Introduction

Signaling systems are important infrastructure ensuring safe and stable transport, and the principle of securing safety assumes that the systems are fail-safe. Conventional systems have been composed mainly of electric circuits using signaling relays that are fail-safe on their own. However, as the systems become larger, issues come up such as the number of relays and volume of wiring become huge, making it easy for human error to occur, and much time and effort being required for design and construction. On the other hand, since the establishment of fail-safe technology in computer control systems in the late 1980s, computerization of various signaling systems such as electronic interlocking equipment has advanced. With this, complex electronic circuits were replaced by software, functions were standardized, and wiring was reduced, thereby reducing human error and contributing greatly to improving safety, stability, and ease of construction.

With the advancement of computerization, however, improvement of productivity of safety-related software has become an issue. Safety of signaling systems is ensured not only by fail-safe properties of computers, but also by safety-related software having no defects or bugs. However, as safety-related software has become larger and more complex, a huge amount of labor has come to be necessary for its development, pushing up costs of signaling systems. This is becoming an issue in completely switching signaling systems to computer control at JR East, so technical innovation to improve productivity of safety-related software is an urgent issue.

This article covers the flow of computerization of signaling systems and technical development to improve productivity of safety-related software.

2 Flow of Computerization of Signaling Systems

2.1 Purpose of Computerization

The background of computerization of signaling systems is shown in Fig. 1, with interlocking equipment used as an example. The initial purpose of computerization was to improve safety and stability. Later, with the advance of network technologies and establishment of highly safe transfer technologies, improved design and simplicity of construction by simple integration of signaling systems came to be prioritized.

2.2 Improvement of Safety and Stability

(1) Issues with relay interlocking equipment

Relay interlocking equipment is still the mainstream form of interlocking equipment for railways in Japan as a whole. Some reasons given for that are that all operations can be read from a connection diagram with those to allow the safety and validity of its functions to be easily confirmed and that the life cycle cost at small stations is less than with electronic interlocking equipment. However, the number of connections is large and they are complex in large stations, it is difficult to eliminate human errors such as incorrect connections and wiring mistakes at construction, and it is difficult to completely eliminate malicious obstacles such as the possibility of malfunctions occurring due to external interference such as relay chattering and track circuit chattering. Moreover, the number of components is very large, making it difficult to build a redundant structure, so there are limits in terms of improving stability.

(2) Electronic interlocking and its advancement

Switching to electronic interlocking eliminated the need for connection diagrams and reduced mistakes at the design stage. And high-level elimination of external interference that could not be achieved in relay logics became possible, safety was improved by almost complete elimination of malfunctions, and stability was improved due to redundant structures becoming possible. Those were achieved by high-level software processing. Thanks to those advantages, computerization of signaling systems spread to areas other than interlocking equipment, and it is still evolving today.
2.3 Simplification and Integration of Signaling Equipment

(1) Network-based Signal Control System

With the advancement of computerization of signaling systems, hard-wired logic with relays was replaced with software, reducing the amount of wiring work in signal houses. However, to control field signaling devices, many control lines are required, so a huge number of multicore metallic cables are laid from the signal house to field signaling devices. In this situation, serious transport orders caused by wiring mistakes have occurred in the greater Tokyo area. And as a countermeasure to reduce labor in wiring, the Network Signaling System for Station Yards was developed and introduced. In this system, interlocking equipment and field signaling devices are connected by dual optical network. This greatly reduced metallic cables and wiring work. The Network Signaling System for Station Yards was first introduced at a small station in the greater Tokyo area, and introduction has been spreading to large stations thanks to the good operating results. Based on a similar concept, the Network Signaling System for Automatic Block Signals has been developed and introduced.

(2) Integrated logical controllers of signaling devices for station yards (LC).

Computerization of signaling systems is developed with individual functions such as interlocking, ATS, and level crossings. So, a variety of signaling equipment is scattered throughout a signal house and connected by a variety of interfaces. For that reason, it was difficult to increase the reliability of the entire signaling system. Integrated logical controllers of signaling devices for station yards (LC) were developed to improve efficiency of design and construction of the signaling system. That was realized by improving reliability through simplifying the system composition by integrating logic controllers in the signal house and connecting them to field devices via network connection and through unification of the system composition and integration of functions. LC will be introduced to Okegawa Station on the Takasaki line and Omagari Station on the Ou line, and they are expected to become standard for interlocking equipment at medium- to large-scale stations in the future.

