Development of an integrated signal control system and consideration for its practical use

H. Ito[1], T. Shigeta[1], Y. Niibori[1], Y. Umehara[2], M. Hokari[3] & T. Kunifuji[1]
[1]*East Japan Railway Company, Japan*
[2]*Hitachi Ltd., Japan*
[3]*Toshiba Corporation, Japan*

Abstract

The current signalling system in a machine room has a complex configuration, as additional devices like the automatic train protection (ATP) controllers have gradually been installed to raise the safety level. At the same time, these devices and interlocking interact complexly with each other. This complex configuration consequently causes complexity in designing, installing and maintaining the system, and decreases the availability of it. To solve these issues, development of the integrated signal control system, "Logical Controller" (LC) is in progress. LC is a set of high-performance computers integrating the logical devices in a machine room. Toward the practical use of the LC, there are two major challenges: construction and verification of the integrated control logic, and minimization of the range affected in partial software upgrading or partial malfunction. In this paper, the outline of the LC is described and the techniques for solving the above-mentioned challenges are discussed.
Keywords: safety, reliability, control logic, integration, practical use, maintenance.

1 Introduction

Recent sophistication of the customers' needs for railway transport requires better services, such as speed up, more frequent services and extension of direct operation over multiple lines, as well as the safe and accurate transport. To realize these services promptly, capacity for easy upgrading is required for signalling system.

www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/CR120591

With a goal of easy installation, the IP Network-based Signal Control System that achieves information control of the signal devices in the field and improves the flexibility of their upgrading has been developed by Kunifuji *et al.* [1, 2]. By developing this system, field device control was changed from voltage control through metallic cables to information control through an optical fiber network, and thus a reduction of metallic cables, easy installation and simplification of operation tests are achieved.

However, the logical devices to determine the control information installed in a machine room have a complex configuration, as additional devices like the automatic train protection (ATP) controllers have gradually been installed to raise the safety level. At the same time, these devices and interlocking interact complexly with each other. This complex configuration consequently causes complexity in designing, installing and maintaining the system, and decreases the availability of it. This represent that current system has limitation to meet the customers' needs instantly.

To solve these issues, we have been developing the integrated signal control system, "Logical Controller" (LC) [3, 4]. LC is a high-performance computer integrating the logical devices in a machine room. Toward the practical use of the LC, there are two major challenges. First, the control logics of interlocking, ATP, railroad crossing and other signal related devices must be integrated and reconstructed, and the integrated control logic needs to be tested and verified. To verify the adequacy of the logic, field tests and in-plant tests were performed by using the prototype machine. The second challenge is to minimize the influenced range due to partial upgrading or partial malfunction, even though many functions are integrated. To achieve it, relevant software architecture capable of high availability was contrived and assessed. In addition, actual maintenance operation of the system was considered and necessary function of maintenance was discussed. In this paper, the outline of the LC is described and the techniques for solving the above-mentioned problems are discussed.

2 Overview of the Logical Controller (LC)

2.1 Concept

The concepts of the LC are shown below.

(1) Improvement of reliability as a total system

The logical devices in a machine room, conventionally provided by individual function, will be integrated into one set of high-performance computers (fig. 1). By this integration, many interfaces between the conventional devices, which have been the weak points for securing reliability, will be reduced. In addition, integration will simplify configuration control among multiple systems and thus eliminate troubles related to it. Moreover, LC adopts a dual-duplex configuration of fail-safe computers, and therefore it can remove output matching by majority decision control and configuration control. These features improve availability of the system.

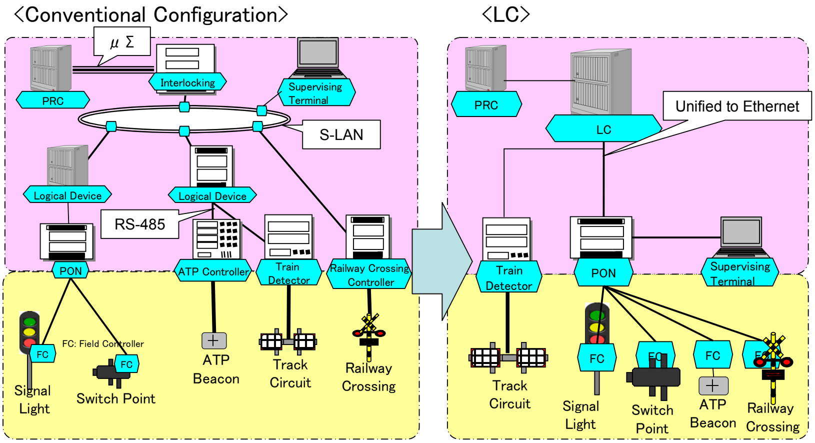

Figure 1: Integration of the logical devices.

(2) Simplification of design work

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

(3) Simplification of operation tests at the installation site

By integrating the control logics, connection tests between devices, conventionally performed at the installation site, will be feasible in the factory.

(4) Cost reduction

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

2.2 Structure of the system

Basic development of the LC was implemented in order to confirm the adequacy of its hardware and the control logic. Fig. 2 shows the entire configuration of the system. This system is roughly divided into four blocks: LC block, field controller (FC) block, supervising block and interface block. The interface 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 remote observation server) and field controllers (FCs: 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 observation and remote control system for the LC and IP Network-based Signal Control System (inside and outside a station). This system consists of a remote observation server (that collects status information of each device), 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 adjacent LC, the IP Network-based Signal Control System for Block Signal outside a station yard and non-network based signal devices outside the station that LC is responsible for. Relays, RS-485 or Ethernet are used for connections. For devices without Ethernet ports, hardware for a connection converter will be developed and the connections to the LC will be finally unified to Ethernet.

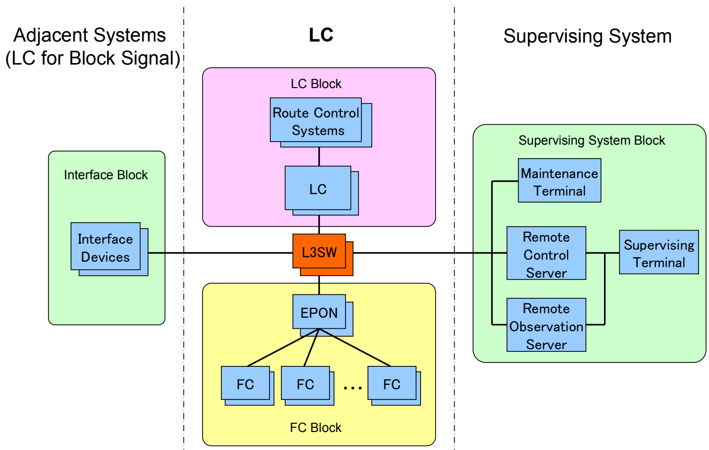

Figure 2: System configuration around LC.

2.3 Data sharing through a database

Conventional signal devices exchange their control information directly among each other. Each device therefore needs to hold the control data, and as a result it holds the data from multiple devices. On the other hand, as the LC has an integrated structure, holding all of the data by each function is inefficient. For this reason, we adopted a database where the common control data for each function is stored and shared by all the functions. All of them read and write the shared data instead of communicating between the functions. In 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 into shared data for all the logical functions, interface specification for each device does not need to be defined. By integrating logical devices and employing shared data, the shared data can be read uniquely; every function can obtain the same data in the same way.

3 Verification of the control logic

Prototypes of LC with the concept of section 2 were experimentally manufactured and evaluated. Evaluation of the control logic by field tests and simulation (in-plant tests) is described in this section.

3.1 Field tests

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

3.1.1 Method of the field tests

The field tests were performed at Minami-Matsumoto Station on the Shinonoi Line and at Iwanuma Station on the Tohoku Line.

To enable practice route control and signal device control by the LC, information of the existing relay interlocking equipment and the train detection information need to be sent to the LC. In addition, to compare control timing of the LC and the relay interlocking equipment, the controlled results of the relay interlocking equipment need to be obtained in real-time. To obtain the information, the relay contacts are used. If those contacts are not available, the current sensors are utilized.

Verification by the field tests is performed by comparing the timing of the control outputs obtained from the LC and the relay interlocking equipment and stored to the comparison PC (fig. 3).

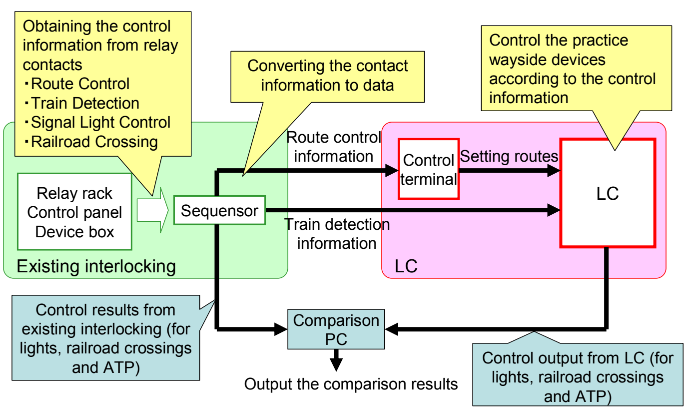

Figure 3: Configuration of the field test.

3.1.2 Evaluation of the 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. The evaluation 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, the number of mismatched control and the evaluation are shown in table 1.

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

Table 1: Mismatch occurrence.

	Minami-Matsumoto		Iwanuma		Evaluation
	Control Times	Mismatch	Control Times	Mismatch	
Interlocking	139,476	647	61,452	3,679	Differences caused from scanning and the spec difference between relaying interlocking and LC. No problem was found on LC's spec.
ATP Control	128,728	29,836	98,877	6,883	Differences caused from spec and coverage of devices. No problem was found on LC's spec.
Railway Crossing Control	13,616	28	25,372	15	Differences caused from the spec difference between relaying interlocking and LC. No problem was found on LC's spec.

3.2 Verification of the control logic by in-plant tests

In the evaluation by the field tests, adequacy of operations that do not exist at Minami-Matsumoto and Iwanuma Stations was not confirmed. In addition, when introducing the general electronic interlocking equipment [5] in the past, there were some functional modifications made to deal with operation that were not considered at the time of development. Therefore, we confirmed the presence of issues in deploying the LC to various stations through test cases.

3.2.1 Method for verification

The procedure of verifying the control logic of LC 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 confirmed. When some cases that need dynamic analysis of train run timing were found, verification by simulation was executed by the plant simulator using the model stations of Zushi (Yokosuka Line) and Koganei (Tohoku Line).

3.2.2 Extraction of test cases

(1) Interlocking

Test cases from the “Writing Rules of the Interlocking Table” were extracted and verified about whether LC specifications could deal with them. In addition, the functionally modified cases in introducing general electronic interlocking in the past were also applied and evaluated.

(2) Railway crossing

Test cases of warning conditions or warning stop conditions from the "Writing Rules of the Railway Crossing Control Table" were extracted and verified. In addition, cases of control disorders in the past and their countermeasures, operation of substitution lever of railroad crossing and control in failure of train tracking were considered and evaluated.

(3) ATP control

For ATP devices, test cases were extracted from all of the control tables of general electronic interlocking introduced in the past. In addition, cases of the past transport disorders derived from inappropriate design were evaluated.

(4) Supporting equipment control

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

3.2.3 Results of in-plant tests and their evaluation

As a result of the in-plant tests, some issues were found derived from specifications of LC control logic. However, their countermeasures were proposed and therefore starting on development of a practical system based on the current specifications was conceived not to be a problem.

4 Consideration for practical use

The control logic of the prototypes of LC was verified to be adequate through field tests and in-plant tests. In addition, a certain level of improvement on availability and cost reduction can also be expected. Therefore, start of development of the LC practical system was determined. In this section, we will clarify the issues in practical use and discuss their countermeasures.

4.1 Software configuration

The LC integrates functions of interlocking, ATP control, railroad crossing and supporting equipment control into one logical device. On the other hand, by integrating multiple functions into one device, the range affected by software maintenance, partial functional upgrading or partial disorder was anticipated to be large. To minimize the range, LC software architecture and function of software upgrading were reconsidered.

4.1.1 Range affected in partial software upgrading or partial disorders

Software in protective devices is created to secure the safety as the top priority, and thus keeping the designed order of processing is very important. In this viewpoint, a program that operates in one logical device has traditionally adopted single thread configuration. The software of the LC prototype was also created as single thread and the functions of interlocking, ATP control, railroad crossing and supporting equipment control and their control data are composed

www.witpress.com, ISSN 1743-3509 (on-line)

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

(1) Expanded range affected in partial software upgrading

If the software consists of one program, the whole software needs to be reconstructed even in partial functional upgrading. Moreover, by reconstructing the whole program, entire operation tests also need to be performed accordingly.

