Regular paper http://dx.doi.org/10.13067/JKIECS.2013.8.12.1905

유도 루프식 열차 제어 시스템 안전 무결성 등급 할당

류승균* · 박재영** · 윤학선***

An Allocation of Safety Integrity Level to Inductive Loop type Train Control System

Sung-Kyun Ryou* · Jae-Young Park** · Hak-Sun Yun***

요 약

본 논문은 유도 루프식 열차제어시스템에 대하여 준 정량적 안전무결성 등급(Safety Integrity Level : SIL) 할당 방법을 적용하여 안전무결성 등급을 할당한 결과이다. 유도 루프식 열차제어시스템은 ATS장치, 지상ATP장치, 차상ATP장치, 지상ATO장치, 차상ATO 지상장치 하드웨어 및 소프트웨어로 구성되어 있으며, 안전무결성 등급 할당은 각 서브시스템에 대한 안전무결성 등급을 의미한다. 준 정량적 방법의 세 원칙에 근거하여, 열차제어시스템을 구성하고 있는 서브시스템에 대한 안전무결성 등급을 할당하였다.

ABSTRACT

This paper demonstrates the result of Safety Integrity Level (SIL) allocation for IL-type Train Control System(IL-TCS), by applying the semi-quantitative approach. IL-type TCS is defined in this paper as the set of Hardware and Software ATS equipment, Track-side ATP equipment, On-board ATP equipment, Track-side ATO equipment, On-board ATO equipment. SIL allocation is performed for these constituent subsystems of TCS. Based on three principles of the semi-quantitative method, the SIL allocation process is performed for the subsystems composing TCS.

키워드

Inductive Loop, Train Control System, Signalling, Safety Integrity Level
유도루프, 열차제어시스템, 철도신호, 안전무결성등급

Ⅰ. 서 론

본 논문에서는 인천국제공항에 설치된 유도루프식 열차제어시스템(Inductive Loop type-TCS)에 대한 안전무결성 등급(SIL) 할당한 결과이다. 유도루프식 열차제어시스템은 차상장치, 지상장치, 기계실장치, 관제설비, 선로변설비 등으로 구성되어 있으며 각 서브시스템의 기능을 고려하여 안전무결성 등급을 결정한다. SIL 할당은 시스템 수명주기 중 초기단계에서 설비의 기능요구사항에 기반하여 설비별 위험원(Hazard)을 식별하여 안전요구기능을 식별하고 위험도를 평가하여 시스템의 위험조건 관리 및 후속 조치를 판단하기 위함이다. 또한 시스템의 위험원에 대하여 필요 시 위험도 저감을 통하여 위험도를 허용할 수 있는 수준 이하로 유지하기 위한 방안의 일환으로 수행된다.

* 우송대학교 대학원 박사과정(danice@hanmail.net) ** 우송대학교 철도전기시스템학과 교수
*** 교신저자(corresponding author) : 한국철도시설공단연구원(kamayun@kr.or.kr)
접수일자 : 2013. 10. 15 심사(수정)일자 : 2013. 11. 25 게재확정일자 : 2013. 12. 16

II. SIL 할당 방법 비교 연구

SIL 할당은 IEC 61508의 개발과정에서 시스템의 기능적 안전을 보증하기 위한 기준으로서 정의되었으며[1] 일반적으로 허용 가능한 위험률 (Tolerable Hazard Rate, THR)과 시스템 운영을 고려한 정량적인 방법과 상대적으로 간단한 Risk Graph[2]을 활용한 정성적인 방법, 그리고 이들의 중간적 방법으로 준 정량적(Semi-quantitative) 방법 등으로 분류된다. IEC 61508과 연관된 SIL 할당 방법 외에 IEC 61511[3] 또는 IEC 61513[4] 등에서도 SIL 할당에 대한 몇 가지 방법을 제시하여 각각 Process 산업분야 및 원자력분야에서 적용하고 있다. 또한 자동차분야에서는 MISRA[5]에서 SIL 할당에 대한 방법을 제시하고 있다.

철도분야에서의 SIL 할당은 안전-관련 시스템의 경우 설계 이전에 결정해야 할 중요한 요건 중의 하나이고 이 수준에 따라 설계 및 그 이후 RAMS 활동의 범위와 깊이에 크게 영향을 주는 요소이지만 위에서 소개한 SIL 할당방법의 선택에 따라 서로 상이한 SIL 수준이 도출될 수 있기도 하다 [6]. 정성적인 방법은 Risk Matrix와 Risk Graph를 활용하는 방법으로서 과도하게 비관적인 결과를 초래하여 높은 안전무결성 요건을 초래하는데, 이는 위험도 기준과 연계하여 이 방법의 “Calibration”에 대한 어려움이 있어 보수적으로 접근하는 경향이 있기 때문이다.

반면에 정량적인 방법[7]은 상대적으로 낮은 수준의 안전무결성 수준결과를 도출한다. 즉, 정량적인 방법에서는 위험도 기준에 대해 상대적으로 용이하게 접근할 수 있지만, 사용되는 사건/사고의 자료가 충분하지 못하여 실제 평균적 사고확률보다 통계적으로 낮은 사고확률이 도출될 경향이 있다.

준 정량적인 방법은 Risk Matrix와 Risk Graph을 조합하는 관점에서는 정성적인 방법과 동일하지만 정량적 방법에서의 THR을 SIL 수준의 정의와 연계한다는 점에서 정성적인 방법보다는 상대적으로 정량적 방법에 접근하고 있다. 다만, THR 산출에 있어서 시스템의 기능적 위험원을 식별하고 그 개별적인 위험원와 발생빈도를 추정하여 상위 위험원을 고장트리분석 등의 방법으로 연결하여 THR을 산출하는 정량적 방법 대신에 THR/SIL 기준표를 활용하여, THR의 수준과 위험원의 심각도와의 관계식을 설정하여 위험도 저감 요소의 판단으로 SIL을 결정하는 방법이다.

이 방법은 정성적인 방법보다는 보수적인 것으로 알려져 있지만[8], 상세한 연구결과는 없다.

본 논문에서는 사건 또는 사고 자료가 가용하지 않고 또한 설비의 고장률 등이 산출되기 이전이어서 정량적 방법에 의한 THR 산출이 용이하지 않고, 유사 시스템에 대한 위험발생빈도 등에 대한 경험적 자료가 가용하지 않은 상태에서 Risk Matrix를 기반으로 한 준 정량적(Semi-quantitative)인 방법을 적용한다.

III. 준 정량적 SIL 할당 방법 및 절차

설비에 대한 SIL 할당은 만약 그 설비가 설치되지 않은 경우 초래되는 위험도를 허용위험도 수준으로 저감해야 하는 정도에 따라 결정된다. SIL 할당은 다음의 절차를 따른다.

(1) 기능 분석: 안전기능 식별
(2) 안전기능의 안전시스템 할당
(3) 안전기능에 부과되는 안전수준의 식별
(4) 위험도 저감 방안 식별

준 정량적 방법의 기본 원칙은 다음과 같다.

1) [원칙 1] 위험도는 아래와 같이 정의한다. 즉,

$$\text{위험도}(Risk)=\text{위험발생빈도}(f)\,x\,\text{위험심각도}(C)$$

2) [원칙 2] 위험 심각도 범주는 SIL 범주와 동일하다. 즉, $THRn = SILn$이다. 여기서 n은 위험 심각도의 수준이다 (n=4 : 재난적, n=3: 심각한, n=2: 보통의, n=1: 무시할 만한).

3) [원칙 3] 위험발생빈도(f)는 다음과 같이 분해한다. 즉,

$$\text{위험발생빈도}(f) = F \cdot W \cdot P$$

F : 위험에 노출될 가능성 (F)
W : 위험사건 발생확률 (W)
P : 위험사건을 회피하지 못할 가능성(P)
이때 위험도는 다음과 같이 정의된다. 즉,

위험도$(Risk) = (F \cdot W \cdot P) \cdot C$

위 세 원칙의 의미는 다음과 같다. 위험심각도는 어떤 위험원이 초래하는 피해의 최대의 심각도이기 때문에 어떤 설비가 부재할 경우 발생될 수 있는 피해 결과여서 해당 설비의 요구되는 SIL 수준의 요소에서는 고정값이 할당된다. 즉, 그 설비 외 타 설비 또는 외부의 위험저감 방안이 부재하다고 가정하면, 그 설비의 기능적 중요성은 요구되는 SIL 수준의 위험심각도와 동일하다. 따라서 SIL 수준에 영향을 주는 인자(혹은 위험도를 저감하는 인자)는 위험발생빈도를 구성하는 세 가지 영향 인자 (Risk Impacting Factor)가 된다. 따라서, F, W, P의 수준을 식별하여 그 설비의 위험도 수준을 결정한다. 만약, 어느 위험이 초래하는 결과를 회피할 수 없다면 위험발생빈도의 저감을 통하여 위험도를 저감할 수 밖 에 없다.

표 1. 위험도 메트릭스
Table 1. Risk matrix

		Severity(C)			
		Ⅳ.Insignificant	Ⅲ.Marginal	Ⅱ.Critical	Ⅰ.Catastrophic
Frequency (f)	A.Frequent	Undesirable	Intolerable	Intolerable	Intolerable
	B.Probable	Tolerable	Undesirable	Intolerable	Intolerable
	C.Occasional	Tolerable	Undesirable	Undesirable	Intolerable
	D.Remote	Negligible	Tolerable	Undesirable	Undesirable
	E.Improbable	Negligible	Negligible	Tolerable	Tolerable
	F.Incredible	Negligible	Negligible	Negligible	Negligible

먼저 원칙 2를 적용하기 위해서는 Risk Matrix 및 위험도 구성요소의 특성과 IEC62425/EN50129에서 정의한 허용위험발생률 (Tolerable Hazard Rate, THR)과 SIL 수준과의 관계를 활용한다. Table 1의 THR-SIL의 관계에서 보면 SIL n의 THR은

$$10^{-(5+n)} \le THR \le 10^{-(4+n)}$$

이다. 즉 SIL 의 증감으로 인한 해당 THR은 $10^{\pm m}$ 배(m=1,2,3 또는 4)가 된다. (m 단계 SIL 감소이면 10^{+m}, m 단계 SIL 상승이면 10^{-m}) 예를 들면, 위험발생빈도를 한 단계 저감하거나 (예, 빈번한->있음직한), 위험결과의 심각도를 한 단계 감소시키는(예, 치명적인->중대한) 방안을 마련하여 SIL 수준을 한 단계 하향시키는 경우 원래의 만족해야 할 THR은 THRx10^{-1}이 된다.

표 2. THR과 SIL과의 관계
Table 2. Relation of THR & SIL($THR_n = SIL_n$)

THR/time	SIL
$10^{-9} \le THR4 < 10^{-8}$	SIL 4
$10^{-8} \le THR3 < 10^{-7}$	SIL 3
$10^{-7} \le THR2 < 10^{-6}$	SIL 2
$10^{-6} \le THR1 < 10^{-5}$	SIL 1

원칙 3을 적용하기 위해서는 위험발생빈도(f)를 F, W, P로 분해하고 표 3과 같이 위험발생빈도 저감 요소 (즉, 위험도 저감 요소)를 정의한다.

표 3. 위험도 저감 요소 분류
Table 3. Factors of reduction risk

Fac	Define	V	Description
F	risk factor	1	Risk occurrence frequency is frequent and continuously
		10^{-1}	Risk generation frequency is occasional
		10^{-2}	Risk generation frequency is very rare
W	accident reduction factor	1	Not exist
		10^{-1}	Only one exist
		10^{-2}	Several case exist
P	risk evasion possibility	1	Not exist risk
		10^{-1}	Only one exist
		10^{-2}	Several case exist

마지막으로, SIL 수준의 결정은 다음 식을 따른다.

$$\frac{THR_n}{F \cdot W \cdot P} = THR_m \rightarrow SIL_m \, (n, m = 1,2,3,4)$$

Ⅳ. 적용 결과

4.1 유도루프식 열차제어시스템 개요

열차제어시스템의 장치별 하드웨어 및 소프트웨어 분류는 그림 1과 같다. 최상위 레벨인 열차제어시스템에 Subsystem으로 차상신호설비, 지상신호설비, 관제설비, 신호기계실설비, 전원설비, 안전설비로 나뉠 수 있다. 좀 더 상세히 설명하면 차상신호설비는 차상 ATP/ATO장치, 화면표시장치, ATP/TD장치, ATO Local 장치, 속도 검출기, ATO 데이터장치 등으로 구성되며, 지상신호설비는 지상ATP장치와 그 부속장치, 지상ATO 장치 및 그 부속장치, 전자연동장치는 연동논리 랙, 현장 단말 랙, Local console 등으로 구성되며, 관제설비는 주컴퓨터인 TCC, DCC, Operator console, Programmer console, Supervisor console, Wall controller, Depot console 등으로 구성되며, 신호기계실설비의 FT/OT랙, I/F 랙으로 전원설비는 UPS, Battery, 분전반 등으로 구성되며, 추가 안전설비로 강풍, 강우 검지장치로 구성된다.[10][11][12]

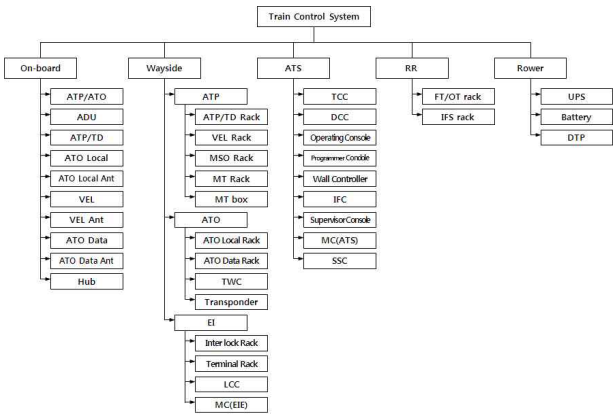

그림 1. 열차제어시스템의 개요
Fig. 1 Overview of TCS

4.2 HAZOP (HAZard and OPerability Study)

HAZOP은 위험요인 규명을 위해 주로 활용되는 brainstorming 방식의 분석 방법이다. 이는 설계에 대한 체계적이고 창의적인 의견 도출 및 설계 경험이 풍부한 전문 엔지니어들의 기술사항을 바탕으로 수행된다.

HAZOP은 시스템 수명주기 동안 위험요인 도출을 위한 각 단계별로 수행되는 분석방법인 예비 위험요인 분석(PHA), 시스템 및 서브시스템 위험요인 분석(SHA/SSHA), 인터페이스 위험요인 분석(IHA), 운영 및 지원상의 위험요인 분석(O&SHA) 등 다양한 분석 방법에 적용된다.

본 논문에서는 예비 위험요인 분석(PHA)을 위하여 HAZOP방법론을 적용하여 표 4와 같은 가이드워드(Guideword)를 사용하여 설계의도에서 벗어난 예외항목들을 도출함으로써, 위험요인을 규명하였다.

표 4. HAZOP의 가이드 워드
Table 4. Guideword of HAZOP

Guide word	Description	Remark
NO/Not	No output on the design	
More	Quantitative output increase than design	
Less	Quantitative output decrease than design	
As Well As	Qualitative output increase than design	
Part Of	Qualitative output decrease than design	
Reverse	Provides a logically opposite outputs	
Other Than	Provides a completely different output	
Too Late	Output too late compare to design	
Too Fast	Output too fast compare to design	
Too Much	Output too much compare to design	
Too Little	Output too little compare to design	

4.3 위험요인 발생빈도와 안전무결성등급 관계

위험요인 발생빈도에 대해 년간 발생빈도 분류를 참고하여 표 5와 같은 안전무결성 등급 Matrix를 나타내었다.

표 5. HAZOP의 가이드 워드
Table 5. Guideword of HAZOP

		Severity			
		1.Insignificant	2.Marginal	3.Critical	4.Catastrophic
Frequency	F.Incredible	SIL 0	SIL 0	SIL 2	SIL 2
	E.Improbable	SIL 0	SIL 0	SIL 2	SIL 2
	D.Remote	SIL 0	SIL 0	SIL 2	SIL 2
	C.Occasional	SIL 0	SIL 2	SIL 4	SIL 4
	B.Probable	SIL 0	SIL 2	SIL 4	SIL 4
	A.Frequent	SIL 0	SIL 2	SIL 4	SIL 4

4.4 기능 분석 및 안전기능 할당

표 6은 TCS 기능분석 결과이며, 기능에 해당되는 TCS의 서브시스템을 대응한 결과이다. 표 6은 3장에서 기술한 SIL 할당 방법 및 절차를 적용한 결과이다.

