
[††]The authors are with Research and Development Center of JR East Group, East Japan Railway Company, Saitama-shi, 331-8513 Japan.
a) E-mail: sryoki@s.h.k.u-tokyo.ac.jp

DOI: 10.1587/transcom.2017ADI0002

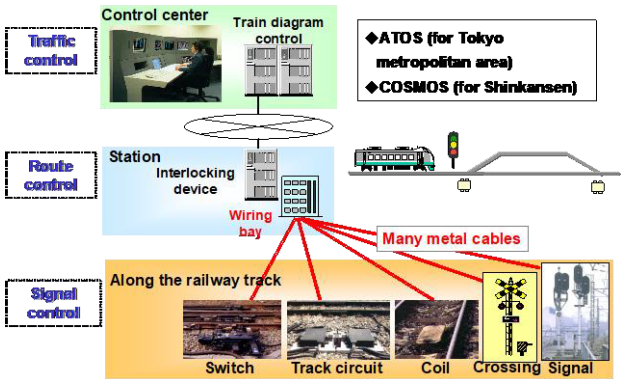


Fig. 1 A typical control system of railway.

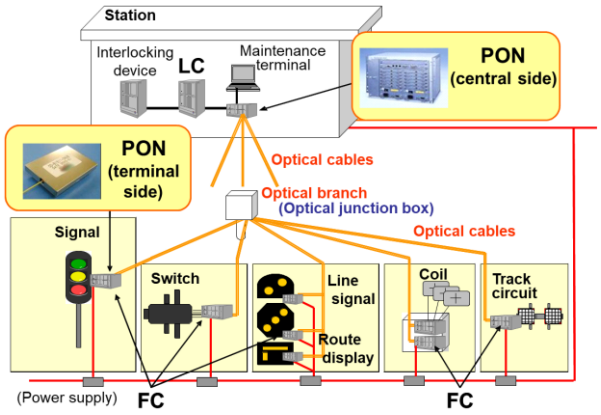


Fig. 2 Configuration of a new signalling system.

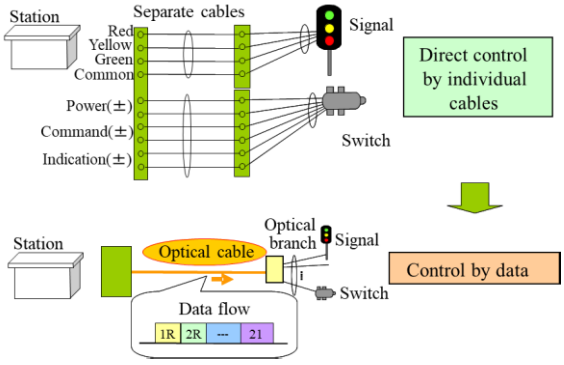


Fig. 3 Two methods of signal devices controlling.

these cables. As mentioned above, signal control system is a unification of computer, signalling devices and cables. So, it is difficult to expand or maintain partially.

In updating the system to the next generation, we want to improve the following three points. First, the cable-laying costs is very high. The cable costs occupy the much of the system construction costs, reducing it leads to significant cost reduction. Second, the wiring enormous numbers of cables is a heavy task, because we have to install or rearrange the cables with great care. Unfortunate human errors in wiring tasks sometimes occur, the errors may cause serious transport disorders. Third, since the transmission path of the current system is a simplex structure. The structure causes serious transport disorders if a damage accident of cables happens. Therefore, the duplex structure of the control system for field devices is required.

For example, interlocking equipment directly controls signal devices by applying electric voltage to copper wires through relay circuits. Enormous amount of wirings are required because an interlocking device controls a number of signal devices. When the transport capacity increases, or an interlocking device deteriorates, the interlocking device will be improved or replaced where large number of wirings are needed. It requires much time and is a manual work that may cause human errors. The errors can result in a big transport disorder.

