신호시스템 요구사항 도출방안

이종우*°, 정의진*, 황종규*, 신덕호**
*한국철도기술연구원, **광운대

A Study on Reliability and Safety Calculation of vital system in Railway Signalling System

LEE Jong-Woo*°, JOUNG Eui-Jin*, HWANG Jong-Gyu*, SHIN Duck-Ho**
*Korea Railroad Research Institute, **Kwangwoon University

Abstract - Railway signalling system is required to be high safety against collision, derailment and collision at level crossing and to be high availability. The signalling system is usually divided into automatic train control, interlocking and centralized traffic control systems and each system must be high fail safe and availability. This study focused on reliability calculation of vital systems in train control system.

1. Introduction[1][4][5][6]

-Signalling System Configuration

Signalling system is composed of ATC, IXL, CTC, communication module which links between systems. Recently, many signalling systems adopt onboard signal using transmission based system to ensure high operation in which wayside color signalling cannot be discrete above 200km/h, and, also metropolitan railway, can easily control train speed by using on board speed monitoring system. CTC is normally considered as a non vital system, so we exclude CTC analysis and reliability calculation.

-ATC

ATC generates train running speeds. A train permissible running speed in a block is dependant on the variables : location of train ahead, track condition, climatical condition, intrusion monitoring, additionally, transmission delay and information amount. The speed is minimum value of the variables. The calculated speed is transmitted through track circuit to a onboard system, with which train is controlled.

-IXL

IXL performs as vital functions of train routing, protections and prohibitions. IXL processes the orders from CTC or local operation panel and transmit track equipments controlling information to track function modules, in which track equipment control signals are generated and transmitted to each track equipment. The track signalling equipment comes to activate to received control orders and then routing or signalling is carried out.

The function elements of ATC and IXL are shown in Figure 1 and 2, respectively.

2. Signalling System Safety and Reliability Requirements[3][7]

2.1 Safety

Risk is contrary to safe. Because risk ·can be define widely in concrete forms, a safe sometimes defined where no risk exists The fail safe, a system being in trouble, is to have the system be safe, which becomes under no risk. Signalling system safety properties have the system do alway functions to fail safe when a vital system goes wrong.

Generally, we say, if failures take place in railway, then a train have the speed decrease, and safety is ensured. Briefly speaking, fail safe is such that "if failure takes place, we have train stop." Safety properties against · failure of parts or system have a dominant character by which the system transfers to no risk state.

Functions	description
Train detection	tracking occupied blocks using track circuit
Meteorology	train stopping when wind speed is above35m/s, the snow filed up above a limit, the amount of rainfall above 60mm/h, 250mm/day and flooding area running 80~90km/h
Intrusion Monitoring	train running limiting to 170km/h when rocks and intrusions are detected on track
Train Status Monitoring	train stopping when wheel shaft temperature is above 90℃, when train detects objects being dragged
Permitted Speed Calculation	maximum train running speed generation in blocks
Train running speed Monitoring	train running speed control by comparing actual train speed with permitted train speed in blocks
Protection	train speed limiting to 0km/h and 90km/h for protection of human and equipment
Maintenance	data archiving and offering for maintenance
Communication	offering train locations and track informations to other system

Figure 1. functional elements of Automatic Train Control

function	description
Interlocking	Interlocking functions process routing control orders from CTC and local control panel including lockings. Interlocking I/O transmits control orders to track equipment, receive status informations of track equipment, alarms, status informations.
Operating	Operation functions perform as follows : remote and local control mode converting, communication between systems, and local control orders input.
Signalling	One of interlocking signalling functions is relate to point machines : point machine control to be requested, point machine locking, point machine status feedback. Another is relate to signals : signal control to order, signal status feedback.
Communication	offering vital informations related to point machine status to ATC and track status

Figure 2. functional elements of Interlocking

Because fail safe is applicable to such a logic that no risk must be ensured, fail safe is realized by that part or material inference with high reliability. This is called as "design using IST(Inherently Safe Techniques). Another fail safe design methods using not proven parts exit FMEA(Failure Modes & Effects Analysis) and RM (Redundancy Management).

An example demonstrated on safety requirement in Figure 2. It, generally accepted idea, is reasonable that the rate of risks accompanying deaths is $10^{-9} \sim 10^{-10}/h$ (1 times per 10~100 million year per system). The rates of fail safe and fail unsafe is shown in the figure 14. The safety rates of signalling system equipped with micro electronic computer is generally considered the fail unsafe rate 10^{-10}(1 times/100 million years/system) and the fail safe rate 10^{-5} ~ 10^{-6} (1 times/ 10~ 100 years/system)[2].

Finally, the fail unsafe rate of vital systems, which become a catastrophe accident, is decided 10^{-9} ~ $10^{-10}/h$ For example, the signalling vital relay have highly safe a fatal failure probability.

