Analysis of the Formal Specification Application for Train Control Systems

Hyun-Jeong Jo, Yong-Ki Yoon and Jong-Gyu Hwang*

Abstract – Many critical control systems are developed using formal methods. When software applied to such systems is developed, the employment of formal methods in the software requirements specification and verification will provide increased assurance for such applications. Earlier errors of overlooked requirement specification can be detected using the formal specification method. Also, the testing and full verification to examine all reachable states using model checking to undertake formal verification are able to be completed. In this paper, we proposed an eclectic approach to incorporate Z (Zed) formal language and 'Statemate MAGNUM', formal method tools using Statechart. Also we applied the proposed method to train control systems for the formal requirement specification and analyzed the specification results.

Keywords: Formal specification, Statechart, Train control system, Zed

1. Introduction

Recently, in accordance with the development in computer and telecommunication technologies, the existing mechanical and electric train control systems used in railroad systems are being changed to electronic control systems. During this transformation to computerization, it became very difficult to secure the safety of the system. Train control systems are required to maintain a high level of safety as they are a very vital component and responsible for the safe operation of a train. As for the plan to solve these problems, the relative international standards recommend the application of formal methods in specifying development specifications and design for train control systems [1, 2] and the research and efforts to apply such formal methods are being progressed by centering on countries advanced in the railroad industry, especially Europe [3-6].

Among them, the case of applying formal specification of train control systems to subway line #14 in Paris, France is introduced as the first case of applying a formal method to the actual commercial system [3]. The studies to apply various formal methods such as Z (Zed), VDM (Vienna Development Method), Statechart, etc. as well as the B method in [3] to train control systems has progressed, but because they are unpracticed, they are not prepared to be utilized for the development of actual railroad sites. The application plan of the formal method presented as a result of studies is now based on excessively complex mathematical formulas or theories, and therefore, it has problems that the specialists in that field are needed and a very long development time is required, etc.

Moreover, in Korea, the research stage involving application of formal methods for the development of train control systems is very far behind in comparison with that of advanced countries, and though there are some cases applying formal methods to the design of railroad signaling protocol [7], there is no actual situation of application for the train control system yet. Currently in Korea, although it is already recognized at the research level that the formal method is essential for securing the stability of software, it is required to conduct researches on realistic and material procedures and methods enabling it to be applied to the railroad field since the application plan for it has not actually been raised as an issue in the industry. Accordingly, this thesis presents the specific plan and procedure to apply formal methods in practice to the train control systems in the railroad field for the first time in Korea.

For this purpose, this thesis proposes the approach applying Z, which is based on the mathematical form, for the essential part while using the Statechart, which is one of the languages for the graphical formal specification, rather than depending on the excessive mathematical formula as that is one of the drawbacks of the formal method application. The order of this paper is as follows:

* Corresponding author, regular member: Train Control & Communication Research Department, Korea Railroad Research Institute, Gyounggi-do, Korea (jghwang@krri.re.kr).

Received 3 July, 2008 ; Accepted 14 October, 2008

The application plan for domestic train control systems using the compromised plan of Z and Statechart for which we would like to propose in Chapter 2 will be presented. After showing the results of formal specifications using the method of our proposal, we would like to conclude in Chapter 3.

2. Application plan of formal method for domestic train control system

Every formal method has its unique applicable area, and the maximum effects can be achieved only if used to suit that particular area. In addition, as mentioned in the foregoing section, convenience of use shall be considered for the actual applicability, and various considerations such as selection of reliable tool supporting the formal method, etc. In this study, based on the formal specification languages shown in Fig. 1 and the tool selection basis to support it, we compared and analyzed various formal methods to adopt a formal method suitable for the vital software of domestic train control systems and announced some of its results [9].