Moreover, a system changes as adding a new colour signal device needs all signal devices to be rearranged or restructured. Since all signal devices are individually settled, and they have different software and independently operate, we have to handle all devices one by one and pay great attention to avoid harmful influence on each other.

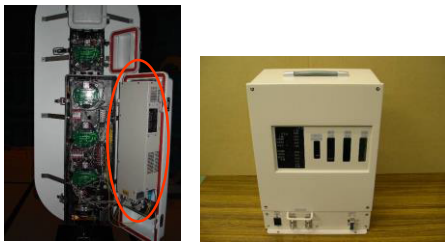
2.2 SignalControl System Based on IP-Network

In order to address these issues, we have developed a new railway signalling system based on IP-network. We introduced an optical LAN and the Internet technologies to the transmission between the central control unit and the field devices [7]–[11]. The optical LAN drastically changes the control method of the field devices. Figure 2 schematically illustrates the system.

The system consists of a central control unit (Logic Controller: LC) and signal devices (Field Controller: FC) connected with optical cables. Both the LC and the FC are duplex. Figure 3 shows two methods of signal device control. In conventional method, a central control device feeds electric power directly to the signal devices by separate cables. In a new method, the control data is sent to the signal devices through optical cable using internet protocol and the device operates its aspect or manipulation.

A similar structure system using optical cables is European Initiative Linking Interlocking Subsystems (EULYNX) [12]. The purpose of EULYNX is to connect subsystems under the interlocking device with the shared network, but our system has autonomous decentralized railway control system in addition to the shared network as shown below.

This system is also an autonomous decentralized system (ADS). The LC is an autonomous safety-related equipment located at the signal house. The LC generates the signal control information (such as aspect for signal light, operation for switching devices etc.,) and translates it into the IP-formatted command data, which is broadcasted to FCs through optical fibre network as a data field (DF). The FC is also an autonomous safety-related equipment located at the wayside. The FC controls the signal device electrically based on the extracted data from the DF. The FC also translates the obtained information from the signal device into the



(a) Built-in type (b) In-case type

Fig. 4 Two types of the FC.

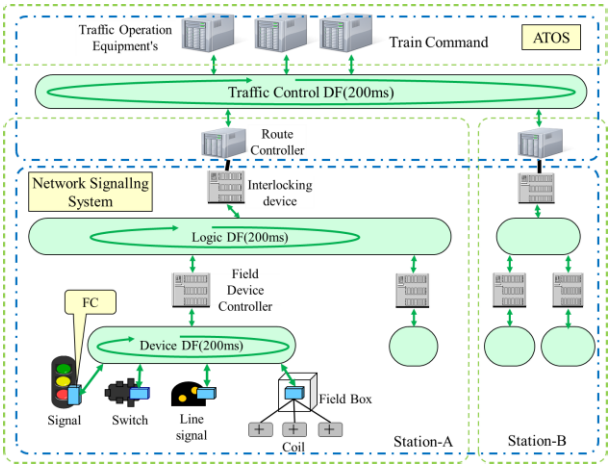


Fig. 5 System architecture of autnomous decentralized railway control system.

IP-formatted feedback data, which is transmitted to the DF. We have developed two types of the FC. One is equipped in signal device itself (Fig. 4(a) is one example), the other one is installed in a wayside case, and we use copper wires from the FC to the signal devices (Fig. 4(b) is another example).

As a result, all layers of the railway control system have become a complete ADS.

2.3 System Architecture of Autonomous Decentralized Railway Control System

Figure 5 shows an architecture of railway control system which deploys autnomous decentralized signal control system. In this model, the system is composed of three hierarchies. In each layer, a different service is provided from other layers. The data field of each layer is separated and different layers of the data field are interconnected by Gate Way (GW) which is also an Autonomous Decentralized Sub-system.

Thus a system that integrates autonomous decentralized systems with different real-time properties is called HRTAIS (Heterogeneous Real-time Autonomous Integrating System Architecture).

3. Safety Technologies in HRTAIS

In this section, HRTAIS and its configuration technologies are described.