3.2 Concepts in Cost Reduction

In cost reduction of the hardware and software that systems are composed of, measures such as use of general-purpose items, reducing number of units by integrating parts, and switching to mass production by unifying the types of interlocking equipment have been implemented for hardware. This is thought to have greatly reduced development costs and product prices. For software, on the other hand, research has not been conducted on optimizing the workload for development.

High levels of safety and reliability are demanded for safety-related software, so it is undeniable that design verification and testing requires a greater workload than ordinary software. We thus believe that the workload needs to be reduced while securing quality. In other words, railway operators and suppliers need to work hand-in-hand in improving productivity.

4.1 Issues in Developing Safety-related Software

The cycle of software development can be seen in Fig. 2. Generally, in software development, system and design documents are drawn up first according to user requirements, and then programming and system integration are performed according to the documents. Verification—confirming that the program meets end user demands—is done mainly by the operator in acceptance tests at the factory or by on-site monitoring tests. On the other hand, validation—confirming that the software is written as designed and that it has functions as specified—is performed mainly by in-house tests at the supplier. On the other hand, validation—confirming that the software meets user demands—is done mainly by the operator in acceptance tests at the factory or by on-site monitoring tests.

![Fig. 2 Lifecycle Model for Software Development](image-url)

Issues faced by the operator in each phase of software development are as follows.

(1) Concept and requirements definition phase

In this phase, the operator draws up the concept and presents to suppliers the requirements by documents such as requirement specifications, but accuracy and detail of items included in those requirement specifications depends heavily on the skill of the person who prepares those. Also, implicit knowledge regarding railway signaling systems not written in the requirement specifications may not be accurately shared between the operator and supplier, resulting in processes proceeding without the intentions of the system concept being accurately conveyed. This leads to discrepancies only becoming evident in accepting tests, resulting in major reworking.

3.1 Effects of Changes in the Socio-economic Environment

Putting first priority on considering the effects of the decline in birthrate and aging of society when deciding the future plans of signaling system development, design and construction needs to be less labor-intensive and technology to be learned needs to be of a smaller volume and uncomplicated from a perspective of there being fewer people to do that work. Promoting introduction of LC and network signaling is probably effective for solving the issues. However, from a perspective of railway operators seeing decreasing income, construction costs need to be kept below those of current systems when replacing systems due to deterioration, and that difference should be reserved as funds for R&D on next-generations systems. We thus need to consider a policy for reducing costs of items developed.

Direction of Future R&D in Signaling Systems

3.2 Concepts in Cost Reduction

In cost reduction of the hardware and software that systems are composed of, measures such as use of general-purpose items, reducing number of units by integrating parts, and switching to mass production by unifying the types of interlocking equipment have been implemented for hardware. This is thought to have steadily reduced development costs and product prices. For software, on the other hand, research has not been conducted on optimizing the workload for development.

High levels of safety and reliability are demanded for safety-related software, so it is undeniable that design verification and testing requires a greater workload than ordinary software. We thus believe that the workload needs to be reduced while securing quality. In other words, railway operators and suppliers need to work hand-in-hand in improving productivity.
(2) Testing and receiving phase

In this phase, the operator should perform the accepting tests from a perspective of the intentions of the system concepts being correctly achieved. In other words, the tests should be performed as validation where test scenarios need to be produced that take into consideration simultaneous operation of multiple trains, delays in field signaling devices, and external interference such as relay chattering and track circuit chattering. Much experience is needed to do that; but with the insufficient succession of skills in the rapidly progressing generational change, checking that items function according to specifications—confirmation of items tested from a perspective of verification—tends to be confirmed at the supplier in-house tests. If potential problems in specifications are overlooked at this phase, it may lead to major problems after introduction starts.

