Special edition paper

Development of an Integrated Logical Controller






Tatsuya Shigeta* Hideo Maruyama* Hiroshi Ito* Yoshinori Saiki* Yohei Niibori** Takashi Kunifuji*

Through the previous development of an IP Network-based Signal Control System, we realized reduction of metallic cables, improvement in installation and simplification of operation tests by replacing voltage control with information control through an optical fiber network. On the other hand, the logical devices to determine control information of signal devices still exist separately according to functions such as those for interlocking equipment and the ATP controller, and those devices remain complex. This complex configuration causes complicated design, installation and maintenance of the system and decreases its availability.

To solve these issues, we developed an Integrated Logical Controller (LC), a set of high-performance computers integrating logical devices in a signal house, and produced prototypes for that. The prototypes were temporarily installed to existing stations, and the adequacy of the control logic was verified for practical use. In addition, prior to developing the practical system, issues in terms of its actual use were clarified and the methods to solve them were considered.

●Keywords: Network, Reliability, Safety, Interlocking, Automatic train protection (ATP), Railroad crossing

1 Introduction

Railway service improvements such as expansion of through service over multiple lines and increase of service have been in high demand recently. To meet these customer needs, the signaling system needs to be upgraded. At the same time, much interlocking equipment is about to reach its service life and needs to be replaced within the next several years. However, signaling systems are designed with a focus on high safety and reliability, bringing about complications in installing and upgrading.

With a goal of easy installation (i.e. shortening the construction period and improving construction work), the new "IP Network-based Signal Control System" signaling system that achieves information control of the signal devices in the field and improves flexibility of their upgrading has been developed. By developing this system, field device control was changed from voltage control to information control through an optical fiber network, thus achieving a reduction of metallic cables, easy installation and simplification of operation tests.

On the other hand, the logical devices to determine the control information of the signal devices still exist separately according to functions such as those for interlocking equipment and the automatic train protection (ATP) controller, and they remain complex. This complex configuration causes complications in designing, installing and maintaining the system, and it decreases the system's availability.

To solve these issues, we have been developing an Integrated Logical Controller (LC), a set of high-performance computers integrating logical devices in a signal house. In this paper, development of the LC and the development policy towards achieving a practical system will be described.

Table 1 Challenges and Policy of Signaling System

No.	Issues	Examples	How to solve
1	Huge amount of construction work and difficulty in quality control for that	· Huge amount of cable laying, wiring work and connection tests	<Solved by the IP Network-based Signal Control System> · Major reduction of cable laying and wiring work by use of the network · Major simplification of operation tests by use of information control
2	Securing high reliability as a total system	· Existence of potential factors of system disorder · Difficulty in correspondence between various devices	<Countermeasures by system architecture> · Integration of all functions to one set of fail-safe computers · Adopting dual-duplex system · Unifying the interface to be Ethernet TCP/IP
3	Increasing trouble in designing	· Difficulty for designer to grasp the adequacy of designing intuitively · Procedures not unified in designing and processing among functions such as those for interlocking equipment and railway crossings	<Countermeasures by control logic> · Unifying similar process and sharing by the entire system <Countermeasures by data> · Standardizing the format of control information and enabling it to analyze the affected range in partial upgrading
4	Many operation tests at the installation site	· Existence of operation tests which cannot be performed in the factory	<Minimization of limitation> · Enabling gradual expansion of different system and reduction of operation tests at the installation site
5	Difficulty in securing upgrading time	· Difficulty in securing enough time for upgrading and operation tests · Difficulty in halting the system to allow installation	<Realization of upgrading while the system is in operation> · Procedure for partial stop and upgrade of the software · Online upgrading feature to enable temporary existence of different versions of software
6	High costs for installing and upgrading	(will be solved by solving the issues above)	—

*Advanced Railway System Development Center, Research and Development Center of JR East Group
**JR East Tokyo Electrical Construction And System Integration Office (previously at Advanced Railway System Development Center)

2 Concept

2.1 Issues of the Signal Control System and Their Solutions

Issues of the current signal control system have been analyzed and six of those were picked up. Examples of those issues and their solutions were also considered (Table 1).