(2) Increased possibility of influencing other functions by partial disorder

If the software consists of a single thread, each function is not independent and another function's data is freely accessible. Therefore, in case of a function's 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 for upgrading. On the other hand, just corresponding ATP encoder needs to be stopped to replace the message ROM in conventional signalling system. This indicates decrease in maintainability.

4.1.2 Dividing a program by functions and keeping its independence

To limit the influenced range to the corresponding function in upgrading or disorder, independence between functions must be established. For this reason, adopting a software architecture divided by functions in LC practical system is considered (fig. 4).

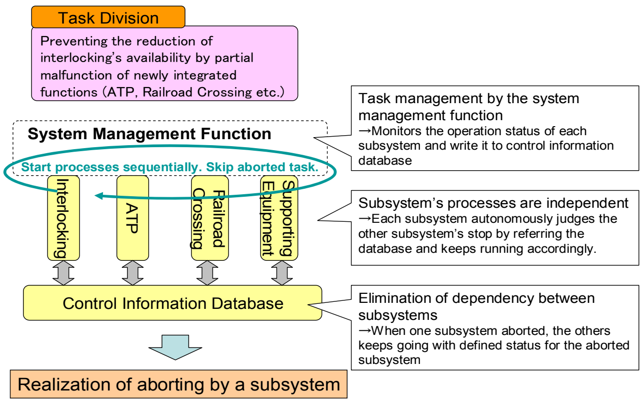

Figure 4: Divided software configuration.

To keep 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 or abnormal behaviour in the software, the task with a problem cannot destroy other programs or data. By this way, disorders are prevented from affecting other functions.

In addition, a control information database developed from shared data adopted in the prototype was contrived and all of the data is considered to be corresponded through the database. In addition to sharing the control information between subsystems, each subsystem's operation status is recorded in the database. This configuration enables the subsystems to secure independence and consequently limits the range of reconstruction or operation tests in partial upgrading.

In general, a multi-task configuration is used to utilize CPU power efficiently. Therefore, when the subsystem execution is waiting, the subsystem next in priority will be called and activated. In protective devices, however, the processing order must be kept for safety. To maintain this requirement, the LC system management function centrally manages the other subsystems' operation. It starts next subsystem after confirming the previous subsystem's completion and avoids activation of multiple subsystems at the same time.

Furthermore, by dividing logical processing into tasks by functions, the system management function can abort processing by a subsystem in maintenance or partial disorder. When the partial abort occurs, 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. In this way, fallback operation of LC is enabled.

4.1.3 Consideration of fallback operation

To improve actual availability of the software, its fallback operation (i.e. software operation along with partial abort) needs to be determined.

To investigate the influence of certain function's abort, we divided LC's function into seven functional element (system management, train tracking, interlocking, aspect control of signal lights, ATP control, supporting equipment control and railroad crossing control) and investigated the influence of a functional element's abort to others (fig. 5).

Range affected by partial abort

Aborted functional element \ Affected functional element	System management	Train tracking	Interlocking	Aspect control	ATP	Supporting equipment	Railroad crossing
System management		×	×	×	×	×	×
Train tracking	○		×	×	×	×	×
Interlocking	○	○		×	×	×	×
Aspect control	○	○	○		×	○	○
ATP	○	○	○	△		○	△
Supporting equipment	○	○	○	○	○		○
Railroad crossing	○	○	○	○	○	○	

○ : Not affected
△ : Partially affected
× : Affected

No fallback due to large range affected

No fallback due to inescapable interruption of transport

Target for fallback

Figure 5: Consideration of fallback.

Abort of the elements of system management, train tracking and interlocking is supposed to have large influence to the others; most of other functions cannot keep running. As for aspect control function, the other functions except ATP will be able to operate even if it is aborted. However, once it is aborted, interruption of train operation will be inescapable. For these reasons, target for fallback is limited to the functions of ATP, supporting equipment and railroad crossing. In addition, the functions of train tracking, interlocking and aspect control, whose abort will cause the entire stop, can be consolidated into one function as "interlocking". This implies the software configuration discussed in the previous section is reasonable.

4.2 Consideration for non-stop upgrading of software

Usual signal control system exchanges control information and software version information among multiple systems. In case of detecting a mismatch, the system will stop for safety. Because of this feature, software upgrading has been executed with the system stopped in order to avoid detecting the mismatch. However, once the interlocking function stops, its effect is very large. Therefore, a method for upgrading without stopping was considered.

