Hazard Identificaiton of Railway Signaling System Using PHA and HAZOP Methods

Jong-Gyu Hwang*[1], Hyun-Jeong Jo[2]

On-demand Transit Research Team, Korea Railroad Research Institute, Uiwang-si, Gyeonggi-do, Soutn Korea

*[1]jghwan@krri.re.kr; [2]hjjo@krri.re.kr

Abstract

Railway signaling system requires the high level of safety since these have to ensure safe operation of the train. According to these reason, safety-related regulations for railway signaling systems are internationally standardized. To secure the safety required by international standards, the hazard control is necessary with system lifecycle, and the hazard identification is needed to hazard control. To draw this hazard which is the basis of whole hazard control, there are very many techniques such as PHL(Preliminary Hazard List), PHA(Preliminary Hazard Analysis), HAZOP, FMEA(Failure Mode Effect Analysis), etc. in the activities and methods. The PHA and HAZOP method is recommended for hazard analysis at IEC standards, but this method has several unsuitable problems to apply to railway signaling system. In this paper we recommend the modified HAZOP method, which would be suitable for analyzing safety of the railway signaling systems. And also an example of PHA and this method applied to real system is also included.

Keywords

RailwaySignaling System; PHA; HAZOP

Introduction

The electronic and computerized railway signaling systems have replaced the existing mechanical systems, resulting in intelligent and automatic high-performance systems. For the existing electrical and mechanical systems, empirical approaches and engineer's intuition are mainly used to identify any faults, assuring a certain degree of safety in the railway signaling systems. However, the new computerized railway signaling systems do not allow the safety assurance based on such empirical approaches to detect faults. Therefore, IEC (International Electrotechnical Commission) requires more rigorous safety activities to assure the safety in the railway signaling systems[IEC 61508, 1998][IEC 62278, 2002] [IEC 62425, 2005].

To secure the safety required by international standards, the hazard control in accordance with the system life cycle is necessary. This hazard control activity is consisted of various stages such as hazard identification stage, hazard risk assessment stage, hazard risk control stage, etc. reflecting them to the design on the basis of results of this hazard and risk analysis. To draw the hazard which is the basis of whole hazard activities among these various stages, the application of PHA and HAZOP method is highly recommended (HR: Highly Recommend) for the hazard analysis on railway system in the IEC 62425, which is the international standard. In addition, these two methods are highly recommended by the Yellow Book also which corresponds to the guideline to safety activities of British railway system[RailTrack, 2000]. Among these two techniques, PHA is methods to identify the early stage hazard, and the HAZOP are used as detailed methods to draw hazards based on the hazard drawn at the early stage. The HAZOP technique is the formalized technology to draw the hazard, and there are cases where HAZOP methods were applied in some preceding studies in Korea to draw the hazard of railway signaling systems.

However, since HAZOP method which was standardized internationally[IEC 61882, 2001][Redmill, 1997] has been initially designed and developed in the chemical plant industry, its effect and efficiency of application are declined due to the elements not suitable for applying existing parameters and guide words to railway signaling systems as they are[Sirnivasan, 1998][M.U.Noh, 2001][Venkat, 2000], E.Habibi]. Therefore, this paper proposed parameters and guide words possible to be applied to the hazard analysis of railway signaling system effectively while maintaining existing HAZOP method, and it was named as HAZOP-R(HAZOP for Railway Signaling) in this paper[KRRI, 2011][J.G.Hwang,2010].

The hazard identification is the basic activity in hazard management procedure. It is impossible to delete or mitigate of hazards in system development lifecycle, if the hazards were not identified. This paper studied

application technology of PHA method to draw the initial hazard which is the most fundamental stage and HAZOP-R method to the railway signaling systems to identify concretely the initial hazards. And also the results of consequence analysis on identified hazards by ETA (Event Tree Analysis) were represented.

Hazard Analysis Technology

The safety activity of railway signaling systems defined by the international standards means a series of all activities which find and eliminate potential hazards embedded in the railway signaling systems being developed, or establish measures so that they can be reduced to below allowable level, and reflect them to the design and development of system.