Although issue No. 1 was solved by introducing the IP Network-based Signal Control System, issues No. 2 through No. 6 still remain. Among these, No. 2 causes traffic suspension due to a complex system configuration and interface. No. 3 causes complications and rework in design because the check of design adequacy depends on human attention. Therefore, No. 2 and 3 are considered to be principal issues.

For this reason, "increase of the total reliability by integrating logical devices" and "simplification of designing by reconstructing control logic" were set to be the principal concepts, and development of the integrated logical controller (LC) was started.

2.2 Schedule

The development schedule of the LC is shown in Fig. 1. The basic development began in fiscal 2007, followed by the field tests and verification of the control logic from fiscal 2008 to 2010. From fiscal 2010, formulation of the basic specifications as development of the practical system began, and full-scale development began in fiscal 2011.

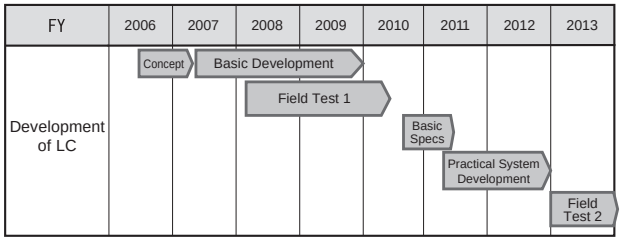


Fig. 1 Development Schedule

3 Outline of the Development

The development items of the LC are shown below.

(1) Improvement of reliability as a total system

The logical devices, conventionally provided by individual function, will be integrated into one set of high-performance reliable computers (Fig.2). By this integration, many interfaces between the conventional devices that have been the weak points for securing reliability will be reduced. In addition, integration simplifies configuration control among multiple systems and eliminates troubles related to configuration control.

Moreover, the logical controller adopts a dual-duplex configuration of fail-safe computers, and thus it can eliminate output matching by majority decision control and configuration control. That feature improves controller availability.

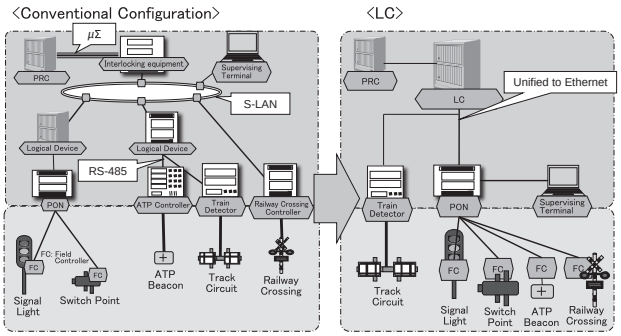


Fig. 2 Integration of Logical Devices

(2) Simplification of design work

Control logic that is conventionally constructed separately is reconstructed on a common platform, and a software architecture with this platform makes it possible to localize the area affected in upgrade of data and functions. In addition, design support software that reduces design work by centralizing logic data will also be created.

(3) Simplification of operation tests at the installation site

By integration of control logics, connection tests between devices that are conventionally performed at the installation site will be possible in the factory.

(4) Cost reduction

Cost reduction as a total system is pursued by reducing hardware by integration, dual-duplex configuration, centralizing data, creating data by design support software and replacing operation tests at the installation site with factory tests.

3.1 Development of the Integrated Logical Controller

3.1.1 Structure of the System

Primary development of the LC was implemented in order to confirm the adequacy of its hardware and the control logic. The entire configuration of the system is shown in Fig. 3. This system is roughly divided into four blocks: LC block, field controller (FC) block, supervising block and interface block. The connection between the blocks is unified to use Ethernet. Different network segments are assigned to each block so that unnecessary data will not flow into an undesignated block. The structure of each block is as follows.