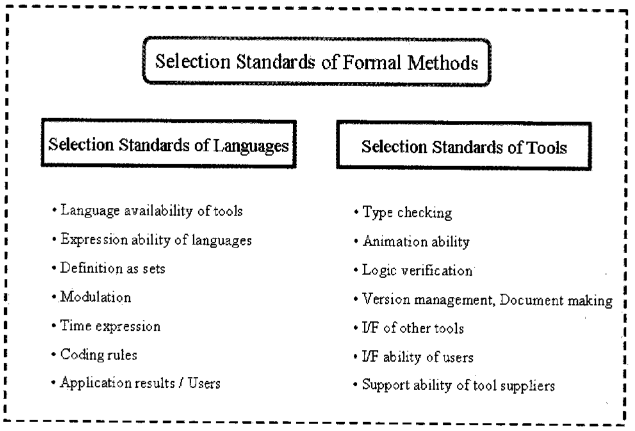

Selection Standards of Formal Methods
Selection Standards of Languages
Selection Standards of Tools
• Language availability of tools
• Expression ability of languages
• Definition as sets
• Modulation
• Time expression
• Coding rules
• Application results / Users
• Type checking
• Animation ability
• Logic verification
• Version management, Document making
• I/F of other tools
• I/F ability of users
• Support ability of tool suppliers

Fig. 1. Guideline for the selection of formal methods

As a result of comparison and analysis on the basis of these selection criteria for the formal method, this thesis selected Z and Statechart as the method for the formal specification, and selected 'Statemate', which is based on the Statechart, for the formal verification. The compromised plan of Z and Statechart proposed in this thesis can accomplish very high integrity when preparing the requirement specifications such as system definition at the formal specification stage compared with other existing methods, and at the same time, it has great advantages to shorten the development time through convenience of use due to the formal specification language based on graphics.

2.1 Analysis on the compromised plan of Zed and Statechart

While Z has great merits of high accuracy throughout formal specification work, it also has demerits of difficulty in representing data flows by including time concepts in the works such as modeling and simulation. Therefore, we considered that the method of using Statechart, based on the state transition possible to complement it compositely, was effective. Accordingly, we presented the method shown in Fig. 2 which applies both Z and Statemate together, the most widely known tool supporting the formal specification and verification.

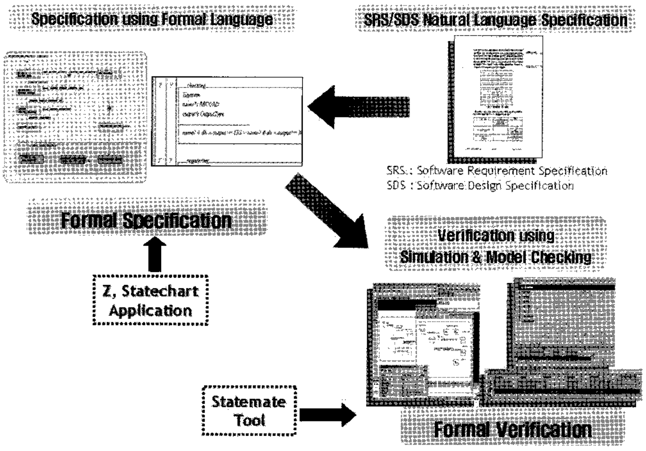

Specification using Formal Language
SRS/SDS Natural Language Specification
SRS : Software Requirement Specification
SDS : Software Design Specification
Formal Specification
Verification using Simulation & Model Checking
Z, Statechart Application
Statemate Tool
Formal Verification

Fig. 2. Proposed procedure of formal method application for vital S/W in train control systems

First of all, it shall pass through the formal specification stage showing the system requirements and development specifications. In the formal specification stage, the accuracy can be enhanced since the specification of written specifications composed of natural languages is prepared by formal specification languages which use graphic expression such as mathematical logic symbol formula or formal diagram with definite meaning, etc. Z proposed for application in this thesis allows for very high integrity in the case of preparing the specification for requirements such as system definition since it uses mathematical logic and sets [8, 10]. Z, which has merits of enabling expression in definite meaning, usually checks the data type of system to be defined, and enables systems to be controlled by expressing such data flows effectively.

The schema in Fig. 3 represents the characteristics of Z language specification very well. The schema makes Z specification distinguished from various other expressions, and it has the architecture introducing variables into the system to be specified while describing the relationship among variables. As it can be identified from the first schema box in Fig. 3, the architecture is composed of; firstly the schema name, the schema signature composing of the system status at the top part of center line, and the schema predicate representing restrictions on the values of those variables at the bottom part of line. The bottom part of Fig. 3 shows a simple example for preparing schema modeling as the 'letter inserting function of text editor'.

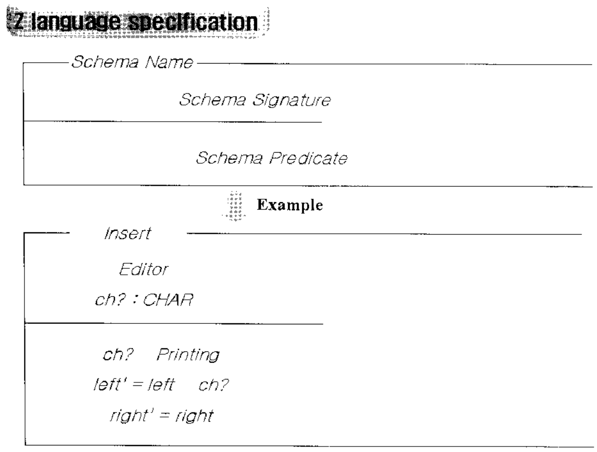


Fig. 3. Schema expression of Z language specification & modeling example

Generally, this motion is being executed at 'Editor' if only pressing one of the characters or numbers located on the keyboard, but it can be applied only for the printable character, not for the control character. In Fig. 3, the schema name was declared as 'Insert', and the schema signature within the 'Insert' shows that the 'Insert' is the motion changing the status of schema 'Editor', and declared the input variable to be inserted as 'CHAR' (ch?:CHAR). In Z, the input variable is always attached with a question mark (?) at the end of a variable, and it is only for the purpose of expression to distinguish variables. The predicate informs us of how the status of editor is changed. The first line of the predicate (ch? printing) shows the precondition, and it describes the condition that must be true before the next motion is occurred. The precondition informs us of the fact that the 'character insertion' motion can be occurred only for the input of a printable character. The remaining part of the predicate is the postcondition and it expresses the status after completion of motion. That is, 'left' = left ch?' means that the input of a new character is being added to the left side of the cursor, and 'right' = right' means that there is no change in the right part of the cursor before and after motion.

Like this, Z language can express definitions and request the data type of a system to be specified to allow data to flow effectively and definitely, but it has demerits requiring accurate knowledge and experience about the set theory and logic. Besides, since data flows include the concept of time, the existence of limitation in the expression is the problem in works such as concrete system modeling and simulation in the development specification using Z.

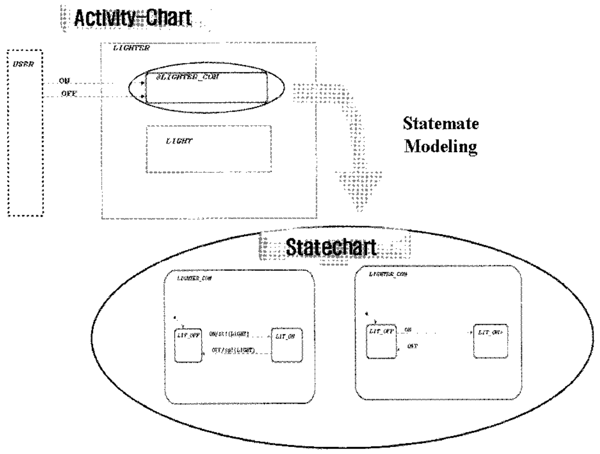


Fig. 4. Specification instance of a flashlight operation using Activity-chart & Statechart in Satemate

Since Statechart is expressed schematically through state-based visual specification language, and therefore, since it is easy to understand and has merits to express behavioral aspects of a system, it is being frequently applied to the design and implementation of the embedded system [11]. By utilizing Statemate, which supports both formal specification and formal verification based on Statechart as one of the formal specification languages, this thesis displays the architecture of the targeted system visually by using the Activity-chart supported by the tool, and it makes concrete behavior of the system easy to understand through simulation of the graphic model. Since Activity-chart has the function to express system status, it can check the operation between interfaces among data flow and module connected with various layers.