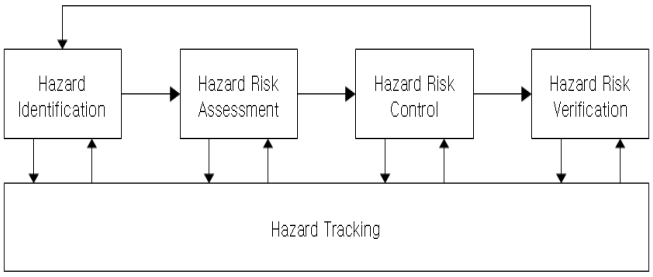

FIG. 1 HAZARD MANAGEMENT PROCEDURE

FIG. 1 is the one showing the process of safety activity in this aspect of hazard management briefly. That is, the safety activity of system requires the identification of hazard, hazard risk evaluation, and the hazard risk control to manage it at the allowable level shown by the hazard, and its verification process. This process will be carried out repeatedly until the feedback of each stage is always done and the hazard is drawn, controlled to make it to the allowable level and validated.

FIG. 2 is the one showing the safety activity stage for signaling systems drawn through relevant international standards and analysis on the preceding studies, etc., and it is the FIGure showing the comparison with each stage of system life cycle presented in the IEC 62278, and the main outputs by each stage of safety activity together.

As explained previously, the hazard management activity of signaling system is based on the identification of hazard, and it is the procedure where drawn hazard is analyzed and controlled. There are very many techniques such as PHL(Preliminary Hazard List), PHA, HAZOP, FMEA(Failure Mode Effect Analysis), etc. in the activities and methods to draw this hazard. Among these techniques, PHL and PHA are methods to identify the early stage hazard, and the FMEA and HAZOP are used as detailed methods to draw hazards based on the hazard drawn at the early stage.

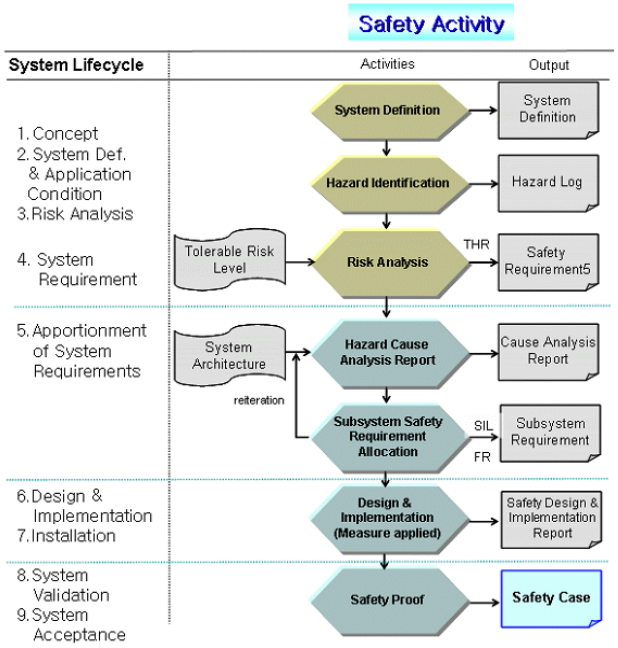

FIG. 2 SAFETY ACTIVITY PROCEDURE WITHR SYSTEM LIFE-CYCLE FOR SIGNALING SYSTEM

Among these techniques, PHA and HAZOP techniques are the well-used method to identify the hazard, and IEC 62425 which is the international standard related with the safety of railway signaling system and the Yellow Book of Bitish railways recommend to utilizing it as the means for hazard analysis. PHA is methods to identify the early stage hazard, and the HAZOP are used as detailed methods to draw hazards based on the hazard drawn at the early stage. The PHA is method to identify the early stage hazard, and the HAZOP is used as detailed methods to draw hazards based on the hazard drawn at the early stage. But the general HAZOP technique has some weakness to apply as it is to railway signaling, we proposed the modified HAZOP technique and applied to identified the hazards in this paper.

The identified hazards from above two methods have to be analyzed the consequence to obtain the deleted or mitigated measures on hazard risk. The consequence analysis on identified hazards was executed using ETA(Event Tree Analysis) method. This paper studied application technology of PHA and HAZOP technique to the signaling systems to draw the hazard which is the most fundamental stage in safety activities, and ETA to analyze the hazard consequence.

HAZOp-R Technology

General HAZOP Technique

HAZOP technique is the formalized systematic technique to draw the hazard, and it analyzes the cause and result for the case where specific parameter is out of it in accordance with the guide word. The most important technology in the deduction of hazard is to analyze the cause and result of hazard, and if HAZOP is used in this stage, the hazard can be drawn usefully at the early stage of safety analysis procedure[IEC 61882][Redmill, 1997].