(3) Update phase

Signaling systems are matured from a perspective of control logic, so opportunities for requirement specifications to be newly drawn up is limited in cases of functions realized by only hard wired logic being replaced with software or changing of system architecture. Seen from the standpoint of signaling system functions as a whole, the ratio of functions needing to be prepared new is not very large. Even so, improvements to productivity are not seen even when repeatedly developing similar systems because requirement specifications are prepared new and suppliers produce software from the beginning when a new system is developed.

In order to overcome this issue and achieve improvements in safety-related software productivity, we have been deliberately studying since fiscal 2012 techniques that can be applied at each stage of the lifecycle (Fig. 3). The following gives an overview of those studies.

4.2 Studies on Improvements in the Concept and Requirements Definition Phase

For this phase, we are conducting basic research that will contribute to improving accuracy of requirement specifications and basic research on safety evaluation technology for specifications. As applied research, we have been working since the second half of fiscal 2015 on utilizing safety evaluation technology for specifications in extracting safety requirements for electric level crossing control equipment for station yards. The following covers our research on improving accuracy of those requirement specifications.

In this research, we developed a requirements analysis template (Fig. 4) so content that should be included in requirement specifications can be extracted without fail, the procedures for using those, and a notation system (Fig. 5) to visualize the relationships between requirements and specifications, between different requirements, and between different specifications. This takes into account the signaling system features of “non-functional performance of safety, reliability, and the like being required as implicit knowledge” and “specifications needing to be defined assuming the movement of various trains” for “overlooking defining of specifications” and “specification relationships being unclear,” two points that are issues in requirements analysis.

In utilizing this tool, requirements analysis work is given a fixed form, and there are expectations for it to prevent the overlooking of specifications that tends to occur depending on the amount of work knowledge and experience and discrepancy between people in understanding of specifications.

4.3 Studies on Improvements in the Testing and Receiving Phase

For this phase, we are studying how to improve testing accuracy. Signaling safety systems are event-driven systems that work by inputting operator actions, field signaling equipment status change, train movement, and the like. Therefore, the test cases
can be generated mechanically by event permutations, but the number of those becomes huge and not all can be tested. We are therefore studying techniques for narrowing down the number of tests cases that can actually be tested while maintaining comprehensiveness. Current study results have almost the same comprehensiveness as conventional test lists made by humans, but the number of test cases is many times that. In other words, humans can be said to be making tests cases many times more efficiently, so further studies are needed.

4.4 Studies on the Updating Phase
For this phase, we are studying reuse from the two perspectives of “increasing software lifespan” that enables the same software to be used even if hardware is updated and “changing to general purpose software” that enables the same software to be used in various systems.

(1) Increasing software lifespan
Safety-related software has used hardware safety mechanisms to assure safety, but the procedures for using those differed by model, so software changes were needed every time the model changed. However, if procedures for using safety mechanisms can be made common even between models, the safety-related software will no longer need to be changed even if the model changes. We are thus studying techniques for defining by mechanism standard procedures that drive those safety mechanisms and building those as common middleware—software independent from both the operating system and the safety-related software (Fig. 6).

(2) Changing to general purpose software
All signaling systems perform the same essential functions, such as interlocking and signal control, even if their system configurations are different. This is the concept of separating signaling functions into elemental functions and giving those functions to specific components to enable just the necessary components to be selected and reused when building new software.

At the current stage, reuse at the function specification level is assumed to be realistic, so we are studying techniques for separating into elemental functions and for describing those separated elemental functions in specifications. In reuse at the function specification level, eliminating vagueness included in function specifications is directly related to improving quality when reusing, so we model with the semi-formal method of Systems Modeling Language (SysML)* and are working to improve accuracy (Fig. 7).

* Modeling language for system engineering that allows specification description, analysis, design, verification, etc.

5 Conclusion
This article covers advancement in computer technologies contributing greatly to improving safety, stability, and design/constructability of a safety-related signaling system through examples of interlocking equipment. On the other hand, safety-related software is becoming larger and more complex, pushing up signaling systems development costs. Those are becoming an issue in complete computerization of signaling systems at JR East, so we are working on the cost-reduction measure of improving productivity of safety-related software as has been introduced herein.

Issues to work on in the future are further improving the individual techniques, developing techniques where quality control has consistency throughout the entire development process, and maximizing productivity improvement effects in the lifecycle.

Reference: