Journal of the Korean Society of Safety, Vol. 30, No. 6, pp. 164-173, December 2015
Copyright@2015 by The Korean Society of Safety (pISSN 1738-3803, eISSN 2383-9953) *All right reserved.* *http://dx.doi.org/10.14346/JKOSOS.2015.30.6.164*

결과 심각도 및 리스크 그래프에 기반한 철도 승강장 도어시스템의 안전 무결성 수준 할당

송기태 · 이성일†

한국교통대학교 안전공학과

(2015. 6. 22. 접수 / 2015. 11. 11. 수정 / 2015. 11. 29. 채택)

Allocation of Safety Integrity Level for Railway Platform Screen Door System based on Consequence Severity and Risk Graph

Ki Tae Song · Sung Ill Lee†

Department of Safety Engineering, Korea National University of Transportation

(Received June 22, 2015 / Revised November 11, 2015 / Accepted November 29, 2015)

Abstract : There exists required safety integrity level (SIL) to assure safety in accordance with international standards for every electrical / electronics / control equipment or systems with safety related functions. The SIL is allocated from lowest level (level 0) to highest level (level 4). In order to guarantee certain safety level that is internationally acceptable, application of methodology for SIL allocation and demonstration based on related international standards is required. However, application standard differs from every industry in domestic or international for application on mythology for allocation and demonstration of SIL. Application or assessment is not easy since absence on clear criteria or common definition . This research studied not only fundamental concept of SIL required to guarantee safety in accordance with international standards for safety related equipment and system, but different types of methodologies for SIL allocation. Specifically, SIL allocation for Platform Screen Door system of railway is studied applying methodology of severity of accidents and risk graph among different methodologies for SIL allocation.

Key Words : consequence severity, risk graph, safety integrity level, railway, platform screen door, safety integrity allocation, tolerable hazard rate

1. 서 론

최근 전 세계적으로 크고 작은 안전사고들이 발생하고 있으며, 이러한 사고는 더 이상 단순한 사고나 재산상의 피해로만 여겨지지 않고, 사회적 불안, 갈등 및 경제적 침체를 발생시키고 있어 사회적으로 더욱 심각한 문제가 되고 있다. 이러한 사고에 대한 관리적 대책뿐만 아니라 사고 발생과 관련된 기술적인 측면의 명확한 원인 분석을 통해 개선/조치 방안을 제시하고 추후 사고 관련 장치 또는 시스템의 안전성을 근본적으로 향상시키기 위한 연구와 노력이 필요하다.

상기와 같은 맥락에서 안전성과 관련된 기능이 존재하는 전기/전자/제어 장치나 시스템을 대상으로 국제적인 기준에 따라 안전성을 보증하기 위하여 요구되는 안전 무결성 수준(Safety Integrity Level, SIL)이 있으며, 안전 무결성 수준은 가장 낮은 수준의 Level 0부터 가장 높은 수준의 Level 4까지 할당 될 수 있다[1]. 이에 따라 국제적으로 수용 가능한 안전성을 보증하기 위해서는 관련된 국제규격에 근거하여 적합한 수준의 안전 무결성 수준(Safety Integrity Level)의 할당(Allocation)과 입증(Demonstration) 방법론의 적용이 요구된다. 하지만, 안전 무결성 수준의 할당과 입증과 관련한 방법론의 적용에 있어서는 아직까지 해외나 국내의 여러 산업분야별로 적용규격이 상이하며, 공통된 정의나 명확한 기준이 존재하지 않아 적용이나 평가가 쉽지 않다.

본 연구에서는 안전성과 관련된 장치 또는 시스템과 관련하여 국제 규격에 따라 안전성을 보증하기 위하여 요구되고 있는 안전 무결성 수준에 대한 기본적인 개

† Corresponding Author : Sung Ill Lee, Tel : +82-043-841-5334, E-mail : silee@ut.ac.krDepartment of Safety Engineering, Korea National University of Transportation, 50, Daehak-ro, Chungju-si, Chungbuk 27469, Korea

념과 할당 방법론의 유형에 대하여 연구하고 여러 종류의 안전 무결성 할당 방법론 중 사고심각도와 리스크 그래프 방법론을 적용하여 철도 승강장 도어시스템의 안전 무결성 수준 할당에 대해 연구하였다.

2. 안전 무결성 수준 할당 방법론

안전 무결성 수준은 안전성과 관련된 기능에 대하여 정의될 수 있으며, 이러한 안전성 관련 기능을 구성하는 하위 기능별로 안전 무결성 수준이 할당될 수 있다. 전기/전자/제어 시스템과 관련하여 안전성 무결성 수준에 대한 공통적인 요구사항이 제시되어 있는 대표적인 국제 규격은 "IEC 61508 (Functional safety of electrical / electronic / programmable electronic safety - related system)"이며, 해당 규격에서 정의하고 있는 안전 무결성 할당의 개념은 아래의 Fig. 1과 같다[1].

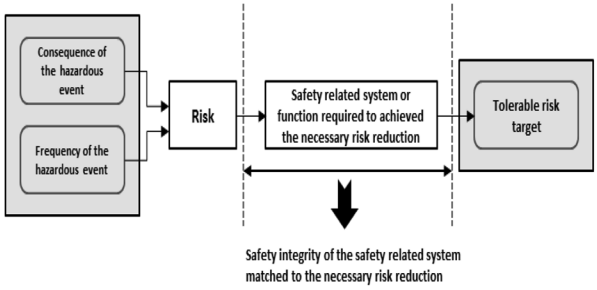

Fig. 1. Concept of safety integrity allocation[1].

또한, 상기의 안전 무결성 할당의 개념과 동시에 각 안전 무결성 수준에 따른 정량적 요구수준으로서 허용 위험요인 발생빈도(Tolerable Hazard Rate, THR)를 아래의 Table 1과 같이 정의하고 있다[1,3].

Table 1. THR and SIL table

Tolerable hazard rate THR per hour and per function	Safety integrity level
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

상기의 Fig. 1, Table 1과 같이 안전 무결성 수준은 안전성 관련 시스템에 대한 위험도 평가 결과에 기반하여 초기 평가된 위험도를 허용 가능한 수준으로 저감시키기 위해 요구되는 시스템 또는 기능에 대한 무결성 수준에 따라 할당되어야 한다. 즉, 잠재 위험요인의 발생

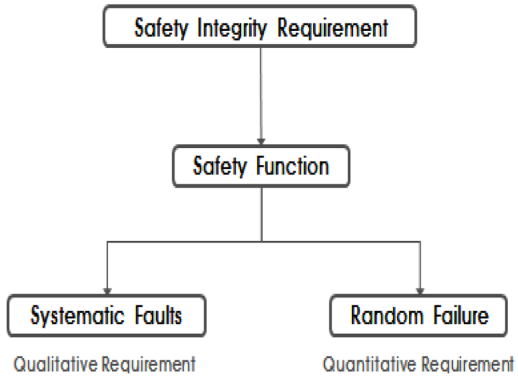

Fig. 2. Concept of safety integrity requirement[3].

빈도 및 결과의 심각도를 고려하여 초기 위험도가 평가되며, 평가된 초기 위험도를 사전에 정의된 허용 가능 위험도까지 저감시키기 위하여 위험요인과 관련된 시스템이나 기능에 요구되는 무결성 수준에 따라 결정될 수 있다. 또한, 여기에서의 무결성(Integrity)은 아래의 Fig. 2와 같이 우발적 결함(Random faults)에 대한 무결성과 계통적 결함(Systematic faults)에 대한 무결성으로 구분되며, 최종적인 안전 무결성은 이러한 두 가지 유형의 무결성이 모두 보증될 때 성취 가능하다[2,3].

여러 산업 분야별 특성을 고려하여 IEC 61508의 일반적 방법론에 기반한 주요 산업분야 별 국제 규격이 별도로 정의되어 있다. 안전 무결성 수준과 관련한 요구사항 및 방법론을 제시하고 있는 여러 산업 분야별 주요 국제 규격은 아래의 Table 2와 같다.

Table 2. International standards for related industries field

Standard No.	Description	Industry
IEC61508	Functional safety of electrical / Electronic / Programmable electronic safety - related system	Electrical / Electronic
IEC61511	Functional safety - Safety instrumented systems for the process industry sector	Process
IEC62278	Specification and demonstration of reliability, availability, maintainability and safety (RAMS)	Railway
IEC62279	Communications, signalling and processing systems - Software for railway control and protection systems	Railway
IEC62425	Communication, signalling and processing systems - Safety related electronic systems for signalling	Railway
IEC62061	Functional safety of safety-related electrical, Electronic and programmable electronic control systems	Machinery
ISO26262	Road vehicles - Functional safety	Automotive industry

상기 정의된 각 산업분야 별 규격에서 제시하고 있는 안전 무결성 할당에 대한 주요 방법론의 종류는 아래의 Table 3과 같다.

Table 3. Safety integrity level allocation method

No	Method
1	ALARP(As Low As Reasonably Practicable) allocation method
2	Quantitative allocation method
3	Risk graph based allocation method
4	Allocation method by layer of protection analysis
5	Consequence severity based allocation method

상기의 주요 방법론 이외에도 실제 여러 산업분야 별로 적용되고 있는 안전 무결성 할당 방법은 더 많이 존재하며, 현재도 상기의 기본적인 방법론에 기반하여 적용 분야 및 대상 시스템 특성에 따라 전체적으로 새롭거나 일부 변경된 형태의 방법론이 제시되고 있다. 이렇게 다양한 할당 방법론이 존재하지만, 기본적으로 안전 무결성 할당을 위하여 수행되어야 하는 일반적인 활동은 공통적으로 존재한다. 시스템에 존재하는 안전성 관련 기능에 대하여 안전 무결성 수준을 할당하기 위하여 기본적으로 대상 시스템의 정의 및 기능 분석, 위험요인 및 위험도 분석, 안전성 관련 기능 정의, 안전 무결성 할당 방법론 적용에 따른 SIL 할당의 절차에 따라 수행된다.

상기의 Table 3에 기술된 할당 방법론을 통해 안전 무결성 수준을 할당하기 위하여 수행되는 일반적인 절차는 아래의 Fig. 3과 같다.

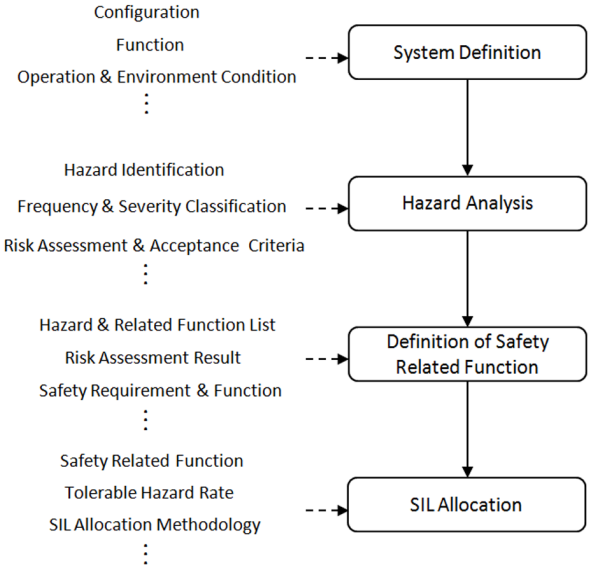

Fig. 3. General procedure of safety integrity allocation.

본 연구에서는 Table 3과 Fig. 3에 정의된 방법론 및 절차에 기반하여 철도 산업분야 적용 연구를 위해 철도 시스템 중 승강장 스크린 도어 시스템을 대상으로 리스크 그래프에 근거한 할당 방법론과 결과 심각도에 근거한 할당 방법론 적용에 관련한 연구를 수행하였다.

2.1 결과 심각도에 기반한 할당 방법론

결과 심각도에 기반한 할당 방법론(Consequence severity based allocation method)은 정성적인 할당 방법론으로서 시스템 위험요인 분석 및 위험도 평가 결과 중 위험요인의 결과에 대한 심각도만을 고려하여 해당 위험요인과 관련된 안전성 관련 기능에 대해 사전에 정의된 심각도 등급별 허용 위험요인 발생률 기준을 적용하여 요구되는 안전 무결성 수준을 할당하는 방법론이다[1,3].

상기에서 언급한 바와 같이 결과 심각도에 기반한 할당 방법론 적용을 위해서는 국가별 또는 산업분야 별로 적합한 근거 및 절차에 기반하여 심각도 분류기준/등급에 따른 허용 위험요인 발생률이 정의되어 있어야 한다. 하지만, 국내에서는 철도시스템과 관련한 허용 위험요인 발생률이 명확하게 정의되어 있지 않으므로, 본 연구에서는 안전 무결성 수준과 관련하여 국제규격에서 제시하고 있는 허용 위험요인 발생률과 국내 철도 운영 기관에서 정의하고 있는 심각도 분류 등급을 적용하여 유럽의 여러 국가에서 적용하고 있는 공통적인 허용 기준으로서 승객 1인 사망사고 허용 발생률로서 10^{-6}/h을 심각도 등급 Major 등급에 할당하였다[2,3]. 이는 국제적인 허용 기준에 기반하여 보수적인 기준으로 판단할 수 있다. 이러한 방법을 통해 결과 심각도에 기반한 안전 무결성 할당 기준을 아래와 같이 사전 정의하였다.

2.2 위험도 그래프에 기반한 할당 방법론

위험도 그래프에 기반한 할당 방법론(Risk graph based allocation method)은 기본적으로는 정성적인 할당 방법론으로서 시스템 위험요인 분석 및 위험도 평가 결과에 근거하여 위험요인의 결과 심각도, 위험요

Table 4. Severity level & THR allocation criteria

Cat.	Severity level	THR	SIL level
C6	Disastrous	10^{-9}/h	SIL4
C5	Catastrophic	10^{-8}/h	SIL4
C4	Critical	10^{-7}/h	SIL3
C3	Major	10^{-6}/h	SIL2
C2	Minor	10^{-5}/h	SIL1

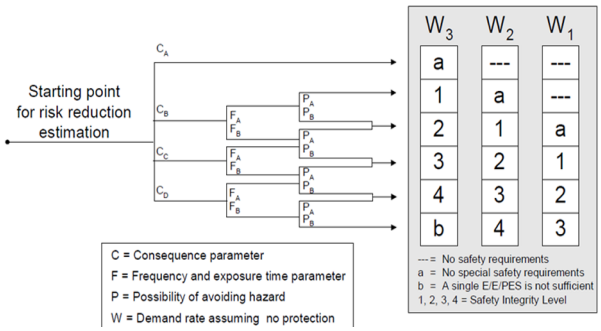

Fig. 4. Risk graph for safety integrity level allocation[1,3].

인 발생/노출빈도, 위험요인 회피 가능성, 위험상황/조건 발생확률에 따라 사전에 정의된 리스크 그래프를 통해 안전 무결성 수준을 할당하는 방법론이다[1,3].

상기에서 언급한 바와 같이 리스크 그래프에 기반한 할당 방법론 적용을 위해서는 리스크 그래프와 리스크 그래프에서 적용되는 각 파라미터의 분류기준이 사전 정의되어 있어야 한다. 국제규격에 근거하여 해외에서 전기/전자/제어 시스템과 관련하여 일반적으로 사용되는 리스크 그래프는 아래와 같다.

Fig. 4에서 정의된 리스크 그래프 방법론 적용 시 안전 무결성 수준 할당결과에 주요한 영향을 미치는 것은 해당 방법론 적용 시 고려되는 파라미터이다. 따라서, 이러한 파라미터에 대한 명확한 의미 및 분류기준은 적용될 산업분야의 특성, 국가 별 안전 허용 기준, 대상 시스템의 운영환경 및 특성을 고려하여 명확하게 정의되어야 한다. 본 연구에서는 안전 무결성 할당 방법과 관련된 국제규격[1,3,5] 및 참조문헌[4,6]에 기반하여 아래의 Table 5와 같이 정량적 및 정성적 분류기준을 정의하였다.

Table 5. Risk graph parameter categories & criteria

Category		Quantitative description	Qualitative description
C	C_A	Death $\leq$ 0.01	Minor
	C_B	0.01 < Death $\leq$ 0.1	Major
	C_C	0.1 < Death $\leq$ 5	Critical
	C_D	5 $\leq$ Death	Catastrophic
F	F_A	Occupied/Exposed < 10% of time	Rare to more frequent
	F_B	Occupied > 10%	Frequent to continuous
P	P_A	N/A	Possible (considering the alert measure or avoidable time)
	P_B	N/A	Hardly possible
W	W_1	< 0.1 per year	Slight
	W_2	Between 1 and 0.1 per year	Occasional
	W_3	> 0.1 per year	Frequent

3. 적용 사례

본 연구에서 제시한 결과 심각도 및 리스크 그래프에 기반한 안전 무결성 할당 방법론을 철도 승강장 도어 시스템을 대상으로 다음과 같이 적용하여 결과검토를 수행하였다.

3.1 시스템 개요

국내 지하철 승강장에 적용되는 일반적인 스크린 도어 시스템은 주요하게 구동부, 제어반, 센서 등으로 구성되어 있으며 아래의 Fig. 5와 같다.

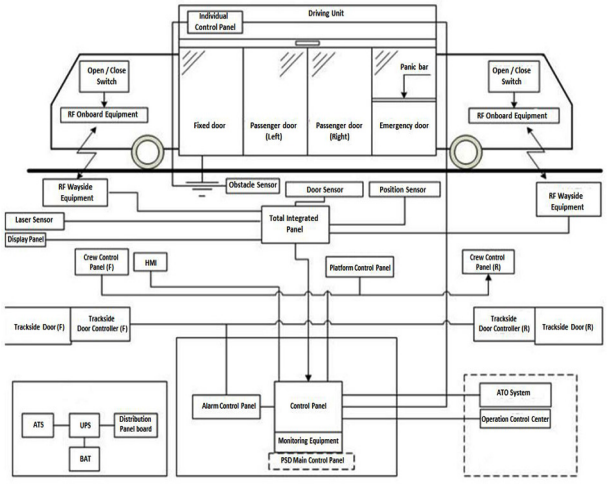

Fig. 5. Platform screen door system configuration.

3.2 위험요인 분석 및 위험도 평가

국내 지하철 승강장에 적용되는 승강장 스크린도어 시스템에 대한 위험요인을 도출하기 위하여 우선적으로 승강장 스크린 도어시스템의 주요 하부구성장치 분류 및 각 장치별 기능을 정의하였다. 이렇게 정의된 승강장 스크린 도어시스템 정보를 기반으로 국내 철도 안전성 분석 및 평가 경험을 보유한 전문가들이 참여한 브레인스토밍 방식의 회의를 통해 주요 구성기능상에서 발생 가능한 잠재 위험요인을 식별하고 위험요인의 원인 및 영향을 분석하였다. 또한 분석된 위험요인 관련 원인 및 영향에 근거하여 위험도 평가를 수행하였다. 위험도 평가 시 적용된 위험도 매트릭스는 국내 철도 운영 기관에서 적용된 사례가 있는 위험도 평가 기준을 적용하였으며, 다음의 Table 6과 같다.

상기에서 언급한 위험요인 분석 방법과 위험도 매트릭스에 기반하여 수행된 승강장 스크린도어 시스템의 위험요인 분석 결과의 일부는 아래 Table 7, 8과 같다.

Table 6. Risk matrix

Application: Specific railway line (including KTX, EC & existing line)				Cosequence (Service)	Disruption to line services	<10 mins	>10 mins <20 mins	>20 mins <2 hours	>2 hours <8 hours	>8 hours <1 day	>1 day
				Consequence (Service)	Fatality	0	0	0	1	2-10	>10
					Major Injury	0	0	>1			
					Minor Injury	0	>1				
					Ranking	C1	C2	C3	C4	C5	C6
	Qualitative	Descriptive	Numeric	Ranking		Neqliqible	minor	major	Critical	Catastrophic	Disastrous
Likelihood	Has occurred frequently at specific locations	More than 100 times per year	>100	F6	Very likely	B	A	A	A	A	A
	Has occurred frequently in the railway line	10 to 100 times per year	10 to 100	F5	Frequent	B	B	A	A	A	A
	Has occurred once or twice in the railway line	Once to 10 times per year	1 to 10	F4	Probable	B	B	B	A	A	A
	Has occurred many times in the industry, but not in the railway line	Once every 1 to 10 year	1 to 1/10	F3	Occasional	C	B	B	B	A	A
	Has occurred once or twice in the industry	Once every 10 to 100 year	1/10 to 1/100	F2	Remote	C	C	B	B	B	A
	Unheard of in the industry	Less than once every 100 years	<1/100	F1	Improbable	C	C	C	B	B	B

Table 7. Hazard analysis sheet(1/2)

Subsystem &Equipment ID	Subsystem& Equipment	Function	Hazard ID	Hazard	Cause	Mode	Effect / Consequence	Sev.	Freq.	Risk	Mitigation measure / Safety requirements	Remark
1-2-1	Emergency door and manual opening equipment	In emergency situation, Provide emergency door opening manually by passenger from track side	SH_03	Fail to make room for passenger evacuation in emergency situation	Mechanical / Physical failure of emergency door Manual open device failure	Emergency	• In worst case, multiple fatalities are possible due to failure of evacuation from track side to platform in emergency situation	C6	F3	A	• Emergency door and manual open device should be designed that the doors opening are available in emergency situation • Faults of door should be checked by regular function test • In the situation of fail to open emergency door, the emergency tool such as emergency hammer should be furnished in order to break glass • Operation and maintenance procedure should be defined to prevent possible accident due to the hazard	
1-3-1	Crew and platform control panel	Provide all passenger door opening / Closing manually by crew in train or station	SH_05	Fail to manual control and bypass of passenger door	Failure of open / Close button for passenger door	Emergency	• In worst case, multiple fatalities are possible due to failure of evacuation from track side to platform in emergency situation by fire in train	C6	F3	A	• Open / Close button should be applied in accordance with related standards or regulation • Periodic maintenance activity should be conducted	• It is assumed that there is emergency door opening equipment which can be controlled by passenger in case of failure of crew and platform control panel
1-3-2	Crew and platform control panel	Provide all passenger door opening / Closing manually by crew in train or station	SH_06	Fail to manual control and bypass of passenger door	Failure of open / Close button for passenger door	Normal	• In case of necessity, Passenger falling in door open status, or passenger has been stucked in door close status	C4	F4	A	• Open / Close button should be applied in accordance with related standards or regulation • Periodic maintenance activity should be conducted	
1-3-3	Position sensor	Detection of precise stopping of train	SH_07	Fail to detect precise stopping of train	Failure of infrared ray sensor for precise stopping	Normal	Passenger door can't open and passenger can't alight form train due to failure of precise stopping detection. It dose not affect safety	C1	F4	B	• Infrared ray sensor should be applied in accordance with related standards or regulation • Position sensor should be designed to be redundancy structure • Operation and maintenance procedure should be defined to prevent possible accident due to the hazard	• It is assumed that platform screen door can be manually opened or closed by crew and platform control panel, also there is emergency door opening equipment which can be controlled by passenger

Table 8. Hazard analysis sheet(2/2)

Subsystem &Equipment ID	Subsystem& Equipment	Function	Hazard ID	Hazard	Cause	Mode	Effect / Consequence	Sev.	Freq.	Risk	Mitigation measure / Safety requirements	Remark
1-3-5	Total integrated panel	Provide automatic passenger door opening / Closing using information	SH_09	Fail to automatic control for open / Close of passenger door	Failure of control module	Normal	• In case of necessity, Passenger falling in door open status, or passenger has been stucked in door close status.	C4	F4	A	• In case of failure of control module, fault detection design should be applied to able that the crew of station and train recognize the faults. • Control module must have certification for environment test and railway signalling product qualification. • Operation and maintenance procedure should be defined to prevent possible accident due to the hazard.	
1-3-6	Laser sensor	Measurement of distance between precise stopping position and train	SH_10	Fail to measure of distance between precise stopping position and train	Failure of laser sensor	Normal	Train can't stop at precise position, but It dose not affect safety because of manual operation by driver in train.	C1	F4	B	• Laser sensor should be applied in accordance with related standards or regulation. • Periodic maintenance activity should be conducted.	
1-3-9	Door sensor	Detection of open / Close status of train door.	SH_12	Fail to detect open / Close status of train door	Failure of detection sensor for train door	Normal	• Due to wrong train door status information from train door detection sensor, Passenger is bumped into passenger door in train door open status, or passenger has been stucked.	C4	F4	A	• Train door detection sensor should be applied in accordance with related standards or regulation. • Train door detection sensor should be designed to be redundancy structure. • In case of failure of train door detection sensor, fault detection design should be applied. • Operation and maintenance procedure should be defined to prevent possible accident due to the hazard.	
1-1-2	Individual door control panel (DCU)	Control opening and closing of passenger door, reception of power, signal control of manual control panel, signal control of total integrated control panel	SH_02	Fail to control opening and closing of passenger door	Failure of DCU	Normal	• In the passenger door open status, if there is failure of door control module, passenger falling to track. • Wrong motor control could happen due to software error. in worst case, passenger falling to track. • Wrong reception and calculation of obstacle information could happen. In worst case, passenger falling to track or jamming in gap between train door and passenger door.	C4	F4	A	• In case of failure of door control unit, fault detection design should be applied to able that the crew of station and train recognize the faults. • Door control unit must have certification for environment test and railway signalling product qualification. • Software and cable in door control unit should ensure quality and safety. • Operation and maintenance procedure should be defined to prevent possible accident due to the hazard.	

3.3 안전성 관련 기능 정의

Fig. 3의 SIL 할당 절차에 따라 위험요인 분석 후의 안전성 관련 기능을 정의하기 위하여 상기 3.2절의 위험요인 분석에서 식별된 각각의 위험요인을 제거하거나 위험도를 저감시키기 위한 기능적 안전성 요구사항을 승강장 스크린 도어 시스템의 안전성 관련 기능으로 정의하였다. 예를 들어, 식별된 위험요인 중 “SH_03 비상 시 승객 대피를 위한 공간 미확보”에 대해서는 비상 시 스크린 도어의 제어와 관련한 안전성을 보증하기 위해 요구되는 승강장 스크린도어 시스템의 기능은 “비상 시 열차 또는 선로로부터 승강장으로 승객을 안전하게 대피시키기 위한 수동 개폐 기능”이 요구되며, “SH_07 열차의 정위치 정차 검지 실패”의 경우에는 “승강장에서의 열차 정위치 정차의 안전한 검지 기능”이 요구된다. 또한, “SH_09 승강장 출입문 자동 개폐 제어 실패”의 위험요인과 관련해서는 안전성 보증을 위하여 “열차의 정차 위치와 출입문 상태정보에 기반한 승강장 스크린도어 시스템의 안전한 승객 출입문 자동 개폐 제어 기능”을 안전성 관련 기능으로 정의하였다. 결과적으로, 위에서 설명한 방법에 의해 Table 7과 Table 8에서 식별된 각각의 위험요인을 기반으로 정의된 승강장 스크린도어 시스템의 안전성 관련 기능

Table 9. Safety related functions for platform screen door system

ID	Safety Function	Ref. Haz. ID
SF_01	Provide safe platform screen door opening / Closing operation by manual control of passenger in emergency situation to evacuate from track/train to platform	SH_03
SF_02	Provide safe platform screen door opening / Closing operation by manual control of crew in train or station in emergency situation	SH_05
SF_03	Provide safe platform screen door opening / Closing operation by manual control of crew in train or station in normal situation	SH_06
SF_04	Provide safe detection of precise train stopping	SH_07
SF_05	Provide safe platform screen door opening / Closing operation by automatic control based on status information for train opening / Closing status and precise train stopping	SH_09
SF_06	Provide safe detection of distance between precise stopping position and train	SH_10
SF_07	Provide safe detection of train door opening / Closing status	SH_12
SF_08	Provide safe automatic individual door control for platform screen door opening / Closing operation by opening / Closing command and power	SH_02

은 아래의 Table 9와 같다.

3.4 결과 심각도에 기반한 안전 무결성 수준 할당 결과

Table 7, 8의 위험요인 분석결과를 참조하여 Table 9에 정의된 각 위험요인 별 안전성 관련 기능에 SIL을 할당하기 위해서 Table 4에서 정의된 심각도 수준에 따른 허용 위험요인 발생률(THR) 기준을 적용하여 최종적인 SIL을 할당하였다. 즉, 각 위험요인의 초기 위험도 평가 결과에서 심각도 평가 결과에 따라 Table 4에서 정의된 THR을 할당하고 해당 THR에 의해 요구되는 SIL을 할당 하였다. 예를 들어, 안전성 관련 기능 "SF_01"과 관련된 위험요인 "SH_03"의 경우 Table 7, 8의 위험요인 분석결과에 기반하여 초기위험도 평가에서의 심각도 수준이 "C6 (Disastrous)"이므로, 이에 따라 THR은 10^{-9}/h로 할당되며, Table 1과 Table 4에 근거하여 SIL4가 할당된다. 또한, "SH_07"의 경우 심각도 수준이 "C2 (Minor)"이므로, 이에 따라 THR은 10^{-5}/h로 할당되며, Table1과 Table 4에 근거하여 SIL1이 할당된다. 이러한 방법에 따라 Table 7, 8에서 식별된 모든 위험요인 별 THR 및 SIL 할당 결과는 Table 10과 같으며, 해당 결과에 근거하여 Table 9에서 정의된 각각의 안전성 관련 기능에 대한 심각도 기반 안전 무결성 수

Table 10. Severity based THR&SIL allocation for each hazard

Ref.ID	Hazard	Effect / Consequence	Estimated Severity	Allocated THR	Allocated SIL
SH_03	Fail to make room for passenger evacuation in emergency situation	In worst case, multiple fatalities are possible due to failure of evacuation from track side to platform in emergency situation	Disastrous C6	10^{-9}/h	4
SH_05	Fail to manual control and bypass of passenger door	In worst case, multiple fatalities are possible due to failure of evacuation from track side to platform in emergency situation by fire in train	Disastrous C6	10^{-9}/h	4
SH_06	Fail to manual control and bypass of passenger door	In case of necessity, Passenger falling in door open status, or passenger has been stucked in door close status	Critical C4	10^{-7}/h	3
SH_07	Fail to detect precise stopping of train	Passenger door can't open and passenger can't alight form train due to failure of precise stopping detection	Negligible C1	N/A	0
SH_09	Fail to automatic control for open / close of passenger door	In case of necessity, Passenger falling in door open status, or passenger has been stucked in door close status	Critical C4	10^{-7}/h	3
SH_10	Fail to measure of distance between precise stopping position and train	Train can't stop at precise position, but It dose not affect safety because of manual operation by driver in train	Negligible C1	N/A	0
SH_12	Fail to detect open / close status of train door	Due to wrong train door status information from train door detection sensor, Passenger is bumped into passenger door in train door open status, or passenger has been stucked	Critical C4	10^{-7}/h	3
SH_02	Fail to control opening and closing of passenger door	• In the passenger door open status, if there is failure of door control module, passenger falling to track • Wrong reception and calculation of obstacle information could happen. In worst case, passenger falling to track or jamming in gap between train door and passenger door	Critical C4	10^{-7}/h	3

Table 11. Consequence severity based SIL allocation results for safety related function

ID	Safety function	SIL Allocation result
SF_01	Provide safe platform screen door opening / Closing operation by manual control of passenger in emergency situation to evacuate from track / Train to platform	SIL4
SF_02	Provide safe platform screen door opening / Closing operation by manual control of crew in train or station in emergency situation to evacuate from track / Train to platform	SIL4
SF_03	Provide safe platform screen door opening / Closing operation by manual control of crew in train or station in normal situation to evacuate from track / Train to platform	SIL3
SF_04	Provide safe detection of precise train stopping	SIL0
SF_05	Provide safe platform screen door opening / Closing operation by automatic control based on status information for train opening / Closing status and precise train stopping	SIL3
SF_06	Provide safe detection of distance between precise stopping position and train	SIL0
SF_07	Provide safe detection of train door opening / Closing status	SIL3
SF_08	Provide safe automatic individual door control for platform screen door opening / Closing operation by opening / Closing command and power	SIL3

준 할당 결과는 최종적으로 Table 11과 같다.

3.5 리스크 그래프에 기반한 안전 무결성 수준 할당 결과

리스크 그래프에 기반한 안전 무결성 수준 할당을 위해 Table 7, 8의 위험요인 분석결과를 참조하여 Table 5에 정의된 리스크 그래프 파라미터 분류 및 기준에 따라 각 위험요인 별 리스크 파라미터를 정의하였다. 이렇게 결정된 각각의 리스크 파라미터 데이터를 기반으로 Fig. 4에 정의된 리스크 그래프에 적용하여 각 위험요인 별 SIL을 최종적으로 할당하였다. 즉, 각 위험요인 분석 결과에 근거하여 리스크 그래프를 적용하기 위한 리스크 파라미터를 Fig. 4에 정의된 적용 절차에 따라 C(consequence), F(frequency or exposure time), P(possibility of avoiding the hazardous event), W(probability of the unwanted occurrence) 순으로 결정하고 해당 결과에 따라 최종적으로 도달되는 SIL 수준을 최종 결정한다. 예를 들어, 안전성 관련 기능 "SF_01"과 관련된 위험요인 "SH_03"의 경우 Table 7, 8의 위험요인 분석결과에 기반하여 결과적 심각도가 Table 5에 정의된 기준으로 "C_D"에 해당하며, 발생빈도는 승객 출입문 수동제어 기능과 관련하여 별도의 설계적인 저감대책이 적용되지 않았음을 보수적으로 가정하여 "F_B"로 결정 하였다. 또한, 터널 내 또는 열차 내 화재 발생 시와 같은 최악의 상황에서 승객대피를 위한 스크린 도어의 수동제어가 불가능한 경우를 고려하여 회피 가능성 또한 보수적으로 "P_B"로 결정하였으며, 위험요인 발생 시 최악의 사고발생이 가능한 위험상황 또는 조건의 발생 확률과 관련해서는 터널에서의 차량 내 화재발생 조건을 고려하여 낮은 발생 확률 분류의 "W_1"으로 결정하였다. 이러한 방법에 따라 Table 7, 8에서 식별된 모든 위험요인 별 리스크 파라미터 분석 결과와 SIL 할당 결과는 Table 12와 같으며, 해당 결과에 근거하여 Table 9에서 정의된 각각의 안전성 관련 기능에 대한 리스크 그래프 기반 안전 무결성 수

Table 12. Risk graph based risk parameter&SIL allocation for each hazard

Ref.ID	Hazard	Consequence (C)	Frequency, and exposure time in, the hazardous zone (F)	Possibility of avoiding the hazardous event (P)	Probability of the unwanted occurrence (W)	Result (SIL)
SH_03	Fail to make room for passenger evacuation in emergency situation	C_D	F_B	P_B	W_1	3
SH_05	Fail to manual control and bypass of passenger door	C_D	F_B	P_A	W_1	2
SH_06	Fail to manual control and bypass of passenger door	C_B	F_B	P_B	W_2	2
SH_07	Fail to detect precise stopping of train	C_A	F_B	P_B	W_3	0
SH_09	Fail to automatic control for open / Close of passenger door	C_B	F_B	P_B	W_3	3
SH_10	Fail to measure of distance between precise stopping position and train	C_A	F_B	P_B	W_3	0
SH_12	Fail to detect open / Close status of train door.	C_B	F_B	P_B	W_3	3
SH_02	Fail to control opening and closing of passenger door	C_B	F_B	P_B	W_3	3