HAZOP uses the concept of guide word to draw the hazards of system. Guide words such as More, No, Less, etc. identify deviations possible to be out of intention of the design by combining with various conditions of system in the course of drawing hazards and find the occurrence of hazard. The purpose of HAZOP is to analyze and verify deviations of system possible to be occurred from planned intention of operation to the special use of guide words. This potential system deviation can be developed to the accident. HAZOP includes sufficient explanation about the system to prove how deviations can be occurred from the intention of design, and the systematic survey on the whole parts of it. Once verified, the analysis will be made with respect to whether these deviations and results according to them can have an adverse effect on the safe and efficient operation of system. HAZOP includes sufficient explanation about the system to prove how deviations can be occurred from the intention of design, and the systematic survey on the whole parts of it. Once verified, the analysis will be made with respect to whether these deviations and results according to them can have an adverse effect on the safe and efficient operation of system.

This general HAZOP technique is the technique initially developed in the chemical process and has been advanced, and parameters and guide words are consisted of items such as change in the qualitative transformation amount. Although parameters and guide words are suitable for the chemical process where the control of liquid or gas, etc. is done generally, in case of train control system almost all of whose control outputs are digital signals and control targets were mostly made up with digital values, there are some parts not suitable for applying these general parameters and guide words. Due to these inappropriate parameters and guide words, it has the problem such as failure to make the best use of merits of HAZOP technique sufficiently, or application of some parts of guide words by interpreting them arbitrarily, etc. in the hazard analysis of train control systems.

HAZOP-R Technique

The digital control based signaling system has its limitation to conduct accurate hazard analysis only with the analysis on deviations in accordance with the qualitative changes such as More, Less, etc. based on the temperature, pressure and liquid, etc. That is, many facilities located at various locations such as trackside, on-board and control center, etc. are being operated generally in the signaling systems, and almost all of input/output signals are consisted of digital signals. In addition, the signaling system is the facility in charge of the safe driving of train, and it has different characteristics from general chemical process system in that the hazard becomes an important problem in countermeasure procedures at the time of emergency and the contents to be reflected in the system according to it, etc.

This paper proposed new parameters and guide words to suit for applying to the signaling systems while utilizing existing HAZOP concepts and procedures as they are, and called it as HAZOP-R[12]. Accordingly, the application case for one hazard of actual signaling system will be described.

Parameters in the HAZOP technique mean the physical, temporal, operational variables where guide words can be applied, and although they are applied in the plant industry by being classified as specific parameter and general parameter as follows, these parameters are the parts not suitable for the train control systems. Parameters intended to be applied to HAZOP-R were proposed as TABLE 1.

General HAZOP guide words is composed as main guide words like quantitative amount of changes in gas or liquid, etc., it is difficult to apply these guide words to the signaling systems as they are. It is possible to apply the function of guide word after changing it to suit for signaling systems if these guide words are applied as they are, and in this case, since characteristics of train control system are not reflected in it, systematic hazard analysis cannot be accomplished. Therefore, we proposed guide words suitable for train control systems like TABLE 2.

TABLE 1 PARAMETERS FOR HAZOP-R

No.	Parameter	Description
1	Interface	.Data interface between wayside equipment and on-board equipment .Communication interface between the wayside operator and vehicle driver .Data interface between sub-systems .Data interface between related systems .Communication interface between the wayside operator (system) and maintainer
2	Time	.Train operation time based on the train schedule .Operation time of the on-site facilities .Software data processing time .Generally defined time
3	Action	.Operation of operator, driver, maintainer .Action of on-site facilities .Action of on-board equipment
4	Limit	.Limit to the train speed .Limit to the line capacity .Limit to the software data processing .Limit to the human labor .Limit to the availability and reliability of facility
5	Procedure	.Operation, driving, maintenance procedure .Countermeasure procedure at emergency
6	Outside	.Natural phenomena (earthquake, storm, snow, rain, etc.) .passenger behavior .Prerequisite to the intentional external obstacle
7	Data	.Control command (train control, on-site facility control, etc.) .On-site information .Database information

TABLE 2 GUIDE WORD FOR HAZOP-R

Guide word	Description	Related parameter
No, Not, None	There is no defined parameter.	Interface, Time, Action, Limit, Procedure, Data
Part of	Performed or considered partly	Action, Procedure, Outside, Data
Early	Performed earlier than defined time	Time, Action, Data
Late	Performed later than defined time	Time, Action, Data
More	Excess and increase of the variables	Limit, Data
Less	Shortage and decrease of the variables	Limit
Other than	Abnormal parameter	Interface, Action, Limit, Procedure, Outside, Data

When defining deviations in the train control systems in combination with parameters and guide words defined previously, it is like TABLE 3.