Country	Admissible Risk Rate
American	self activity : $10^{-5}/year/person$ Damaged from disastor: $10^{-7}/year/man$
U. K	Process Control : $10^{-5}/year/system$
Austria	Chemistry FAFR : 3.5 Individual Risk in system interior : 0.35
	Unmanned Transportation System : $10^{-12}/h$ Man Control System : $10^{-9}/h$
Nuclear	radio activity diffusion to neighbour : $10^{-10}/year/reactor$ (reactor fusion accident : 10^{-5} × Container : 10^{-1})
NASA Airplane Control Computer System	Fail Unsafe : $10^{-10}/10h$ flight
Jumbo Jet Plane	Takeoff Landing Number : 150million times

Figure 3(a). Different Safety Requirement

	Fail Safe(/h)	Fail Unsafe(/h)
Interlocking System	4.6×10^{-4}	6.4×10^{-9}
Signal Vital Relay	1.5×10^{-8}	1.4×10^{-10}
Micro Electronic System	10^{-5}~10^{-6}	10^{-10}

Figure 3(b). Failure rates of Conventional System and Micro Electronic System

-Reliability

Any transmission based signalling system should be designed for application on a railway operation for 24 hour /day, everyday. The availability figure is often expressed as the·mean time Between Failure of a Transmission based system function and the system down time that cause delays to a train(or trains) of time no greater than some minutes. a mass transit railway might expect MTBF as 25 minutes in any 10 days for a given line. Such a high availability is of the utmost importance, sine failure will cause widespread delays and result in alternative and generally more hazardous procedural based methods of ensuring train movements.

The availability of signalling system is decided as 99.98% like ETCS.

2.2 System Safety Analysis

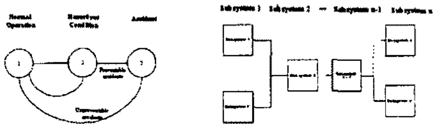
System Safety Analysis performs on H/W and S/W of which elements consist of subsystem and system. SSA allocate severity to H/W and S./W like as shown Figure 4. The safety requirement of vital systems is set up $10^{-9}/h$ and the reliability is set up 99.98 % for all H/W and S/W.

2.3. Modelling and Testing

Several reliability modeling techniques are available to estimate reliability and safety. We present Markov reliability models of two critical systems of Railway signalling system : ATC and IXL. Safety was calculated on the basis of the transition of a safe state into unsafe shown in the Figure 5. Reliability was calculated a mixed model of serial and parallel.

sys	Function	H/W	S/W	Safety Requirement	Availa -bility
ATC	Speed Generation	wayside processor	speed calculate module	$10^{-9}/h$	99.98 %
	Train Detection	Track Circuit		$10^{-9}/h$	
		Block	Management		
	Train Detection & Speed Calculation	I/O Functional Module	transmission and device management	$10^{-9}/h$	
	train detection	Vital Relay		$10^{-9}/h$	
	Intrusion Monitoring	Intrusion Detector			
	Meterological Detection	meteorological Detector	Permissible Speed Calculation		
	Train Running Speed Monitoring	Onboard Processor	Speed Monitoring	$10^{-9}/h$	
		Display Unit	Speed Display	$10^{-9}/h$	
	Interface	Antenna			
IXL	Interlocking	Processor	interlocking	$10^{-9}/h$	
	Operating Function	Operational Panel			
	Track Function	Track Functional Module	Track functional Module	$10^{-9}/h$	
	Route Setting	Point Machine			
	Communication	I/O module	Communication /signalling, validation of data	$10^{-6}/h$	

Figure 4. System Safety Analysis of ATC, IXL and CTC



(a) (b)

Figure 5. Transition of Safe to Unsafe(a) and Redundancy model(b) of ATC and IXL

2.3.1 Safety and Reliability Models

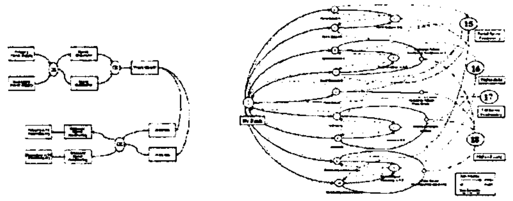
The simplified models built in redundancy of ATC and IXL are shown in Figure 6(a) and Figure 7(a), respectively. One parts of the systems cannot inherently be built-in redundancy because of physical restraints. The simplified state transition models of ATC and IXL are shown in Figure 6(b) and Figure 7(b), respectively.

2.3.2 ATC and IXL reliability calculation

The reliabilities of the ATC and IXL systems, of which the structures are constructed of serials and parallels combination being redundancy like Figure 6(a) and Figure 21(b), are calculated with the defined variables shown in Figure 10.