Statechart expresses all the designs of a system schematically, expressing the input and output of a system as input and output of the signal and data, and the behavior of a system as the transition of phase diagram. Fig. 4 shows an example which specifies the motion of a flashlight by using the Activity-chart and Statechart. In the top figure, it shows the interface architecture between the whole flashlight motion structure and exterior (user: 'USER') by using the Activity-chart on the flashlight. As you may check at the Activity-chart, the external 'USER' controls '@LIGHTER_CON' module through 'ON/OFF' control flow indicated in the dotted line. This

'@LIGHTER_CON' module includes the Statechart diagram at its bottom as shown in the figure.

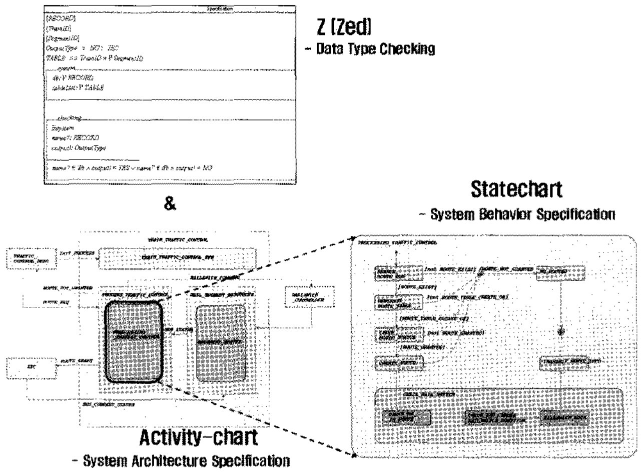

Z (Zed)
- Data Type Checking
&
Statechart
- System Behavior Specification
Activity-chart
- System Architecture Specification

Fig. 5. Formal specification application according to proposed method

Like this, it indicates the architecture of the system and input/output interface by using the Activity-chart, and expresses the function and motion status of the system through Statechart, which is the sub-module of Activity-chart. Fig. 5 is the figure that explains the formal specification method proposed in this thesis, and it verifies its relevancy, etc. by specifying definitions on data type, etc. by Z, and then it explains the procedures of specifying the architecture of system and interface by Activity-chart, and the function of system and system behavior such as data flow by Statechart. Especially, by using the Statemate tool which supports both Activity-chart and Statechart, it enables us to check visibly how the graphic-based specification modeled as Fig. 5 operates the system through simulation.

2.2 Results of formal specification in accordance with proposed methods

To verify the feasibility of proposed methods, we carried out a study on applicability to make requirements specified in formal specification form for the vital train control system. The target system for formal specification application is defined as a mock-up system, which is the CRD (Control Route Distance) system. The core function of this target system is divided into the interlocking function such as route control and the train protection function such as train distance control in Fig. 6. The route control part interlocks and processes commands, etc. in relation to the routes and point machines received from ATS (Automatic Train Stop). It must carry out the interlocked processing in relation to the information on route and point machine received externally, and there are safe interlocking functions for the interlocked processing. In the train distance control part, the movement of the train is being carried out in accordance with the block information included in the message of permissive movement authority, and this message of permissive movement authority will be created at the distance control system and transmitted to the ATP (Automatic Train Protection).

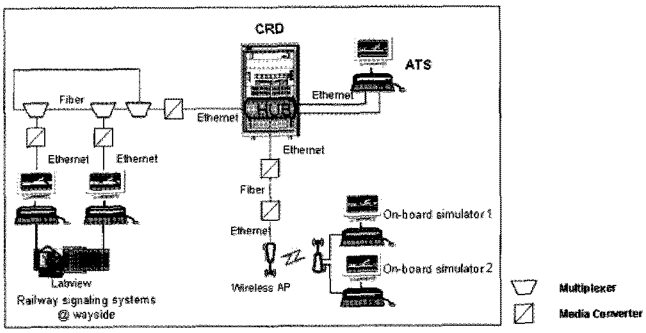


Fig. 6. Target system of formal specification application

In this paper, we especially specified the function of train distance part. The main functions of the train distance control system are summarized as follows; Control route distance, Validation of train location, Supervision on the train movement/direction, Processing of the temporary speed limit command, Block opening/closing. The system carries out the function of processing on-site control commands such as the processing of route setup control being received from the ATS, etc., the function of processing on-site signal equipment status after receiving it, the function of processing information on train operation after receiving it from the ATP, and the ATP function, etc. such as processing of train distance control, etc. for the train control.