TABLE 3 DEVIATION FOR HAZOP-R

Deviation	No	Part of	Early	Late	More	Less	Other
Interface	Interface impossible						Abnormal Interface
Time	No defined time		Earlier than defined time	later than defined time			
Action	No action	Act partly	Quick operation and action	Late operation and action			Other abnormal operation and action
Limit	No defined limit				Exceed defined limit	Fall short of defined limit	Other abnormal limit
Procedure	No procedure	Part of procedure only existed					Abnormal procedure
Outside		External factor acts partly					Abnormal external factor
Data	No data	Only part of data created, transmitted, received	Quick data creation, transmission, receipt	Late data creation, transmission, receipt	Excessive data creation, transmission, receipt		Other abnormal data

Identification of Hazards

The first step hazards are drawn by PHA technique in the previous description, and the detailed hazards are identified by HAZOP-R one. HAZOP-R technique to the hazard analysis of railway signaling system can perform the safety activity for both hardware and software as signal-related signaling system among various railway systems.

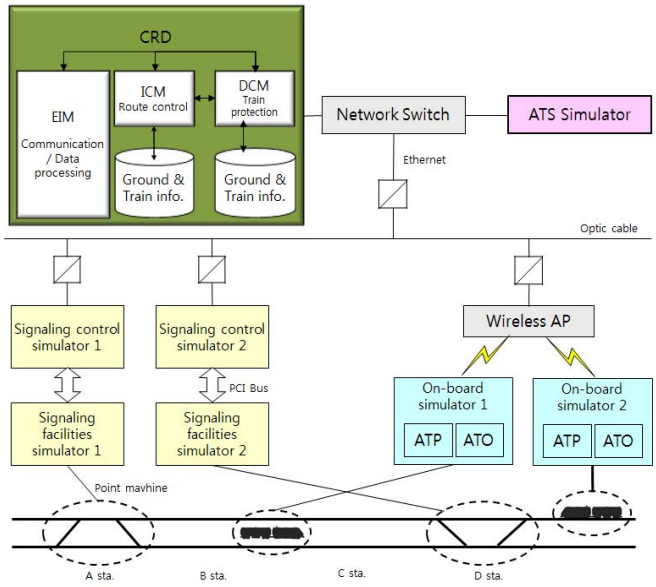

FIG. 3 BLOCK DIAGRAM OF CRD SYSTEMS AS A TARGET SYSTEM

Target system to study is the signaling system performing the train route control and train distance control through interlocking logic, and it is referred to as CRD(Control Route & Distance) system. FIG. 3 shows the functional block diagram of CRD system. Basic concept of CRD system is as follows.

- Track method shall be the logical block method which classifies existing track virtually by software, not the block track method which classifies existing track physically by track circuit. That is, logical blocks are blocks defined by software and they are not those present within the track physically. Therefore, it must be composed in the mock-up by classifying tracks properly by software with the target station as its target.
- Implements the virtual transponder among trackside equipment to verify the train location in the on-board simulator.
- ICM shall be composed in the redundancy system and it shall maintain its train route control function by converting to the second system automatically if the first system lost its function.
- DCM shall be composed in the redundancy system and it shall maintain its train distance control function by converting to the second system automatically if the first system lost its function.
- EIM shall be composed in the redundancy system and it shall maintain its interface function with external system by converting to the second system automatically if the first system lost its function.