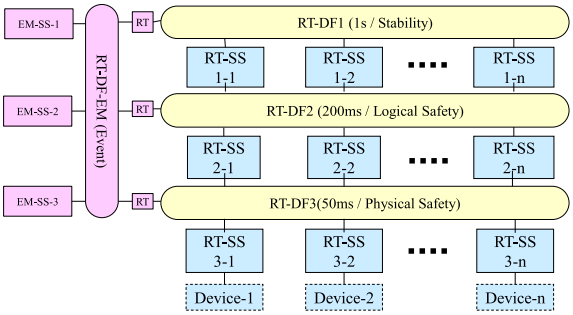


Fig. 6 Generic System architecture of HRTAIS.

3.1 Generic System Architecture of HRTAIS

Generic system architecture of HRTAIS is shown in Fig. 6. HRTAIS consists of several heterogeneous real-time data-fields (RT-DF) and many autonomous real-time subsystems (RT-SS). Emergency data-field (EM-DF) is one of the Event-DF and connected to all DF's via router. Emergency subsystems (EM-SS) are only connected to the EM-DF. EM-SS activate an alarm and this alarm is broadcasted to all the subsystems via each RT-DF.

3.1.1 Real-Time Data Field (RT-DF)

In HRTAIS all kinds of data which flows in the DF's have real-time properties that are defined in section two. And all the data in same DF should have same real-time property. This type of DF is called real-time data field (RT-DF). To ensure maintaining time restriction, the DF should be refreshed within properly time. The refreshing method should be selected according to the service level by which real-time is guaranteed.

a) Refreshing by event

In this method, the data is refreshed only when the processing result is changed. In the sub-system that uses concerned data, when there is no reception from the DF, the latest value is used for processing. When the delivery confirmation is done to confirm the reception in time by the subsystem that uses it due to a change in the processing result for this method, and if it is not possible to receive it, it is necessary to send it again. Therefore, this method can not be applied if time limits are shorter than overheads according to re-transmission. Moreover, the technology that the transmission line judges whether data disappeared on the way and whether data is sent on the receiving side is newly needed.

b) Refreshing by cyclic

In this method, the data is refreshed periodically regardless of the presence of the change in the processing result. Latest information is expected to be able to regularly be received, and in the subsystem that uses concerned data, when the time-out is generated, a preset value is used and processed.

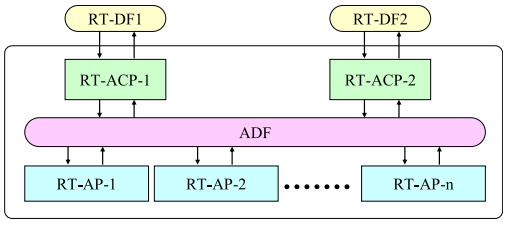


Fig. 7 Architecture of real-time subsystem.

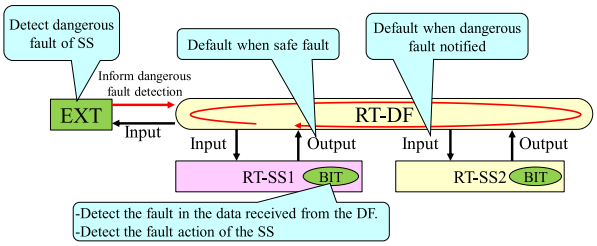


Fig. 8 Fault detection mechanism and default value at subsystem's fault.

It should be noted this method causes high load to the transmission system. Moreover, it is necessary to shorten the transmission cycle to an extent to which it can follow to the change frequency of the transmission data.

3.1.2 Real-Time Subsytem (RT-SS)

Architecture of the RT-SS is shown in Fig. 7. The subsystem has two heterogeneous autonomous real-time control processors (RT-ACP). Each RT-ACP is connected to different RT-DF. Therefore, the subsystem is connected to maximum of two heterogeneous RT-DF's. The data is shared by real-time applications (RT-AP) via atom data field (ADF) in the subsystem.