(1) LC block

This block consists of LC hardware (dual-duplex) and processes all the control logic within a station.

(2) Field controller (FC) block

This block consists of a PON network (conveys control and status data between LC and FC and supervising information between FC and supervising terminal) and field controllers (built-in computers that control the field signal devices based on control

data from the LC)

(3) Supervising system block

The supervising system is an integrated remote control and observation system for the LC system and IP Network-based Signal Control System (inside and outside a station yard). This system consists of a remote observation server (that collects operation status), remote control server (that processes the remote control commands for each system) and supervising terminal (for human interface).

(4) Interface block for adjacent system

This block connects with adjacent signal devices or systems such as the IP Network-based Signal Control System for Block Signal outside a station yard, adjacent LC and non-network based signal devices outside the station that LC is responsible for. Connection is by relays, RS-485 or Ethernet. For devices without Ethernet connection ports, hardware for a connection converter will be developed and the connections to the LC will be eventually unified to Ethernet.

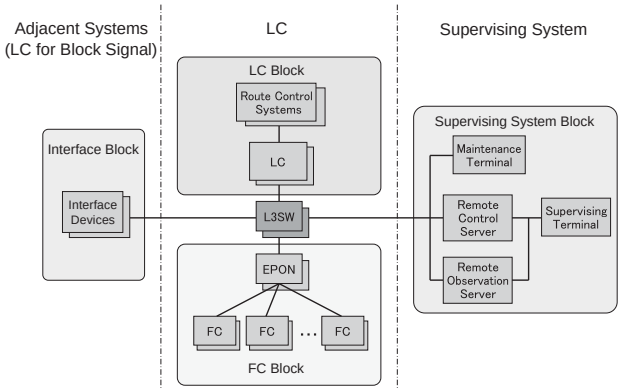


Fig. 3 System Configuration around LC

3.1.2 Data Sharing Through a Database

Conventional signal devices communicate their control information directly among each other. Each device thus needs to hold the control data, and it consequently holds the data from multiple devices.

On the other hand, the LC has an integrated structure, so holding all of the data by each function is inefficient. For this reason, we adopted a structure whereby the common control data for all functions is stored to the place shared by all the functions and all of them read and write the shared data instead of communicating between the functions (Fig. 4). This way, each function does not need to hold the same data redundantly, and thus redundant processing will be eliminated. Moreover, as the control data is unified to be shared data for all the logical functions, interface specifications for each device or bit allocation for each station does not need to be defined.

By integrating logical devices and adopting shared data, the shared data can be read uniquely; every function can obtain the same data in the same way.

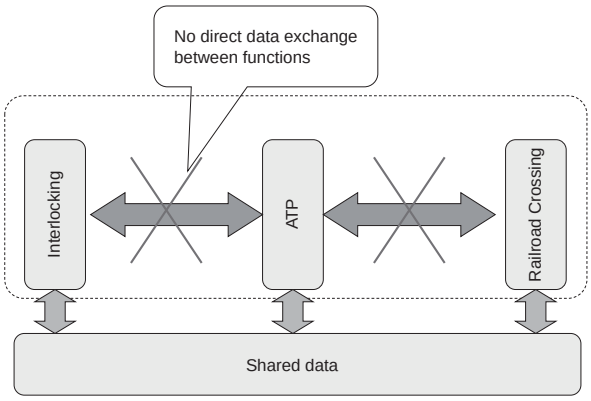


Fig. 4 Data Structure of Shared Data

3.1.3 Reliability of the System

The reliability block diagram of the conventional system and an LC system with the IP Network-based Signal Control System is shown in Fig. 5. As the conventional system uses the existing interlocking equipment to limit the volume of new development, its diagram has series construction. In contrast, the LC combines the logical part of the signal house (FCP) and the interlocking (FX), and it processes both of them. By this configuration, the failure rate of the LC will be reduced to one fifth that of combination of the conventional interlocking equipment and the IP Network-based Signal Control System. This is thanks to the reduction of parts by removing the internal network (S-LAN) and the field device control part (ACP).

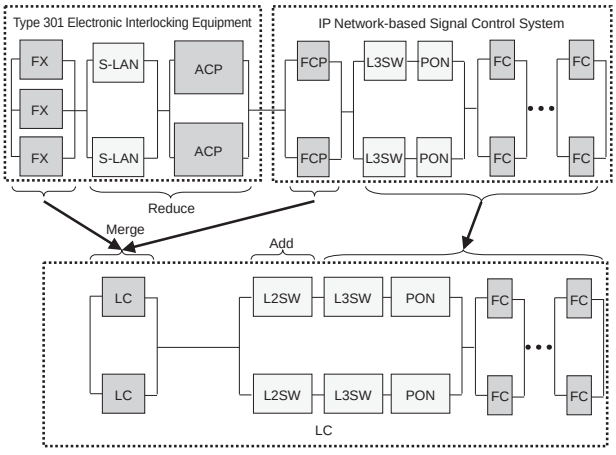


Fig. 5 Reliability Block Diagram

4 Prototypes of LC and Their Evaluation

Prototypes of LC with the concept of section 3 were manufactured and evaluated. Evaluation of their reliability and the control logic by field tests and simulation are described in this section.

4.1 Verification of Control Logic by Field Tests

In order to verify the adequacy of the control logic, field tests that compare the control timing with the existing interlocking equipment and the prototype LC were implemented.

4.1.1 Method of the Field Tests

The field tests were implemented at Minami-Matsumoto Station on the Shinonoi Line and at Iwanuma Station on the Tohoku Line. The target devices to compare the control timing through the field tests are shown in Table 2.

To enable route control and signal device control by the LC, information of the existing relay interlocking equipment route control and the train detection information need to be transmitted to the LC. In addition, to compare control timing of the relay interlocking equipment and the LC, the controlled results of the signal lights, railroad crossings and ATP of the relay interlocking equipment need to be obtained in real-time. In these field tests, the information is obtained by the relay contacts or the current sensors if those contacts are not available.

Table 2 Devices for which to Compare Timing in Field Tests

Devices		Minami–Matsumoto	Iwanuma
Route, Levers	Home/Starting Signal	16 routes	20 routes
	Shunting Indicator	76 routes	119 routes
	Check Lever	4 routes	0 routes
ATP Beacon		22	27
Warning Route of Railway Crossing	Outbound/inbound	10 routes	10 routes
	Shunting	0 routes	12 routes

Verification by the field tests is performed by comparing the timing of the control outputs obtained by the comparison detector from the LC and the relay interlocking equipment. (Fig. 6, 7)

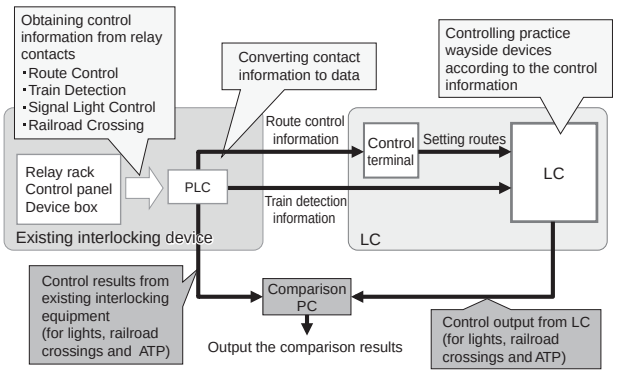
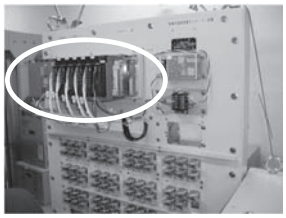


Fig. 6 Concept of the Field Test

LC

Interlocking terminal and comparison PC



PLC

Fig. 7 Configuration of Field Test Equipment

4.1.2 Evaluation of Field Tests

Field tests were implemented from June 2008. While some troubles occurred at the beginning, no additional troubles caused by LC control logic have occurred after fixing them. The evaluation term was set to be after the functions for control of interlocking equipment, ATP and railway crossing were introduced to LC. Actual terms were from June 27, 2009 to September 9, 2009 for Minami-Matsumoto and from December 4, 2009 to January 31, 2010 for Iwanuma. The total number of times control was implemented and the number of mismatched control are shown in Table 3.

Mismatched control was investigated and the LC specifications related to them were evaluated. The contents and the evaluation of the mismatches are shown in Table 4.

Table 3 Mismatch Occurrence

	Minami–Matsumoto		Iwanuma	
	Times Control Implemented	Mismatch	Times Control Implemented	Mismatch
Interlocking	139,476	647	61,452	3,679
ATP Control	128,728	29,836	98,877	6,883
Railway Crossing Control	13,616	28	25,372	15

Table 4 Evaluation of Mismatches

Functions	Contents	Evaluation
Interlocking	(1) Slight difference of control timing (Timing of simulated switch points was different.)	Differences caused from scanning and the spec difference* between relay interlocking and LC. No problems found in LC specs.
	(2) Delay of scanning of PLC	
	(3) Spec difference of relay interlocking and LC	
ATP Control	(1) Spec difference of relay interlocking and LC	Differences caused from spec and coverage of devices. No problems found in LC specs.
	(2) Difference from control definitions (ATP controls of shunting indicators designated to LC were not covered by the relay interlocking.)	
Railway Crossing	(1) Spec difference between relay control and LC (Difference in warning stop timing)	Mismatch caused by spec difference* between relay interlocking and LC. No problems found in LC specs.

* LC specifications are based on those of general electronic interlocking. As the spec differences between general electronic interlocking and relay interlocking are known, the mismatches were considered not to be a problem.

Concerning the mismatches occurred in these field tests, no problems requiring reconsideration of LC specifications were found. Therefore, difference from the specification of relay interlocking also was considered to be adequate in terms of LC operation.

4.2 Verification of LC Control Logic by Simulation

In the evaluation by field tests, adequacy of operations that do not exist at Minami-Matsumoto and Iwanuma Stations was not verified. In addition, when introducing the general electronic interlocking equipment, there were some functional improvements made to deal with operation that were unexpected at the time of development. Therefore, we verified the presence of issues in deploying the LC to stations through test cases.

4.2.1 Method for Verifying Control Logic

The procedure of verifying LC control logic is as follows. First, test cases to verify were extracted. Desk analysis was performed for the cases, and existence of issues in control logic was checked. For some cases that need dynamic analysis of train run timing, verification by simulation was executed by the plant simulator using the model stations of Zushi (Yokosuka Line) and Koganei (Tohoku Line).

4.2.2 Extraction of Test Cases

(1) Interlocking

Based on the "Writing Rules of the Interlocking Table," test cases from writing in the table were extracted and verified as to whether LC specifications could deal with them. In addition, the functionally improved cases in introducing general electronic interlocking in the past were also considered and evaluated.

(2) Railway crossing

Based on the "Writing Rules of the Railway Crossing Control Table," test cases of warning conditions or warning stop conditions were extracted and verified. In addition, cases of past control disorders and their countermeasures, operation of substitution lever of railroad crossing and control in failure of train tracking were compared with existing railway crossings and evaluated.

(3) ATP control

For ATS-S and ATS-P devices (types of ATP), test cases were extracted from all of the control tables of general electronic interlocking introduced in the past. Especially for ATS-P, cases of the past transport disorders derived from inappropriate design were evaluated.

(4) Supporting Equipment Control

For control trigger for next station, automatic guidance, train approach indicator, clearance indicator of the train end and the train approach warning device, test cases were extracted from their control tables of introduced general electronic interlocking equipment and evaluated.