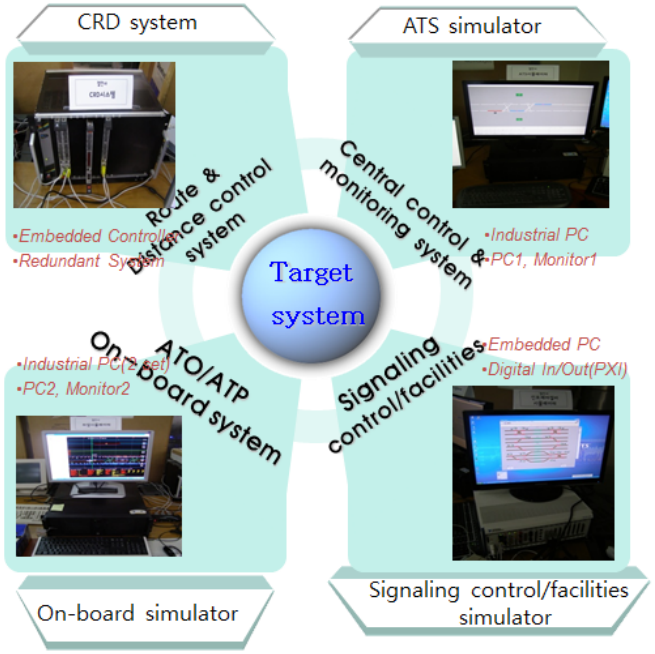

FIG. 4 SYSTEM CONFIGURATION OF CRD SYSTEMS

CRD system is the control system to make interlocking system such as train distance control and route command processing for the train protection which is the important function of signaling system carried out, and it is consisted of various simulators for the interface of CRD system such as on-board simulator, signaling equipment control simulator, etc. with actual on-site signaling equipment or on-board equipment, etc. CRD system performs on-site control command processing function such as processing of the route setup control command, etc. which is received from ATS simulator, function of receiving and processing on-site signaling equipment status, function of receiving and processing train operation information from the on-board simulator(ATP), and the automatic train protection function, etc. such as processing of train distance control for simulated train operation of on-board simulator(ATP). CPU module in charge of the core function of CRD system shall be classified into EIM(Electronic Interlocking Module) which is in charge of the interlocking function such as route

control and DCM(Distance Control Module) which is in charge of the train protection function such as train distance control. The actual conFIGuration of CRD system is shown FIG. 4.

Prelimilary Hazard Analysis

PHA analysis technique is the starting stage of hazard control which finds out and analyzes hazards possible to be occurred in each of the systems. PHA will analyze potential hazards which can be occurred in the system by drawing hazards to be drawn in the preliminary design stage. Analysis is performed on the basis of higher level documents for the function and conFIGuration of target system and the entire interface of human being with other systems. Hazard analysis activity to be performed during the PHA process shall perform the initial stage evaluation on the severity of drawn hazards and frequency of occurrence. Results are used to determine where the quantified analysis will be necessary in the future, and they make the complete analysis and risk evaluation possible to be performed through repetition and complementation according to the progress in detailed design of system.

The start of PHA analysis is the PHL which is the collection of identified hazards, and PHA analyzes these hazards in more details. Additionally, design information is compared with the hazard checklist to identify the hazard which was not predicted in advance. And the PHA output includes the design method which was established to remove or mitigate identified hazards and system safety requirements. Since PHA starts in the early stage of project in the design stage, the usable data are in the incomplete level. In case where these incomplete data are modified and complemented, they must be modified and added in the next stage accordingly.

After drawing hazards, the process which establishes causes and measures against them must be performed. Since it is the stage where the design was not accomplished concretely yet, the measure to be established cannot be detailed also.

We drew the highest level 4 hazards for hazard analysis as follows with CRD system based on explained in the previous PHA analysis as its target. Among of them, an example hazard is shows in TABLE 5. Among them, one example hazard is shown in TABLE 5.

- Hazard 1 : Train was entered into the abnormal route
- Hazard 2 : Another train was entered within the permitted movement authority
- Hazard 3 : Direction of point machine was converted during the movement of train
- Hazard 4 : Train driving too fast at the abnormal speed

TABLE 4 PHA RESULTS ON HAZARD-2 OF CRD SYSTEMS

Hazard	Causes	Effect	Mitigation
Hazard-2 : Another train was entered within the permitted movement authority	Failure in setting the permitted movement authority of train	Train collision	Perform the validation on block setup, validation on train location, and validation on train status to set the permitted movement authority.
	Failure in train brake (emergency brake)	Train collision	Receive information on the on-board equipment status continuously and supervise it.
	Failure in identification of train location	Train collision	Perform the validation on train location.

HAZOP-R

The result of HAZOP for the train operating in the direction of route that is not the defined route, which is the first hazard, is shown in TABLE 7. Causes and measures against situations where the entry of train into the wrong route and the movement of train in the wrong direction can be occurred due to the failure in control of train route, which is one of the main functions of CRD system, were established. Total of three parameters applicable to the hazard and two guide words were applied. And they were analyzed as the case where the information on train location cannot be identified due to the interruption of interface between CRD and train or where the movement authority cannot be transmitted, and as the cases caused by the abnormal operation of point machine and abnormal control command.

The hazard analysis through HAZOP-R made the highest hazard of CRD system which was drawn from the definition on the highest function as its target for analysis. After this hazard identification, consequence analysis by identified hazard will be executed through ETA method on it, and it will go through a process to hazard management. And it will go through the stage where the allocated safety requirement, and the mitigation technologies presented in the course of

hazard analysis are reflected to the system design.

TABLE 5 HAZOP-R RESULTS FOR HAZARD-1 OD CRD SYSTEMS

Hazard-1			Train was entered into the abnormal route			
Parameter	Guide word	Deviation	Causes	Description	Consequences	Mitigation
Interface	No	No interface	Failure in identification of train location	Approach between trains cannot be identified due to the unavailability of identifying train locations	Train collision	Emergency stop of train if it is impossible to interface with the train
			Failure in receipt of train route setup command	Unable to receive a route setup command from ATS	Stoppage of train	Redundancy design of CRD system
			Failure in transmission of movement authority for train	Failure in transmitting a movement authority for train to the on-board	Train collision	Emergency stop of train if it is impossible to interface with the train
Action	No	Not operated	Failure in switching of point machine	Train entered into the unsafe direction since the point machine was not operated	Train collision	Identification of information on failure of point machine
	Other	Abnormal operation	Switching of point machine in the wrong direction	Train entered into the unsafe direction since the point machine was switched in the wrong direction	Train collision	Identification of information on failure/direction of point machine
Data	No	No data	Failure in information on moving direction of train	Omission of information on direction of train movement from CRD system	Train collision	Redundancy design of CRD system
			Error in setting movement authority for train	Setting of movement authority for train different from the train route setup	Train collision	Redundancy design of CRD system
	Other	Abnormal data	Error in setting train route	Approach to the other train due to the wrong route setup of train	Train collision	Redundancy design of CRD system
			Error in command to switch point machines	Train entered into the unsafe route due to the abnormal switching of point machine	Train collision	Redundancy design of CRD system

Consequence Analysis of the Identified Hazards

Analysis on causes and consequences of occurrence must be performed for the drawn hazards of target system, and the degree of risk according to it must be calculated. Consequence analysis to be applied to the hazard is performed by the question like 'what if the hazard is occurred?' Purpose of the consequence analysis is to draw, record and quantify possible consequences which can be excluded from the hazards. The most important matter in the consequence analysis is to draw concrete defense measures which can suppress the potential increase of hazard as follows.

- Physical measures such as the technical diagnosis, warning, control, and protection system
- Procedural engineering measures such as the rules, procedures, and process knowledge of operator
- Derivation of environment which can defend unintended accidents
- Concept of consequence analysis can be expressed as the FIG. below.

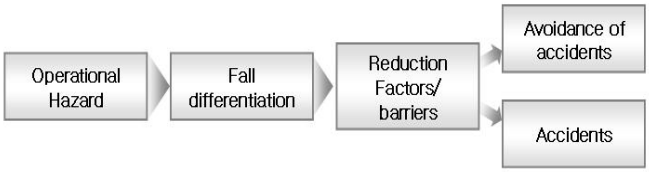

FIG. 5 CONNECTIONAL PROCESS OF CONSEQUENCE ANALYSIS

The ETA(Event Tree Analysis) method is applied to the consequence analysis for the identified hazards on CRD systems. The ETA method is known as a popular approach to consequence analysis of vital systems. Result on performance of consequence analysis on hazard of target evaluation system by above described ETA method is as follows. Results of consequence analysis on target evaluation system Hazard-3 were drawn in the ratio of 30.5% for train collision, 5% for stoppage of train, and 64.4% for the safety status. That is, the safety in the level of 70% can be guaranteed if we can cope with it systematically by receiving the speed, location and status information, etc. from the train, even though the train enters into the abnormal route. Therefore, the most important thing in the Hazard-3 is to prepare the plan which can secure the interface with the train to the maximum.

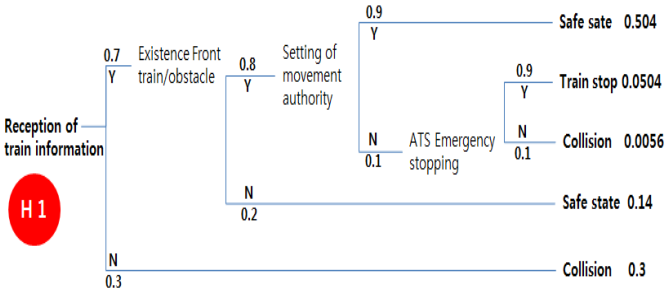

FIG. 6 CONSEQUENCE ANALYSIS OF TARGET SYSTEM HAZARD-1

Conclusion

The PHA and HAZOP are recommended in the related international standards to draw and analyze hazards among safety activity stages of railway signaling systems. However, since identification of hazard through among of them HAZOP technique is the technology developed in the chemical process field, parameters and guide words to be used in this technique are not suitable to be applied to signaling systems. This paper presented parameters and guide words suitable for signaling systems on the basis of this fundamental HAZOP technique, and its applicability was verified by applying it to signaling systems being developed actually. As its result, it was verified that the number of causes were remarkably increased in comparison with causes drawn by existing general HAZOP method, and in addition, it was verified that the hazard identification and analysis on signaling system based on the proposed parameters and guide words are efficient. Since this could classify and inquire into the cause in details which made one hazard occurred due to the definition of parameter and guide word suitable for signaling systems, and it was possible to draw more effective and detailed result.

We could establish the procedure for applying the hazard identification of railway signaling system through the consequence analysis according to the derivation of hazard and ETA by these PHA and HAZOP-R.

REFERENCES

E Habibi, M Zare, A Barkhordari, SJ Mirmohammadi, GhH Halvani, “Application of a Hazard and Operability Study Method to Hazard Evaluation of a Chemical Unit of the Power Station”, Journal of Research in Health Sciences, Vol. 8, No. 2, 2008.

IEC 61508, “Functional safety of electrical/ electronic /programmable electronic safety-related systems”, 1998.

IEC 61882, "Hazard and Operatbility Studies(HAZOP Studies)-Application Guide", 2001.

IEC 62278, "Railway Applications - The specification and demonstration of RAMS", 2002.

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

J. G. Hwang, H. J. Jo and D. H. Kim, “Hazard analysis of train control system using HAZOP-KR methods” International Conference on Electrical Machines and Systems(ICEMS 2010), 2010.

KRRI Research Report, “Evaluation of Safety Performance of Train Control System and the Technical Development of Prevention against Accident”, June 2011.

M. Y. Noh, et al., “Knowledge Framework and Algorithm for Automating HAZOP Analysis of Batch Processes", Journal of the Korean Institute of Chemical Engineers, vol39, No.3., 2001.

RailTrack, "Engineering Safety Management - Issue 3", Yellow Book 3., 2000.

Redmill F., Chudleigh MF, Catmur JR., “Principles underlying a guideline for applying HAZOP to programma-ble electronic systems”, Reliability Engineering & System Safety in Elsevier, Vol.55, No. 3, pp. 283-93, 1997.

Srinivasan R., Venkatasubramanian V., "Automating HAZOP analysis of batch chemical plants : Part I. The knowledge representation framework", Computers chem. Eng. Vol. 22, No. 9, pp.1345-1355 (1998)

Venkat Venkatasubramanian, Jinsong Zhao, Shankar Viswanathan, “Intelligent systems for HAZOP analysis of complex process plants”, Computers and Chemical Engineering, Vol. 24, pp. 2291-2302, 2000.

Jong-Gyu Hwang received the B.S and M.S. degrees in Electrical Engineering from Konkuk University, Korea in 1994 and 1996, respectively. He has been working towards his Ph.D. in the Division of Electrical and Computer Engineering, Hanyang University since the year 2000. As of 1995, he has been a Principal Researcher with the Korea Railroad Research Institute. He was a visiting scholar at Virginia Commonwealth Univ. from 2011 to 2012. His research interests are in the areas of railway signaling system, computer network technology, PRT(Personal Rapid Transit) system, software testing of embedded system.

Hyun-Jeong Jo received the B.S. degree from the Hankuk Aviation University, Goyang, Gyonggi-do, Korea, in 2003. She worked toward the 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). His research interests the areas of railway signaling, software safety, communication application technology.