RT-ACP is periodically driven and driving cycle is the same as other subsystem's RT-ACP which connected to the same RT-DF. Hence RT-ACP's in the same RT-SS is driven asynchronously. Generally, the ADS subsystems are driven by data and the process starts after all required data is received. Therefore, in periodically driven system like RT-ACP, there is no guarantee that all required data has received within the periodical period. If all required data has not received, RT-AP adopts alternative value and starts processing. This alternative value is called default.

3.2 Safety Functions for HRTAIS

3.2.1 Autonomous Safety

In autonomous decentralized safety related system, it is required to have characteristics of autonomous controllability, autonomous coordination and autonomous safety to achieve online property. Autonomous safety is defined as characteristic that if any subsystem fails, is repaired and/or is newly added, the other subsystems can keep safety.

The requirements to realize autonomous safety is that each sub-system can autonomously execute safety functions listed below.

- Fault detection
- Safety control
- Data integrity conversion

3.2.2 Fault Detection Mechanism of RT-SS

Figure 8 shows the autonomous fault detection mechanism. In this mechanism, Built-in Tester (BIT) is prepared as an application of RT-SS. And External Tester (EXT) is prepared as one of RT-SS of a system. These two types of testers detect the fault from different view point.

a) BIT

BIT is an autonomous application which is connected to ADF. It processes self-checking of RT-SS and healthy checking of applications in the RT-SS.

b) EXT

EXT is one of an autonomous RT-SS which is connected to the DF. It is utilized to detect a latent fault in BIT. If EXT detects a fault in BIT, it notifies occurrence of a dangerous fault to all the subsystems in the DF. Subsystems receive the notification and replace the input from the subsystems in dangerous fault mode to the default value autonomously.

c) Fault detection in content code communication

It is a function to detect errors occurring in data exchange between RT-SS via DF. Errors in data communication can be roughly classified into data error, time error, and delivery destination error.

Data errors are detected by redundancy code such as CRC. Time errors are detected by serial numbers and timeouts. Delivery destination errors do not occur in principle in content code communication because of using the multicast protocol.

3.2.3 Safety Control

a) Hardware error

Hardware error is detected by BIT, and the RT-SS will be shut down by BIT. In other RT-SS, the data that was expected to be received from the failed RT-SS is replaced with the default value.

b) Software error

Software error is detected by BIT, and the autonomous application which caused the error will be halted by BIT. The data was expected to be submitted by the failed application is replaced by default value. If error has occurred in ACP or BIT, RT-SS should be shut downed by EXT.

c) Communication error

Communication error is detected by ACP, and the data will be replaced with default value.

Table 1 Variation of default value.

Type	Default Value	Usage
Input	Previous value	Keep availability
	Application specific	Keep service level
	NULL	Keep accuracy
Output	Flag	Notify the default to the receiver
	NULL	Notify the default to the receiver

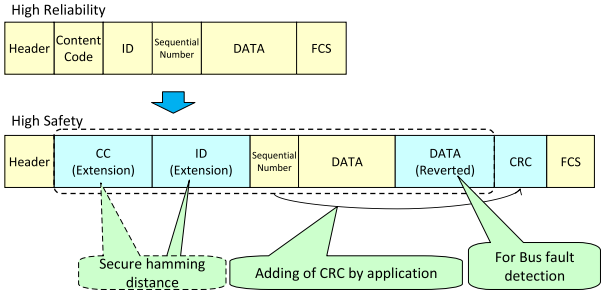


Fig. 9 Service level filtering (reliability to safety).

d) Default value at subsystem fault

Objective of adopting default value is to keep service level of applications as high as possible. To do this, it is desirable that default value shall be autonomously specified at input according to the application's requirements. Default value is classified into 4 types: previous value; application specified value, no data, and flag.

Previous value: This value is the same as what is used in the previous processing cycle. This contributes to keep availability of the system.

Application specified value: This value is constant value which is specified by application.