4.2.1 LC maintenance mode

Because conventional fail-safe system with majority decision configuration (two out of three systems) secures a fail-safe condition by checking and comparing the control results, mismatch of software versions among multiple systems is not allowed. On the other hand, the LC's dual-duplex system can secure the fail-safe condition only for one system. Utilizing this feature, we considered a non-stop upgrading method 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 of slave system for 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.

4.2.2 Flow of non-stop upgrading by LC maintenance mode

The flow considered for non-stop upgrading by using the LC maintenance mode is shown in fig. 6. First, by setting LC maintenance mode in (1), output from the slave stops. After upgrading the slave's software in (2) and switching between the master and slave in (3), the previous slave now delivers the output. At this time, the output is generated by the upgraded software in the previous slave. As switching between master and slave is feasible without interruption of the output, the software upgrading can be completed without interruption. However, when the upgrading involves alignment change of railway track, the assignment of devices in the software also needs to be changed, and data carryover between master and slave is impracticable. This means the entire system has to be stopped for such upgrading.

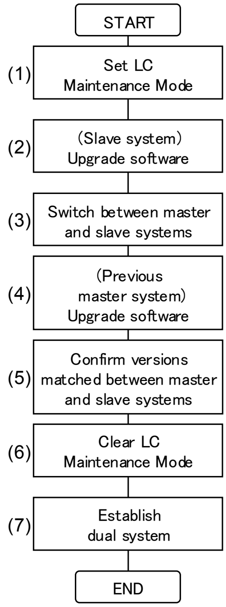

Figure 6: Software upgrading flow.

4.3 Reduction and quality improvement of design work by design support software

One aim of the LC is to realize flexible upgrading. The current signal control system requires substantial effort for designers to make the design tables for logical devices, because the range affected by the upgrade cannot be specified easily due to the structure. Moreover, because the consistency check between the tables relies on human attention, the designer's burden is large.

Therefore, design support software is being created to enable the automatic integrity check between tables by simple procedure of extraction. By this software, extraction of the corresponding data can be executed automatically and at the same time the consistency check will be completed without human attention. It consequently brings reduction and quality improvement of the design work.

We have so far developed design support software capable of centralized management of tables for LC control by utilizing the feature of the integrated control logic. Development of its user interface that is directly connected to supporting actual design work remains an issue to overcome.

5 Conclusion

The prototype of LC was developed to improve reliability as the total signal system and to simplify design work and installation. Adequacy of developed control logic was verified through field tests implemented at Minami-Matsumoto and Iwanuma Stations by comparing the control outputs from the LC prototypes and the relay interlocking. Verification of the control logic by a simulator and cost evaluation also indicated the adequacy. Based on these results, development for practical use of the LC has been determined.

Operational issues on practical use have been clarified and the solutions for them were considered. In particular, to secure the maintainability and availability, necessity of task division for software of integrated protection system was identified. At the same time, methods for fallback operation and non-stop upgrading of the software were considered. We will strive to develop a practical system of LC in accordance with the established policy.

References

[1] Kunifuji, T., Nishiyama, J., Endo, M., Saiki, Y. and Fukui, S., Development of a Network-based Signal Control System for Station Yards, *JR East Technical Review*, No. 15, pp. 20–26, 2009.
[2] Kunifuji, T., Saiki, Y., Masutani, S. and Matsumoto, M., Reliability of the IP Network-based Signal Control System and the Integrated Logical Controller, *Proc. of FORMS/FORMAT 2010 Part 2*, pp. 117-124, 2010.
[3] Shigeta, T., Maruyama, H., Ito, H., Saiki, Y., Niibori, Y. and Kunifuji, T., Development of an integrated logical controller, *JR East Technical Review*, No. 20, pp. 20–27, 2011.
[4] Ito, H., Kunifuji, T., Okada, T. and Hashimoto, T., Kairyo-koji ni Junan na Shingo System no Kaihatsu [in Japanese], *Proc. of 47th Symposium on Railway Cybernetics*, 609, 2010.
[5] Kitahara, F., Miyazaki, T. and Watanabe, K., Tokyo-ken Yuso-kanri System ni okeru Shin Denshi-rendo-sochi [in Japanese], *Railway and Electrical Engineering*, Vol. 5, No. 1 pp. 25–30, 1994.
[6] IEC 62280-1 Railway applications - Communication, signalling and processing systems, *IEC*, 2002.