표 6. TCS 기능분석 및 안전기능 할당 결과
Table 6. TCS allocation of safety function

Function	Description		Facility
Train protection	train detection	trackside monitoring for train position and train detection	TCC, ATP/TD
	train spacing	safety distance margin for prevent train collisions	ATP, EI
	route control	prevention of train collision and unsafe route operation between divided track	ATP, EI
	overspeed protection	overspeed control prevent collisions train	ATP
Train protection	train/track Supervision	train route direction monitoring and safety-related on-board system monitoring	ATS, ATP
Train operation	speed control	limits speed control & service schedule	ATP, ATO
	stop /start	Station stop & departure for specific location	ATO TWC
Train Supervision	Train diagram and display		TCC
	Train route control		TCC,EI
	Performance monitoring and modification		OC,PC
	Alarm and fault record		MS,SSC
	Record storage		DCC,MC
Information	network	Train control systems and other systems interface	LAN

표 7. TCS에 대한 SIL 할당
Table 7. Allocations of SIL to TCS

Item	Severity level(n)	F,W,P			SIL
Wayside ATP HW	Derail, Collision, Stop	F	frequently Error occurs	1	SIL 4
		W	proceed from risk to accident	1	
		P	can't avoid risk result	1	
Wayside ATP SW	Derail, Collision, Stop	F	frequently Error occurs	1	SIL 4
		W	proceed from risk to accident	1	
		P	can't avoid risk result	1	
Wayside ATO HW	Delay, Inconvenience	F	less risk occurrence	10^{-1}	SIL 2
		W	fault monitoring and avoidance method exist	10^{-1}	
		P	can't avoid risk result	1	
Wayside ATO SW	Delay, Inconvenience	F	less risk occurrence	10^{-1}	SIL 2
		W	fault monitoring and avoidance method exist	10^{-1}	
		P	can't avoid risk result	1	
On-board ATP HW	Derail, Collision Stop	F	frequently Error occurs	1	SIL 4
		W	proceed from risk to accident	1	
		P	can't avoid risk result	1	
On-board ATP SW	Derail, Collision, Stop	F	frequently Error occurs	1	SIL 4
		W	proceed from risk to accident	1	
		P	can't avoid risk result	1	
On-board ATO HW	Delay, Inconvenience	F	less risk occurrence	10^{-1}	SIL 2
		W	fault monitoring and avoi-dance method exist	10^{-1}	
		P	can't avoid risk result	1	
On-board ATO SW	Delay, Inconvenience	F	less risk occurrence	10^{-1}	SIL 2
		W	fault monitoring and avoidance method exist	10^{-1}	
		P	can't avoid risk result	1	
ATS HW	Delay, Error	F	less risk occurrence	10^{-1}	SIL 2
		W	fault monitoring and avoidance method exist	10^{-1}	
		P	can't avoid risk result	1	
ATS SW	Delay, Error	F	less risk occurrence	10^{-1}	SIL 2
		W	fault monitoring and avoidance method exist	10^{-1}	
		P	can't avoid risk result	1	

유도루프식 열차제어시스템의 핵심적인 구성 요소인 지상ATP장치, 차상ATP장치, 지상ATO장치, 차상ATO장치, 관제설비 각각의 서브시스템에 대한 하드웨어 및 소프트웨어 대하여 안전무결성 등급을 할당하였다. 분석 결과 지상 및 차상ATP장치 하드웨어, 소프트웨어는 SIL-4로 Vital한 것으로 하드웨어 및 소프트웨어 설계 시 최고의 안전성이 확보되도록 하여야 하고 관제설비와 지상 및 차상ATO장치는 상대적으로 낮지만 SIL2등급으로 안전관련 시스템으로 보증되어야 함으로 알 수 가 있다.

Ⅴ. 결 론

유도루프식 열차제어시스템의 핵심구성설비인 지상/차상ATP장치, 지상/차상ATO장치, 관제설비의 하드웨어, 소프트웨어에 대한 SIL 할당을 수행하였다. 위험도 매트릭스를 기반으로 설비의 고장으로 인한 위험심각도 등급을 SIL 등급으로 설정하고, SIL에 따라 정의된 허용위험발생률(THR)에 위험발생빈도 저감(결과적으로 위험도 저감) 가능성을 10의 멱승으로 판단하여 목표 THR을 산출하여 SIL을 판단하였다.