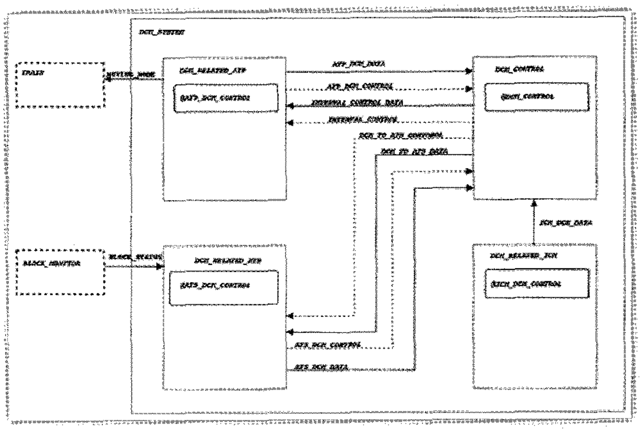


Fig. 7. Formal specification for target system architecture by using Activity-chart in Statemate

This system continues to communicate with all the ATP within the control area, and gives the train the authority of moving or stopping within the logical block in accordance with the information that the front block is not occupied. The result of system architecture specification about this train distance control system is expressed as shown in Fig. 7 by using Activity-chart in the Statemate tool. Data types of main functions in the train distance control system were checked by using Z specification language. Then Z formal specification results can be obtained as Fig. 8.

The location of the train over the whole system is validated by two-way communications between the train distance control system and ATP. The movement of the train is accomplished in the unit of block, and the train distance control system validates and determines current train location by finding out the information on train location among the information transmitted from ATP. The ATP continues to transmit the information on the location of the train being operated currently such as movement or stoppage to the train distance control system. The existence of the train is sensed through wireless communication with the ATP. The method of validating train location is accomplished in the manner as follows: if the train enters into the block, the ATP reports the block where it is currently located to the train distance control system, and then the system recognizes corresponding blocks as occupied blocks; and if it transmits this information to the ATS, then this ATS indicates the occupation status.

$$
\begin{array}{|l}
\hline
\mathit{DCM} \\
\mathit{current} : \mathit{Block} \\
\mathit{direction} : \mathit{Direction} \\
\mathit{pma} : \mathit{Block} \rightarrow \mathit{PMA} \\
\mathit{speed} : \mathit{Block} \mathrel{+\!\!\!\!\rightarrow} \mathit{Speed} \\
\mathit{obstacle} : \mathbb{P}\,\mathit{Block} \\
\mathit{redBlock} : \mathbb{P}\,\mathit{Block} \\
\mathit{yellowBlock} : \mathbb{P}\,\mathit{Block} \\
\mathit{greenBlock} : \mathbb{P}\,\mathit{Block} \\
\mathit{connection} : \mathit{ConnectionStatus} \\
\hline
\langle \mathit{redBlock}, \mathit{yellowBlock}, \mathit{greenBlock} \rangle \ \mathsf{partition}\ \mathit{Block} \\
\mathit{behindOf}(\mathit{redBlock}, \mathit{direction}) \cap \mathit{greenBlock} = \emptyset \\
\forall\, b : \mathit{redBlock} \bullet \mathit{pma}(b) = \mathit{Red} \\
\forall\, b : \mathit{yellowBlock} \bullet \mathit{pma}(b) = \mathit{Yellow} \\
\forall\, b : \mathit{greenBlock} \bullet \mathit{pma}(b) = \mathit{Green} \\
\hline
\end{array}
$$

Fig. 8. Formal specification results using Z language

If any detected train is lost due to communication interruption, etc., the train distance control system stops all the surrounding trains immediately by closing all the related blocks on the basis of train location known to it lastly. When the communication with the train whose detection was lost is resumed, the restoration on the loss of detected train will be accomplished because the existence of train was detected. In this case, the closed block must be opened by the operator so that the normal train operation can be resumed safely. This operation was specified by using Statechart in Statemate tool as shown Fig. 9. We can confirm that the Statechart of Statemate is suitable for expressing the behavior about which reaction the system will make under the condition determined as state-based language.