4.2.3 Simulation Results and their Evaluation

As a result of the verification, some issues were found derived from LC specifications. Their countermeasures were considered, however, and therefore developing a practical system based on the current specifications was considered not to be a problem.

4.3 Evaluation of Introduction Costs

The cost of LC hardware for stations of 30 routes was compared with that of general electronic interlocking equipment. While general electronic interlocking equipment consists of multiple fail-safe computers (FxR, FCP and ACP), the LC has only one set of fail-safe computer integrating these computers. The cost of the hardware is thus reduced over that of interlocking equipment. Moreover, by integrating ATP controllers, about 10% of the entire costs of equipment in the signal house are expected to be reduced. However, the gross construction costs for introducing the LC needs to be evaluated by the site to which it is installed because costs depend on external factors such as daily time assigned to construction and degree of facility transfers.

5 Issues in Practical Use of the LC and their Solutions

The control logic of the LC prototype was verified to be adequate through field tests that compare the control results between the LC and conventional devices. In addition, a certain level of improvement on availability and cost reduction can be expected. Therefore, start of development of the LC towards its practical use was decided. We then picked out the issues in practical use and considered their countermeasures. In this section, that consideration will be described.

5.1 Division of Processing by Functions and Configuration of Data

The LC integrates functions of interlocking, ATP control, railroad crossing and supporting equipment control into one logical device. As described before, the adequacy of integrated control logic was verified through field tests and simulation. In addition, improvement on reliability and cost reduction through integration and consequent reduction of hardware was also confirmed.

On the other hand, by integrating multiple control logic functions into one device, the range affected by maintenance or partial disorder was expected to be large. Especially, once the interlocking function stops, the function to secure safety for other maintenance workers will stop at the same time and the other maintenance work will need to be canceled. We traditionally have trouble in conflict adjustment between the upgrading work of interlocking equipment and other maintenance work, and therefore the interlocking function needs to be prevented from stopping. To prevent stopping, LC software architecture and function of software upgrading were reconsidered.

5.1.1 Range Affected in Software Upgrading or Partial Disorders

Software in protective devices is created to keep the designed order of processing for their safety as the top priority. In this viewpoint, a program that operates in one logical device is basically created as single thread program. The software of the LC prototype was created as single thread and the functions of interlocking, ATP control, railroad crossing and supporting equipment control and their control data consist of one program.

However, if the software of the LC is made as single thread, the following troubles seem to occur.

(1) Expanded range affected in software upgrading

If the software consists of one program, the whole software needs to be reconstructed even in partial upgrading. Moreover, by reconstructing the whole program, operation tests also need to be performed over a larger range.

(2) Increased possibility of partial disorder affecting other functions

If the software consists of a single thread, the functions are not independent and another function's data can be read or written freely. Therefore, in case of software disorder, another function's data or even its program itself can be destroyed in this software architecture.

(3) Expanded range affected in partial upgrading

In changing the ATP control message, for example, the entire LC may need to be stopped. In contrast, just corresponding ATP encoders need to be stopped to replace the message ROM in conventional configuration.

5.1.2 Dividing Processing by Functions and Keeping its Independence

To limit the affected area to the corresponding function in upgrading or partial disorder, independence between functions needs to be established. For this reason, adopting a software architecture divided by functions in a practical system of LC is considered (Fig. 8).

To maintain independence between subsystems, each subsystem is created as a task and is set unable to directly access the other subsystems.

By this protection, even if there is a bug in the software or some other disorder, the task with a problem cannot destroy other programs or data. In this way, disorders are prevented from affecting other functions.

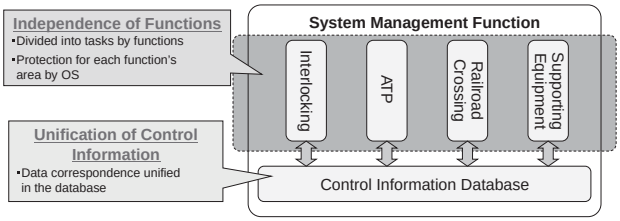


Fig. 8 Divided Software Configuration

In addition, a control information database evolved from shared data adopted in the prototype was established and all of the data correspondence is considered to be executed through the database. In addition to the control information to share between logical subsystems, each subsystem's operation status is stored in the control information database. By this configuration, the subsystems can secure independence, therefore limiting the range of reconstruction or operation tests in partial upgrading.

In general, a multi-task configuration utilizes CPU power effectively. Therefore, when the subsystem executing is waiting, the subsystem next in priority will be called and started. However, in protective devices, the processing order must be kept for safety reasons. To fulfill this requirement, the LC system management subsystem centrally manages the other subsystems' operation and keeps the processing orders. It also monitors so as not to start another task when the current process is waiting.

5.2 Improvement of System Maintainability

Constructing logical processing with tasks divided by functions enabled stopping of a certain subsystem for maintenance. In other words, the system management function enables abortion of processing by a subsystem in maintenance or partial disorder. During the partial abort, the system management function records each subsystem's operation status to the control information database. The other running subsystems can detect the aborted subsystem by referring the database (Fig. 9).

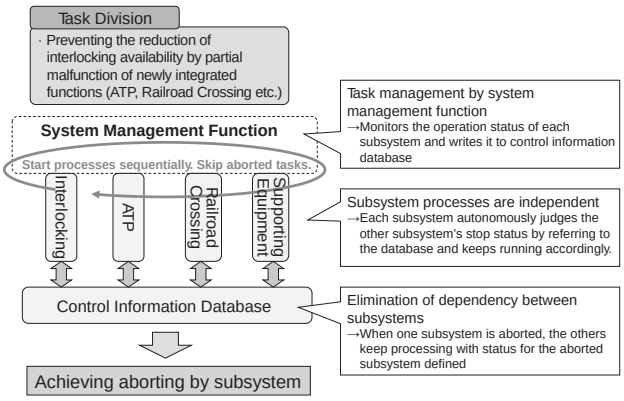


Fig. 9 Improvement of Maintainability

5.3 Achieving Non-stop Upgrading of Software

The signal control system usually exchanges control information or software version information among multiple systems, and the system will stop for safety reasons when detecting a mismatch. Due to this feature, software upgrading is executed with the system stopped so as not to detect the mismatch. As described before, once the interlocking function stops, its effect is very large. Therefore, upgrading without stopping was considered.

5.3.1 LC Maintenance Mode

As conventional fail-safe system with two out of three system configuration secures a fail-safe condition by monitoring to check that control results are the same, mismatch of software versions among multiple systems is not permitted. On the other hand, the LC dual-duplex system can maintain the fail-safe condition only for one system. Utilizing this feature, we considered achieving non-stop upgrading with the "LC maintenance mode" that allows temporary mismatch of the software version.

The definition of LC maintenance mode is as follows.

(1) Allows mismatch of the software versions between master and slave systems.
(2) Stops output for slave system upstream and downstream devices.
(3) Switches between master and slave systems without interruption.
(4) Provides no control for the other system.
(5) Does not allow automatic switching of master and slave systems.
(6) Carries over set maintenance work.
(7) Can be released only when the software versions match or only a master system exists.

5.3.2 Non-stop Upgrading by LC Maintenance Mode

The flow of non-stop upgrading by using the LC maintenance mode is shown in Fig. 10.

First, by setting LC maintenance mode in (1), the slave's output stops. After upgrading the slave's software in (2) and switching the master and slave in (3), the output now comes from the previous slave. At this time, the output is generated by the upgraded software. As switching between master and slave is executed without interruption, the software upgrading can be done without interruption. However, when the upgrading involves change of lines, the assignment of devices also needs to be changed, and data carryover between master and slave is unavailable. This means the entire system needs to stop for such upgrading.