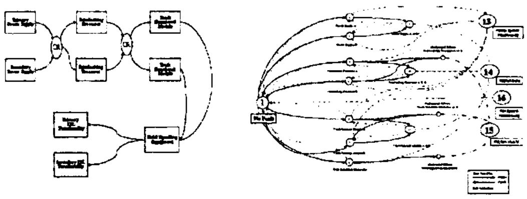
System failure rate is obtained by calculating the availability and MTTR which were given as predefined values from ETCS, and subsystem failures rate and reliabilities with dual redundancy are calculated by using Markov model represented in Figure 8. From Figure 8, a dual system reliability $R(t)$ is obtained as follows.

$$R(t) = p_{(1,1)}(t) + P_{(1,0)}(t) + P_{(U,S)}(t)$$
$$= (1+C)(t)e^{\lambda t} + Ce^{-2\lambda t}$$



(a) (b)

Figure 6 Simple Model(a) and State Diagram Model(b) of ATC



(a) (b)

Figure 7. Simple Model (a) and State Diagram Model (b) of IXL

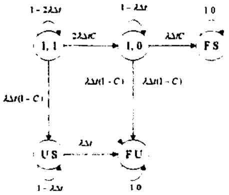


Figure 8. Dual system Reliability of Standby spare

	IXL	ATC	Condition
System Failure Rate	6.68E-5	6.668E-5	Availability : 0.9998 MTTR : 3 hours
MTTF	14,997 hours	14,997 hours	
Subsystem Failure Rate	2.872E-5	2.519E-5	Fault Coverage : 0.9 Using Markov model
Reliability	99.996%	99.996%	

Figure 9. Reliability Calculation Results of ATC and IXL

2.3.3 Safety calculation

An inter-relation of fault rate and "n" redundancy in a system shows in Figure 11. The values in the figure 25 represent the reliability below 0.999 in the case of a system with redundancies. As an example, the reliability of a system with fault rate become to below 0.999 after 100 hours for a system with no redundancy, 200 days for dual redundancies, 342 days for 3 redundancies, and 620 days for 5 redundancies. The higher a fault rate increase, the higher the reliability increases with redundancy. An example curve in case of $\lambda=10^{-5}$is shown in Figure 10.

3. Conclusion

We defined railway signaling functions and sought its safety and reliability requirements for each system. hazard. And we proposed a method to ensure a required safety using redundancy and calculated each subsystem reliability to be secured for requirements.

It's. in reality, difficult for fault rate estimation of a system with high fault rate to evaluate whether the fault rate is true or not, because, for example, the estimation of a system having a fault rate requires more than 110 thousands years. We show how to obtain high reliability by using systems having low reliabilities. We need to develop high fault coverage system to realize a system having high safety with low reliability.

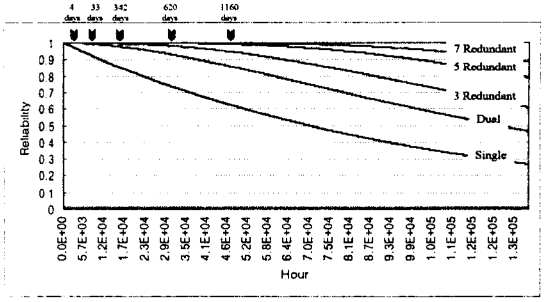


Figure 10. System Reliability with Redundancy (in case of module failure rate $\lambda=10^{-5}$)

(Unit: Hour)

Failure Rate / Redundancy	$\lambda=10^{-3}$	$\lambda=10^{-4}$	$\lambda=10^{-5}$	$\lambda=10^{-7}$	$\lambda=10^{-9}$
Single	Approx. 1	Approx. 10	Approx. 100	Approx. 5,000	Approx. 130,000
Dual	Approx. 10	Approx. 90	Approx. 800	Approx. 70,900	Approx. 130,000
3 Redundancy	Approx. 90	Approx. 900	Approx. 8,200	Approx. 130,000	Approx. 130,000
5 Redundancy	Approx. 100	Approx. 8,200	Approx. 14,900	Approx. 130,000	Approx. 130,000
7 Redundancy	Approx. 300	Approx. 17,900	Approx. 28,900	Approx. 130,000	Approx. 130,000

Figure 11. Relation between Module Failure Rate and Redundancy

[References]

[1] H. Yoshimura and S. Yoshikoshi, "Railway Signal", Japan Association of Signal Industries, 1983

[2] Watanabe et al., technologies on safety and reliability of computerized railway signalling system, RTRI Internal report

[3] CENELEC, "European Standards Railway Application-EN50126 and EN50129 ", 1997

[4] KTGV Contracts, KHRC, part TCS, 1993

[5] H. Fukohoka, Introduction to Safety Engineering on Railway, RTRI internal report

[6] ALC Train course, "Introduction to RDD-100 Student Work book"

[7] S. Jackson, "System Engineering Commercial Aircraft", INCOSE 97

[8] B.W. Johnson, "Design and Analysis of Fault-Tolerant Digital Systems", Addison-wesley Publishing Company

[9] P. Kostiuk and al., "A Method for Evaluation the Safety Impacts of Air Traffic Automation" NASA/CR 1998-207673

[10] P.Kostiuk, and al., "A Integrated Safety Analysis Methodology for Emerging Air Transport Technologies, NASA/CR-1998-207661