This paper could identity the definite input/output data flow and functional motion of the train distance control system through simulation by Statemate on the basis of definitions on data type by this Z and the graphic-based formal specification by using the Activity-chart and Statechart. The requirements made of natural languages and prepared at the early stage of research through this formal specification process were re-prepared more concretely and definitely, and it is anticipated that the requirements passed through formal specification will bring the shortening of time necessary for the detailed design and manufacturing of system and enhancement in safety.

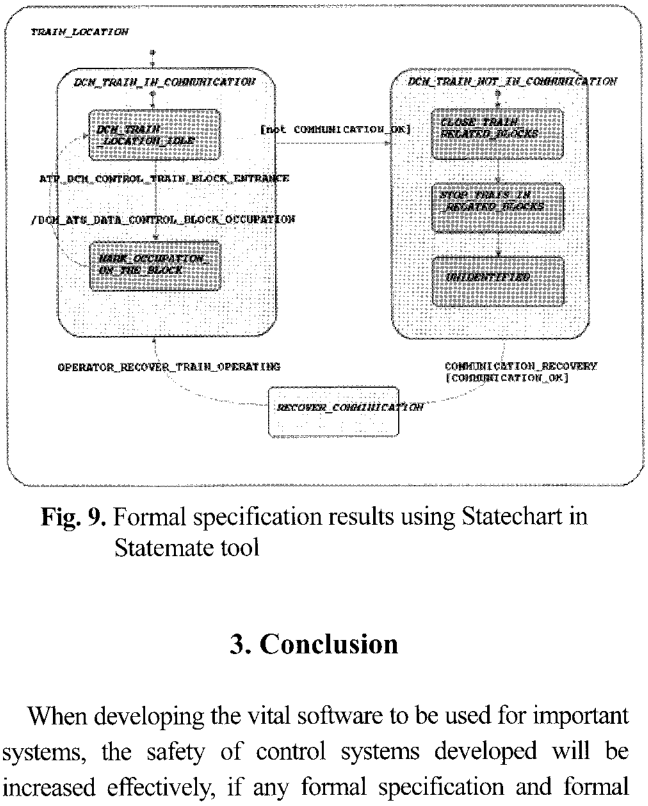

TRAIN_LOCATION
DCM_TRAIN_IN_COMMUNICATION
DCM_TRAIN_LOCATION_IDLE
[not COMMUNICATION_OK]
ATP_DCM_CONTROL_TRAIN_BLOCK_ENTRANCE
/DCM_ATS_DATA_CONTROL_BLOCK_OCCUPATION
MARK_OCCUPATION_ON_THE_BLOCK
DCM_TRAIN_NOT_IN_COMMUNICATION
CLOSE_TRAIN_RELATED_BLOCKS
STOP_TRAIS_IN_RELATED_BLOCKS
UNIDENTIFIED
OPERATOR_RECOVER_TRAIN_OPERATING
COMMUNICATION_RECOVERY
[COMMUNICATION_OK]
RECOVER_COMMUNICATION

Fig. 9. Formal specification results using Statechart in Statemate tool

3. Conclusion

When developing the vital software to be used for important systems, the safety of control systems developed will be increased effectively, if any formal specification and formal verification corresponding to the formal method are used. However, the results of research are still in the unsatisfactory situation for formal methods to be utilized in actual industrial fields, and especially in Korea, it is essential to have concrete procedures on formal methods for train control systems since there is no actual case applied in the railroad field. Like most of the overseas research cases for formal methods, if we utilize only mathematical logic formulas such as B method or VDM for the formal specification and formal verification of train control system, it will be stopped at the laboratory level of research instead of being applied to the actual railroad system like today since high-level expertise is required due to the complexity of these formal specification languages.

However, the application approach of formal methods applied Z and graphic-based Statechart proposed in this thesis complicatedly may be the practical alternative possible to overcome these problems. Especially, in the method proposed through the applicability of formal specification through this thesis, it is anticipated to enhance the actual applicability since the necessity of high-level expertise on the formal methods will be reduced due to the application of formal specification languages in the form of graphics to most functions and data flows. Accordingly, in case of applying the methods proposed in this thesis, it is anticipated that the securement of higher safety in the vital train control system will be possible since we may make much efforts in analyzing train control logic itself rather than professional knowledge on the formal specification languages conducted by existing studies. In addition, it is anticipated to meet the requirements set forth under international standards in relation to the railroad RAMS (Reliability, Availability, Maintainability and Safety) together with it.

References

[1] IEC 62278, "Railway Applications - The specification and demonstration of RAMS", (2002).

[2] IEC 62425 Ed. 1, "Railway Application: Communications, signaling and processing systems - Safety related electronic system for signaling", (2005).

[3] Alain Faivre and Paul Benoit, "Safety Critical Software of Meteor Developed with the B Formal Method and the Vital Coded Processor", World Congress on Railway Research (WCRR), (1999).

[4] L. Allain, O. Lahlou and P. Bon, " Formalization and Simulation of Operating Rules Using Colored Petri Nets" , Computers in Railway Ⅹ, pp. 329-340, (2006).

[5] 福岡 博, 福田 光芳, "ペトリネットによる連動仕様の検証" , RTRI Report, Volume 9, Number 11, pp. 19-24, (1995).

[6] G. marianom, J. L. Boulanger and P. Bon, From UML to B - A Level Crossing Case Study" , Computers in Railway Ⅹ, pp. 351-362, (2006).

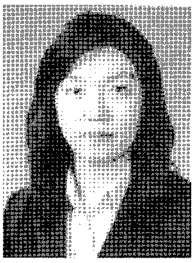
[7] G. T. Park, H. Lee and J. G. Hwang, "Performance Evaluation and Verification of Communication Protocol for Railway Signaling Systems", Computer Standards & Interfaces, Volume 27, pp. 207-219, (2005).

[8] Kotonya, G., and Sommerville, I., "Requirements Engineering: Process and Techniques", Wiley, (1998).

[9] H. J. Jo, J. G. Hwang and Y. K. Yoon, "The Analysis of Formal Methods for Applying to Vital S/W in Train Control Systems", Spring Conference of Korean Society for Railway, (2007).

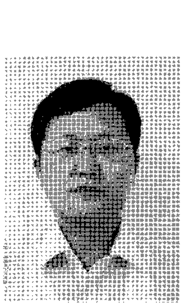
[10] Jonathan Jacky, "The Way of Z", Cambridge, (1997).

[11] Ammon Naamad and David Harel, "The STATEMATE Semantics of Statecharts", ACM Trans. Soft. Eng. Method, (1996).



Hyun-Jeong Jo
Hyun-Jeong Jo received her B.S. degree from Hankuk Aviation University, Goyang, Gyonggi-do, Korea, in 2003. She worked toward her M.S. degree at the Gwangju Institute of Science and Technology (GIST), Gwangju, Korea. Since 2005, she has been engaged with the Train Control System Research Team of the Korea Railroad Research Institute (KRRI).

Jong-Gyu Hwang
He received his B.S. and M.S. degrees in Electrical Engineering from Konkuk University and his Ph.D. in Electrical and Computer Engineering from Hanyang University in 1994, 1996, and 2005, respectively. As of 1995, he has been a Senior Researcher with the Train Control System Research Team of the Korea Railroad Research Institute (KRRI). His research interests are in the areas of railway signaling, protocol engineering, and communication and computer network technology.



Yong-Ki Yoon
He received his B.S. and M.S. degrees in Electrical Engineering from Chungbuk National University in 1994 and 1996. He has been a Senior Researcher with the Train Control System Research Team of the Korea Railroad Research Institute (KRRI) since 1995. Currently, he is working towards his Doctorate in Electronic, Electrical, Control and Instrumentation Engineering at Hanyang University. His research interests are in the areas of railway signaling, train control, S/W development, and safety analysis.