# A safety-related transmission method for a new railway signalling system based on an IP-Network

M. Endo[1], T. Okada[1], D. Watanabe[2], K. Aimi[3], T. Kunifuji[1] & M. Matsumoto[1]
[1]*East Japan Railway Company, Japan*
[2]*Hitachi LTD., Japan*
[3]*Fujitsu LTD., Japan*

## Abstract

We have developed a signalling system which controls signal devices through an IP-Network. This system consists of a Logic Controller (LC) and Field Controllers (FCs) connected with optical cable. The LC is a safety-related device located at the signal house. The LC generates the command data, and transmits the data to the FCs through IP-Network. The FC is a safety-related device equipped in each signal device, and controls the device based on the command data from the LC. In the railway signalling system, high level of safety and reliability are required. In this system, the transmission devices and protocol are based on the general technologies. Therefore, we need to assume all kinds of errors on the transmission devices, and the whole system must keep itself in safe status even if the worst error occurs. In order to comply with the IEC62280-1, we have developed a safety transmission protocol. Moreover, this system needs to operate for 20 years without system down. We have defined the target of the failure rate of each device less than $10^{-7}$/h. We measured the traffic limitation in order to validate the reliability about the transmission between the LC and the FC, and confirmed that the traffic is much less than the traffic limitation of the transmission device. We have evaluated the safety and reliability of this system with prototype system, and put this system into practical use at Ichikawaono station on the Musashino line in February 2007.

*Keywords: IP-Network, PON, safety, reliability, safety-related transmission.*

WIT Transactions on The Built Environment, Vol 103, © 2008 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/CR080121

## 1 Introduction

Railway signalling systems have significant roles in the safe and stable train operations. These systems are still developing to satisfy a lot of demands such as increasing of transportation capacity or revising of train schedules.

Ordinary these systems mainly consist of relay logic circuits, which need specific electric wirings. The wiring requires manual works, and the design of the relay circuits needs expert knowledge. Moreover, demand for high operating rate requires a duplex structure of the systems, but it is difficult to construct the duplex system by the relay circuit.

Recently, the progress of computer technologies has enabled to apply the technology to the railway signal devices to overcome these issues. For example, an electric interlocking system, which is a computerized interlocking system, has computerized logics and achieves duplex structures (ATOS is an example [1]). Other signalling devices, such as a train detector system, an automatic-train-stop (ATS) system, have been computerized and installed. These devices are usually installed in a room like the computer room of a station.

In this paper, firstly we describe issues of the present computerized signalling systems. Secondly, we introduce a signalling system based on an IP-network. Finally, we discuss a safety-related transmission method for this system and a target of the communication error rate for each signal device.

## 2 Issues of the current computerized signalling systems

Fig.1 shows a typical railway signalling system. The signalling systems are much progressed by applying the computer technologies. But they have some issues.

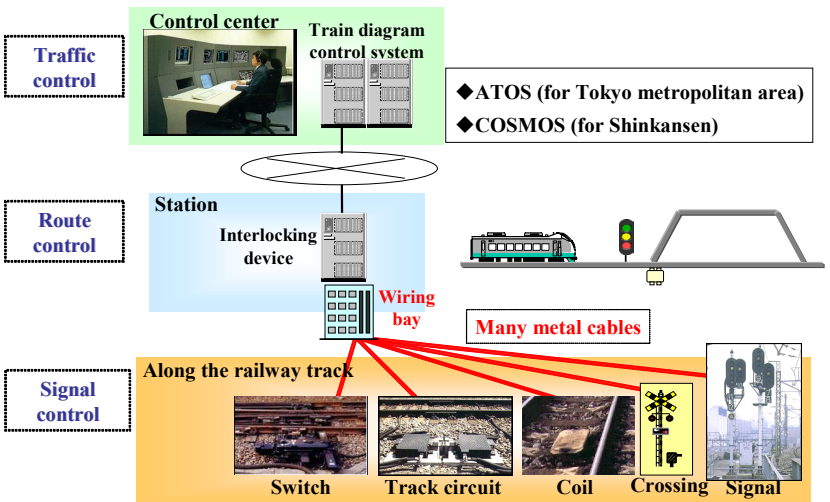



Figure 1: A typical railway signalling system.

1) Enormous number of cables and high construction cost

The interlocking device has computerized logic and duplex structure, which is connected to the control center by optical cable. However the interlocking device controls signal devices located along the railway track electrically using copper wires. Therefore, in a large-scale station yard, enormous number of cables are laid for the signalling system, and it requires high construction cost.

2) Much human task

Since wiring works and confirmation of wirings must be done by human hands, we have to install or rearrange the cables with grate care. If human errors in wiring works occur, it may cause severe transport disorders. When the transport capacity increases, or an interlocking device deteriorates, the interlocking device must be improved or replaced. It needs large number of wirings and manual work, which require much time and may cause human errors.

3) Simplex transmission path

The interlocking device is duplex system. But the copper wires to the signal devices are still simplex with low reliability. If a damage accident of cable occurs, it also causes severe transport disorders.

Therefore it is required to reduce construction work, simplify wiring confirmation, and ensure the high reliability.

## 3 Signalling system based on IP-network

In order to solve 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 [2]. The optical LAN drastically changes the control method of the field devices. Fig.2 schematically illustrates the system.

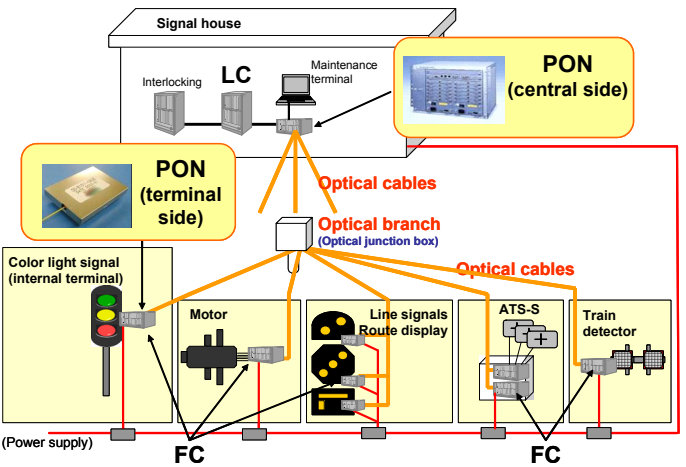



Figure 2: Configuration of a new signalling system.

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. Fig.3 shows two methods of signal devices controlling. 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 with the Internet protocol and the device operates its aspect or manipulation.

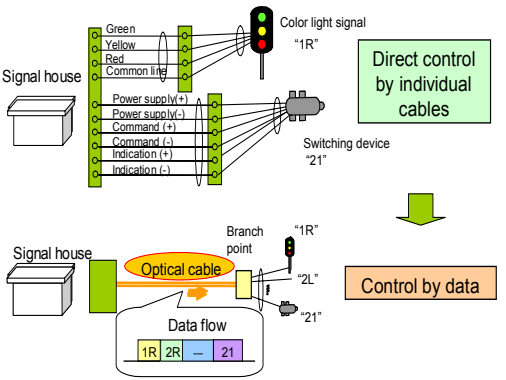
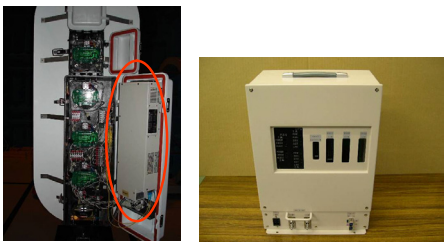



Figure 3: Two methods of signal devices controlling.

The LC is a safety-related device located at the signal house. The LC generates the signal control information (such as aspect for signal light, operation for switching devices), and translates it into the IP-formatted command data, which is transmitted to FCs through optical fiber network. The FC is a safety-related device located at the wayside. The FC controls the signal device electrically based on the received data from the LC. The FC also translates the obtained information from the signal device into the IP-formatted feedback data, which is transmitted to the LC. We have developed two types of the FC. One is equipped in signal device itself (Fig.4(a) is one of 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 one of example).



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

Figure 4: Two types of the FC.

The optical transmitting system is realized by using a Passive Optical Network (PON) system. Since a branch of the PON system is a passive device, it does not need electric power and is very robust. Therefore, the PON system is suitable for this system. One optical line is divided into 32 lines by using the branch devices. When we use 10 optical lines, we can control more than 300 devices. We use a duplex transmission path by arranging two optical fibers for one path in order to avoid communication breaks caused by cable-damage accidents.

By using the Internet technologies, we can achieve multiplex transmission instead of the direct power transmission by copper wires. By using the multiplex transmission technique, we can reduce number of cables. Moreover, by applying optical LAN technologies, the duplex structure is realized in data transmission.

## 4 Requirements of safety and reliability

In the railway signalling system, high level of safety and reliability are required.

### 4.1 Requirements of safety

Fig.5 shows the network configuration of this system. In this system, we divide the network into three segments (a controlling segment, a monitoring segment, and a remote-controlling segment). The safety-related data for signal control is transmitted in the controlling segment. We discuss the compliance with IEC62280-1 (Safety-related communication in closed transmission systems) [3].

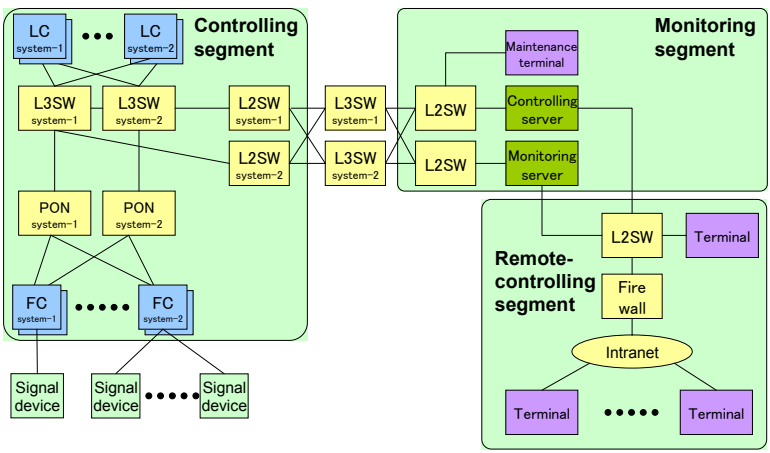



Figure 5: Network configuration of this system.

#### 4.1.1 Preconditions for applying IEC62280-1

In order to evaluate the compliance with this standard, we checked the preconditions for applying the standard (Table 1).

Table 1: Preconditions for applying IEC62280.

| | |
|---|---|
| Pr1 | The transmission system is closed. |
| Pr2 | The number of pieces of connectable equipment - either safety-related or not - to the transmission system has to be known and fixed. |
| Pr3 | The physical characteristics of the transmission system (e.g. transmission media, environment under worst case conditions, …) are fixed. |

The control segment of our system is compliant with the preconditions as following particulars.

1) The network of the control segment is logically independent, and traffic generated by the transmission in the segment is recognized and fixed.

2) The traffic from the monitoring segment to the control segment does not exceed the upper limit defined by the system specification.

3) Remote-controlling terminals access the control segment with the authentication by the controlling server and the monitoring server.

4) We define the upper limit for the number of FCs and the traffic in the control segment, which is much less than the traffic limitation.

### 4.1.2 Compliance with the requirement

In this system, since the transmission devices and protocol are based on the general technologies, it is impossible to restrict errors occurred in the transmission system. Therefore we need to assume all kinds of data errors and time delay errors, and the system is designed to control the signal devices to the safe status when transmission error is detected by the LC or the FC. Since the transmission device does not generate a valid command for safety, we do not consider it. We have confirmed the compliance with the safety integrity requirements (Table 2), the requirements for communication between safety-related equipment (Table 3), and the safety code requirements (Table 4). The compliance with these requirements is explained as follows.

Table 2: Safety integrity requirements.

| | |
|---|---|
| R1 | Safety protection shall be applied to the generation of the data to be transmitted. |
| R2 | Safety reaction shall be applied in case of misoperation. This shall be consistent with the safety requirements of the receiver. |
| R3 | Error detection mechanism shall be applied at the receiver and shall be consistent with the safety requirements of the receiver. |
| R4 | The implementation of the safety reaction R2 shall be functionally independent of the non-trusted transmission system. |
| R5 | The residual data error rate of the safety-related transmission system for each information interchange between transmitter and receiver shall be less than a predefined value. This rate shall be compatible with the SIL of each receiver. |
| R4 | The SIL of the safety-related transmission system shall be consistent with the highest SIL of the safety processes. |

Table 3: Requirements for communication between safety-related equipment.

| | |
|---|---|
| R7 | If the source is not uniquely identified in the transmission system, authenticity shall be provided by adding a source ID to the user data. |
| R8 | Integrity shall be provided by adding a safety code to the user data. The safety process shall not rely on the transmission code generated and checked by IC being part of the non-trusted transmission system. |
| R9 | The timeliness of user data shall be provided by adding time information to the user data. |
| R10 | If necessary the sequence of messages shall be checked by the safety process. |
| R11 | The safety procedures for the safety-related equipment shall be functionally independent of the procedures used by the non-trusted transmission system. |
| R12 | All safety-related equipment shall monitor the performance of the requirements listed in R7, R8, R9, and R10. If the quality of the transmission falls below a level, which is predefined in the system requirement specification then an appropriate safety reaction shall be triggered. |

Table 4: Safety code requirements.

| | |
|---|---|
| R13 | Safety-related and non-safety-related messages shall have different structures achieved by applying a safety code to safety-related messages. |
| R14 | The safety procedures of the safety-related equipment shall be functionally independent from the procedures used by the non-trusted transmission system and by the non-safety-related equipment. |
| R15 | To fulfil the required SIL, it is necessary to detect and act on typical faults of the non-trusted transmission system. |
| R16 | To fulfil the required SIL, it is necessary to detect and act on typical errors. |
| R17 | The safety code shall be functionally independent from the transmission code. |
| R18 | The safety code shall guarantee that the non-trusted transmission system shall be very unlikely to be able to generate a correct safety code word. |

1) Both the LC and the FC are safety-related devices. (R1, R13, R14)

2) If the LC detects an error, the LC controls the FC to the safe status. If the LC or the FC detects an error in received information, it transfers the information to the safe status. (R2, R3, R10, R12, R16)

3) The FC has exclusive two modes. One is a normal mode which controls signal device by the safety-related data. The other one is a maintenance mode which controls it by non-safety-related data.

4) The system fulfils the highest safety integrity level (SIL 4) collectively. (R5, R6)

5) We assign each signal device with uniquely identified number, and add it to the command data and the result data. The LC and FC apply it to recognition of the source and the address. (R7)

6) The LC transmits the command data with a Cyclic Redundancy Check (CRC) code to the FC, which detects errors. (R8, R10, R12)

7) The LC and FC detect a time delay of the transmission and an unreceived error by the sequence number and the out-of-time flag. (R9, R12)

8) If the LC detects a data error or a time error in the transmission system, it controls the FCs to the safe status. (R15)

9) The information assigned in the transmission system does not use the information for check of the safety. (R17)

10) The transmission device does not generate a valid command. (R18)

### 4.1.3 Development of the protocol detecting the delay

Since the LC is not synchronized with the FC, in our system the LC or the FC has examined the timeout independently to detect the delay in the transmission system. In order to detect the delay in the data flow process, we have developed the new protocol which utilizes the flag to notify the failure of the transmission path between the LC and the FC mutually. And we named this flag "out-of-time flag" (Fig.6). The improved protocol is as follows [4].

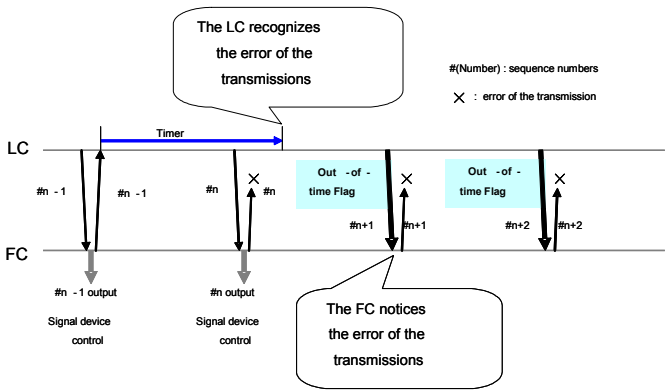



Figure 6: Protocol of detecting the delay.

In this protocol the delay and other errors about transmission such as the disorder of the sequence numbers, incorrect deliveries of the commands, or errors of the CRC in the LC/FC are dealt universally.

a) Notifying of the errors detected by the LC to the FC

In case the data flows from the FC to the LC are incorrect, the LC sets the out-of-time flag to the next command data toward the FC. When the FC receives the out-of-time flag, it recognizes the data which includes the flag may be incorrect.

b) Notifying of the errors detected by the FC to the LC

In case the FC detects the errors in the transmissions, the FC does not send the feedback to the LC. As a result the LC recognizes that the FC detected the errors.

Moreover, while the flag is active, the LC and the FC change their states to the irregular states. When the transmission path changes in a good state, the LC resets the flag and the FC recognizes the recovery of the transmission paths. This procedure is applied to each transmission path independently. In spite of utilizing the UDP for the communication, the assistance of the out-of-time flag enables us

to detect the fault of the transmission paths immediately, and operate the LC/FC adequately in case the commands are in bad states.

### 4.2 Requirements of reliability

#### 4.2.1 Target of communication error rate

In the railway signalling system, high level of reliability is also required. In order to fulfil the requirement, it is necessary that the MTBF is more than the lifecycle (20 years) of this system. Thus the failure rate of the system should be less than $10^{-6}$/h ~ $10^{-7}$/h. In order to realize this rate, the communication error rate of each device should be about $10^{-5}$/h. However, in case of a huge-scale station (more than 300 FCs), the rate of each device becomes high. Therefore, we have defined the target of the communication error rate of each device less than $10^{-7}$/h. In order to fulfil the rate, all electric devices (the LC, PON, FC etc) are duplicated [5].

#### 4.2.2 Evaluation of transmission performance

In this system, the transmission band from the LC to the FC (UDP broadcast) is 100Mbps, and that from the FC to the LC (UDP unicast) is 3Mbps per one FC. In this condition, we measured the traffic limitation (Table 5).

Table 5: Capacity of transmission.

| Transmission aspect | Traffic limitation (kbps) |
|---|---|
| From the LC to the FC | 79,591 |
| From the FC to the LC | 2,268 |

This result means that the LC can transmits about 10,000 Ethernet flames in a transmission period (200ms), and the FC can transmits about 300 flames in a same period. We have confirmed that this performance is good enough.

Further, we measured the transfer delay (Table 6). The transfer delay is much less than the transmission period.

Table 6: Transfer delay.

| Transmission aspect | Maximum delay (ms) |
|---|---|
| From the LC to the FC | Nothing |
| From the FC to the LC | 5.293 |

As these results, we have confirmed that the transmission performances sufficiently meet the traffic limitation condition, and the reliability regarding the transmission is ensured.

## 5 Conclusion

We have developed a new railway signalling system based on IP-network. By using the Internet technologies, we have realized the signal control by the

command data transmission, which leads to the drastic reduction of copper wires. Further, we have developed a safety-related transmission method, and verified that the method complies with IEC62280-1 requirements.

We have evaluated the safety and reliability of this system for two years with prototype system at a real operation condition. And with this evaluation's result, we put this system into practical use at Ichikawaono station on the Musashino line in February 2007.

## References

[1] F.Kitahara, "ATOS System for Realization for Realization of New Transport Operation Control", Rail International, UIC, No.6, PP.14–22, 1996.
[2] Y.Hirano, et al., "Development of Railway Signaling System based on Network Technology", Proc. of IEEE SMC, Oct.2005.
[3] IEC62280-1 Railway applications - Communication, signalling and processing systems -
[4] T.Kunifuji, et al., "A Consideration of Safety-related Transmission for Signal Control System based on Network Technology", Reliability Engineering Association of Japan, Nov.2006 (in Japanese)
[5] T.Kuifuji, et al., "A Design of Safety and Reliability for Safety-related Control System based on IP-Network", Reliability Engineering Association of Japan, Nov.2005 (in Japanese)