NULL value: This value means that the data is not for use.

Flag: This means an indicator that dead-line miss has occurred and the data is not for use.

Variation of default values for input and output are summarized in Table 1.

3.2.4 Data Integrity Conversion

Depending on the service level, the integrity of input data required by system is different. So, data exchange between heterogeneous RT-SS's filtering of service level is also required. Figure 9 shows the difference of data format according to the service level. In case service level is high reliability, it may be sufficient that minimum level of redundant code is added to the data. However, in case service level is high safety, addition of diversified redundant code and extension of code system to increase hamming distance should be required. This filtering is performed by ACP in the RT-SS's autonomously.

To perform these filtering functions mentioned above, RT-SS's should recognize the real-time requirements of each RT-DF. In the ADS, these requirements are recognized as common knowledge and each subsystem distinguishes the requirements according to the CC of the data. So, filtering can be performed autonomously.

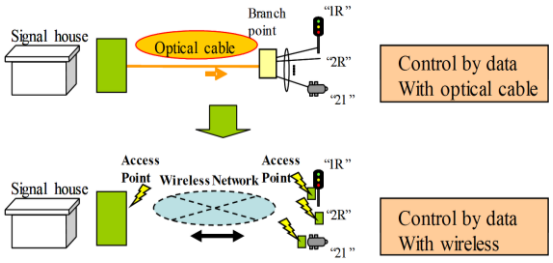


Fig. 10 Wirelessization of the optical cables.

4. Future Studies

4.1 Wirelessization of RT-DF

In the new signaling system, network signaling system, cables between the central control unit and the field devices are reduced. However, optical cables as the information and control line and metal cables as the power supply line for the field devices are still retained. If these cables are removed and completely wireless around the field devices (Fig. 10) can be realized, the following advantages are expected;

- Reduce construction and material costs for cables
- Reduce construction period
- Reduction of failure caused by cables (ex. damaged by rats)

But, there are some technical problems for wireless, and it is described in the next subsection.

4.2 Inprovement of Autonomous Function of the FC

Commonly, the transmission capacity using radio transmission is lower than using optical fiber. For example, the baud rate in train radio communication system in JR-East is lower than 500 kbps. On the other hand, rough estimate baud rate required by the RT-DF is over than 3Mbps, it is necessary to reduce the amount of data. As mentioned in section III-1-a, the method of refreshing by cyclic causes high load to the transmission system. This method is used to transmit the feedback data for signal control information from the FC to the LC. Based on this information, the LC sends the next control information to the FC. Therefore, this network is star connected. If the FC can generate the next control information by itself based on the feedback data from other FC, LC does not need to refresh the feedback data by cyclic for generating signal control information. Each FC refresh its feedback data by event and sent the data to the RT-DF (Fig. 11). As a result, the rate of data transmissions is reduced, as well as the baud rate required by the RT-DF. A suitable network structure for this case is a mesh connection, this structure raises the fault tolerance of the network and is

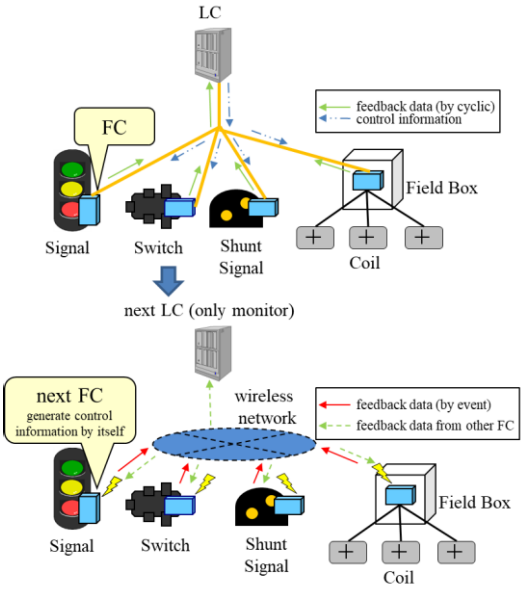


Fig. 11 Comparison of the date flows.