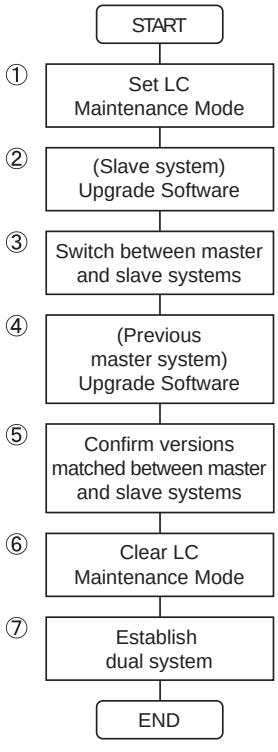


Fig. 10 Software Upgrading Flow

5.4 Reducing Design Work by Design Support Tool

One aim of the LC is to achieve flexible upgrading. The current signal control system requires considerable effort for designers to make the design tables because the range affected by the upgrade cannot be specified easily. Moreover, because checking the consistency between the tables relies on human attention, the designer's burden is increasing.

Therefore, a design support tool is being created to enable the integrity check between tables by simple procedure of extraction. By this tool, extraction of the corresponding data can be performed automatically and the design work will be reduced.

We have so far developed a design support tool capable of centralized management of tables and forms for LC control. Development of its user interface that will lead to support actual design work remains an issue to overcome.

6 Conclusion

The prototype LC was developed to improve reliability of the total signal system, workability for upgrading and flexibility for upgrading. Adequacy of developed functions was verified through field tests implemented at Minami-Matsumoto and Iwanuma Stations by comparing the control results from the LC and the relay interlocking. Verification by a simulator and cost evaluation also brought good results. In light of these results, development for practical use of the LC has started.

Operational issues have been clarified upon practical use and the solutions for them were considered. We will strive to develop a practical LC system according to the established policy.

Reference:

1) Takashi Kunifuji, Jun Nishiyama, Masafumi Endo, Yoshinori Saiki, Satoshi Fukui, "Development of a Network-based Signal Control System for Station Yards," *JR East Technical Review* No. 15 (2009): 20–26

2) Hiroshi Ito, Takashi Kunifuji, Tetsuya Okada, Tetsuo Hashimoto, "Kairyo-koji ni Junan na Shingo System no Kaihatsu [in Japanese]," *Proceedings of 47th Symposium on Railway Cybernetics* (2010): 609

3) Takashi Kunifuji, Yoshinori Saiki, Satoru Masutani, Masayuki Matsumoto, "Reliability of the IP Network-based Signal Control System and the Integrated Logical Controller," *FORMS/FORMAT 2010* Part 2 (2010): 117–124,

4) Jun Nishiyama, Tetsuya Okada, "Eki Konai Ronri Sochi no Kaihatsu [in Japanese]," *JR East Technical Review* No. 20 (2007): 35–37

5) Fumio Kitahara, Takatoshi Miyazaki, Keiichiro Watanabe, "Tokyo-ken Yuso-kanri System ni okeru Shin Denshi-rendo-sochi [in Japanese]," *Railway and Electrical Engineering* Vol. 5, No. 1 (1994): 25–30

6) *IEC 62280-1 Railway applications - Communication, signalling and processing systems* (IEC, 2002)

7) Takashi Kunifuji, Yoshiyuki Hirano, Hiroyuki Sugawara, Dai Watanabe, Tomoaki Kouda; "IP Network o Kiban to Shita Hoan Segyo System no Anzensei/Shinraisei Sekkei [in Japanese]," *Autumn symposium of the Reliability Engineering Association of Japan* (October 2005)

8) Takashi Kunifuji, Yoshiyuki Hirano, Jun Nishiyama, Masayuki Matsumoto; "Hanyo IP Network o Katsuyo Shita Shingo Segyo System no Anzensei ni tsuite [in Japanese]," *Safety study group, the Institute of Electronics, Information and Communication Engineers* (October 2007)