SIL 할당결과 서브시스템단위에서 지상ATP장치, 차상ATP장치 하드웨어, 소프트웨어는 SIL 4로, 그리고 지상/차상ATO장치 및 관제설비는 SIL 2 수준으

로 판단되었다. 본 분석에서 적용된 방법은 철도이용객 수 및 사고건수 등 많은 정량적 자료에 기반하는 정량적 방법보다는 보수적이지만 불확도(Uncertainty)가 크다. 그러나 사건 또는 사고 자료가 가용하지 않고 또한 설비의 고장률 등이 산출되기 이전이어서 Risk Matrix를 기반으로 한 준 정량적(Semi quantitative) 인 방법은 정성적인 방법보다는 상대적으로 덜 보수적인 것을 알 수 있다.

참고 문헌

[1] "Functional Safety of Electrical/Electronic/ Programmable electronic safety related system", Part 5, Annex D.IEC 61508-5, 2010.

[2] "Functional Safety of Electrical/ Electronic/ Programmable electronic safety related system, Part 5, Annex E, IEC 61508-5, 2010.

[3] "Functional Safety of Safety Instrumentation Systems for the Process Industry Sector, Part 3, IEC 61511-3, 2000.

[4] "Nuclear Power Plants-Instrumentation and Control for Systems Important to Safety", General Requirements for Systems, IEC 61513 , 2001.

[5] "Development Guidelines for Vehicle Based Software", MISRA, ISBN 0952415607, 1994.

[6] P. Gruhn, "Different SIL (Safety Integrity Level) Selection Techniques Can Yield Significantly, 2004.

[7] CENELEC Report, Railway Applications- Systematic Allocation of Safety Integrity Requirements, R009-004, 2001.

[8] Modsystem/WP 23, Safety Conceptual Approach for Functional and Technical Prescriptions, D86 2006.

[9] Train Control System Preliminary Hazard Analysis, Korea High Speed Railway Coperation, 2013.

[10] Hyung-Sup Lim, Hak-Sun Yoon, Chel-Huan Kim, Deung-Ryeol Ryu, Hwang Cho, Key-Seo Lee, "F-Hessian SIFT-Based Railroad Level-Crossing Vision System", The Journal of the Korea Institute of Electronic Communication Sciences Vol. 5, No. 2, pp. 138- 144, 2010.

[11] Hak-Sun Yun, Key-Seo Lee, Dong-In Yang, Sea-Hwa Oh, Ho-Hung Jung, Sung-Kyun Ryou, "A Study on the Development of Train Control System Data Transmission Technology Using a Wireless Mesh", The Journal of the Korea Institute of Electronic Communication Sciences Vol. 7, No. 1, pp. 149-156, 2012.

[12] Ho-Hung Jung, Yang-Og Ko, Chang-Long Li, Key-Seo Lee, "Study on Precise Positioning using Hybrid Track Circuit system in Metro", The Journal of the Korea Institute of Electronic Communication Sciences Vol. 8, No. 3, pp. 471- 477, 2013.

저자 소개

류승균(Sung-Kyun Ryou)

1987년 서울과학기술대학교 전기공학과 졸업(공학사)
1991년 연세대학교 대학원 전기공학과 졸업(공학석사)
2011년~현재 우송대학교 대학원 철도시스템학과 박사과정
※ 관심분야 : 무선통신 열차제어, RAMS

박재영(Jae-Young Park)

1989년 2월 서울과학기술대학교 전기공학과 졸업(공학사)
1996년 8월 고려대학교 대학원 전기공학과 졸업(공학석사)
2007년 2월 서울과학기술대학교 대학원 철도전기신호공학과 졸업(공학박사)
2007년~현재 우송대학교 철도전기시스템학과 교수
※ 관심분야 : 철도신호, 무선통신 열차제어

윤학선(Hak-Sun Yun)

1995년 2월 서울과학기술대학교 전기공학과 졸업(공학사)
2000년 8월 광운대학교 대학원 제어계측공학과 졸업(공학석사)
2012년 2월 광운대학교 대학원 제어계측공학과 졸업(공학박사)
2003년~현재 한국철도시설공단 연구원
※ 관심분야 : 철도신호, 무선통신 열차제어