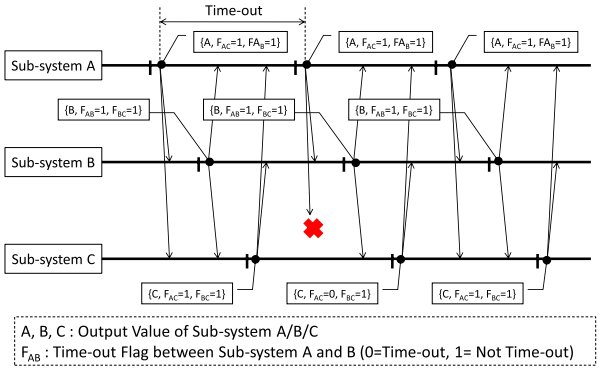


Fig. 12 Autonomous delay detection in optical fiber network.

suitable for wireless construction. Therefore, improvement of autonomous function of the FC is necessary for wirelessization.

4.3 Delay and Data Collision Avoidance

HRTAIS consists of real-time data-fields and subsystems. The delay caused by the network when the RT-DF is constructed with an optical fiber network is very short, but the delay may have serious problems on the real-time system when the RT-DF is wireless. Another thing that affects the real-time system is data collision. The network signaling system is asynchronous system, the data refreshing by event is sent out randomly to RT-DF. In optical fiber network, data collisions are detected as one of the result of transmission delay. Figure 12 shows the detection of transmission delay and data collision in the network signaling system.

This method can be applied because the transmission delay is very short and the transmission capacity is sufficiently large in the optical fiber. In wireless, it is difficult to use this method due to the delay and capacity. Commonly, CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) is used for data collision avoidance in wireless network. In this method, the delay time and the collision probability increases as the data amount increases, it is difficult to apply CSMA/CA for use with safety system like railway control system. Therefore, the new protocol with lower delay and lower collision probability is required.

4.4 Security

As the wireless network implemented across railway systems, security measures against malicious attacks etc are needed [13]. For the measure of this problem, the method described below is more effective in addition to using the conventional internet security measure. First is the network slicing technology which is scheduled to be taken in the 5G network [14]. In this technology, independent logical networks can be constructed. The data in the network signaling system is divided into some levels by its importance of security such as train control information, hardware monitoring information and maintenance information. Separating the logical networks by security levels, the data which is different security levels can be transmitted securely in the same wireless network. Second is dividing wireless transmission frames according to information type and importance. The conventional wireless transmission method uses time division multiplex frame, like TDMA, even when there is no information, sharing one frame. This method is useful for refreshing by cycle, but not for refreshing by event, as it is not an efficient and a secure because of many slots are empty. It is not preferable that there is information with different types of importance in the same frame. As a solution to this issue, a method of giving a dedicated frame for each connection request is useful. In that case, it is necessary to consider optimal protocols considering capacity and collision.

5. Conclusion

In this paper, we clarified issues in the extensibility of the railway control system and showed examples of autonomous decentralized railway control system as a solution to it.

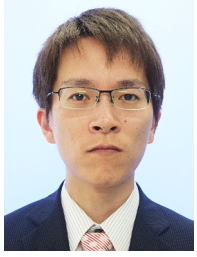
Furthermore, we modelled the autonomous decentralized railway control system as a HRTAIS and proposed a safety technique in it.

And as future studies, we presented some issues for wirelessization of the optical network.

References

[1] K. Kera, et al., “Assurance system technologies based on autonomous decentralized system,” Proc. ISADS’99, Tokyo, Japan, 1999.
[2] F. Kitahara, H. Katano, T. Ono, Y. Kakumoto, K. Kikuchi, and M. Shinomoto, “Distributed management for software maintenance in a wide-area railway system,” Proc. ISADS’97, Berlin, Germany, 1997.
[3] F. Kitahara, T. Iwamoto, K. Kikuchi, K. Fujiwara, H. Kawashima, and H. Yamamoto, “Widely-distributed train-traffic computer control system and its step-by-step construction,” Proc. ISADS’95, 1995.
[4] F. Kitahara and K. Kera, “Widely distributed train traffic control

system," J. SICE32, no.7, 1993.
[5] F. Kitahara, K. Kamijou, Y. Kakurai, K. Bekki, K. Kera, and K. Kawano, "Phased-in construction method of ATOS" Proc. ISADS'99, Tokyo, Japan, 1999.
[6] K. Kera, et al., "Assurance system technologies for large scale transport operation control system," IEICE Technical Report, FTS99-29, June 1999.
[7] Y. Hirano, T. Kato, T. Kunifuji, T. Hattori, and T. Kato, "Development of railway signalling system based on network technology," IEEE SMC, Oct. 2005.
[8] R. Ishima, Y. Fukuta, M. Matsumoto, N. Shimizu, H. Soutome, and M. Mori, "A new signalling system for automatic block signal between stations controlling through an IP network," WCRR May 2008.
[9] J. Nishiyama, H. Sugahara, T. Okada, T. Kunifuji, Y. Fukuta, and M. Matsumoto, "A signal control system by optical LAN and design simplification," IEEE SMC, Oct. 2007.
[10] T. Kunifuji, G. Kogure, H. Sugahara, and M. Matsumoto, "A novel railway signal control system based on the Internet and assurance technologies," IEICE Trans. Inf. & Syst., vol.E91-D, no.9, pp.2293–2299, Sept. 2008.
[11] T. Kunifuji, T. Miura, G. Kogure, H. Sugahara, and M. Matsumoto, "A novel railway signal control system based on the Internet technology and an assurance technology," IEEE ADSN, June 2008.
[12] EULYNX (2017). https://eulynx.eu/index.php/documents/project-description/ (accessed 2017-12-1)
[13] T. Mori et al., "Information security and safety of vehicles: Railway safety and security," J. IPSJ, vol.57, no.7, pp.638–643, June 2016.
[14] A. Nakao, et al., "End-to-end network slicing for 5G mobile networks," J. IPSJ, vol.58, no.2, Feb. 2017.



Shinichi Ryoki is Researcher of Research and Development Centre of JR East group at East Japan Railway Company (JR East), and Ph.D. student in The University of Tokyo, Japan. He has engaged in research and development of telecommunications and networking in railway since 2015. He engaged in maintenance, design, and construction of telecommunication systems in railway from 2009 to 2015. He has joined JR East since 2009. He graduated from The University of Tokyo, Japan, in 2009 with a Master's degree in Physics. He is a member of IEEJ.

Takashi Kunifuji is Principal Chief Researcher of Research and Development Centre of JR East group at East Japan Railway Company (JR East), Japan. He has engaged in research and development of railway signal control systems since 1998. He engaged in maintenance, design, and construction of signalling systems from 1992 to 1998. He has joined JR East since 1992. He has received Ph.D. degree in Engineering from the Tokyo Institute of Technology, Japan in 2008. He graduated from the Tsukuba University, Japan, in 1992 with a Master's degree in Electrical Engineering. He is a Fellow of IRSE and a member of IEEE, IEICE, IEEJ and IPSJ.

Toshihiro Itoh received the BE, ME, and Ph.D. degrees in precision engineering from the University of Tokyo, Japan, in 1988, 1990 and 1994, respectively. He had joined the faculty of the University of Tokyo in 1995 and was an associate professor at the Research Center for Advanced Science and Technology (RCAST) and the Department of Precision Engineering from 1999 to 2007. Since 2007, he has been a research manager of MEMS-related laboratory in National Institute of Advanced Industrial Science and Technology (AIST), Japan. Since 2015, he has been a professor at the Department of Human and Engineered Environmental Studies, the University of Tokyo, Japan. His research interests are in wireless sensor network technologies as well as large area MEMS.