Table 13. Risk graph based SIL allocation results for safety related function

ID	Safety function	SIL Allocation result
SF_01	Provide safe platform screen door opening / Closing operation by manual control of passenger in emergency situation to evacuate from track / Train to platform	SIL3
SF_02	Provide safe platform screen door opening / Closing operation by manual control of crew in train or station in emergency situation	SIL2
SF_03	Provide safe platform screen door opening / Closing operation by manual control of crew in train or station in normal situation	SIL2
SF_04	Provide safe detection of precise train stopping	SIL0
SF_05	Provide safe platform screen door opening / Closing operation by automatic control based on status information for train opening / Closing status and precise train stopping	SIL3
SF_06	Provide safe detection of distance between precise stopping position and train	SIL0
SF_07	Provide safe detection of train door opening / Closing status	SIL3
SF_08	Provide safe automatic individual door control for platform screen door opening / Closing operation by opening / Closing command and power	SIL3

Table 14. Comparison of THR&SIL allocation result

Function ID	THR			SIL		
	Consequence severity based allocation	Risk graph based allocation	Difference	Consequence severity based allocation	Risk graph based allocation	Difference
SF_01	10^{-9}/h	10^{-7}/h	10^{-2}/h	4	3	1
SF_02	10^{-9}/h	10^{-6}/h	10^{-3}/h	4	2	2
SF_03	10^{-7}/h	10^{-6}/h	10^{-4}/h	3	2	1
SF_04	N/A	N/A	-	0	0	-
SF_05	10^{-7}/h	10^{-7}/h	-	3	3	-
SF_06	N/A	N/A	-	0	0	-
SF_07	10^{-7}/h	10^{-7}/h	-	3	3	-
SF_08	10^{-7}/h	10^{-7}/h	-	3	3	-

준 할당 결과는 최종적으로 Table 13과 같다.

3.6 THR 및 안전 무결성 수준 할당 결과 비교

상기 3.4절과 3.5절에서의 결과 심각도와 리스크 그래프에 기반한 각각의 THR 및 안전 무결성 수준 할당 결과를 비교하여 정리하면 아래의 Table 14, Fig. 6과 같다.

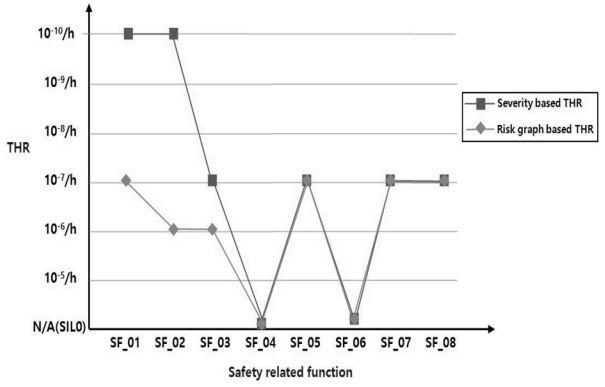

Fig. 6. Platform screen door system configuration.

Table 14와 Fig. 6의 비교 결과를 통해 결과적 심각도 기반의 할당 결과와 리스크 그래프를 통한 할당 결과가 최대 THR 기준 10^{-3}/h의 차이와 SIL 기준 2레벨의 차이가 발생되었음을 확인하였다. 차이가 발생된 안전성 관련 기능(SF_01~SF_03)에 대한 위험요인 분석결과를 고려할 때, 이러한 결과는 심각도만을 고려한 할당 방법론과 비교하여 위험요인 발생 시 사고를 회피할 수 있는 추가적인 대책(Barrier)의 존재여부와 사고발생을 유발하는 요인(Trigger factor) 또는 사건(Trigger event)의 발생 확률을 고려하는 리스크 그래프 특성에 의해 차이가 발생된 것으로 사료된다.

4. 결론 및 고찰

본 연구에서는 철도 시스템의 안전 무결성 수준 할당 방법론 중 심각도에 기반한 안전 무결성 수준 할당 방법론과 위험도 그래프를 이용한 안전 무결성 수준 할당 방법론을 적용하여 승강장 스크린 도어시스템의 할당을 수행하고, 그 결과를 비교하였다. 이러한 두 가

지 방법론에 의한 승강장 스크린 도어 시스템의 안전 무결성 수준 할당 결과, 위험요인의 심각도에 기반한 안전 무결성 수준 할당 결과가 리스크 그래프를 이용한 안전 무결성 수준 할당 결과보다 특정 안전성 관련 기능에 대하여 THR은 최소 10^{-1}/h에서 최대 10^{-3}/h까지 차이가 발생 하였으며, SIL과 관련해서는 최소 1레벨에서 최대 2레벨까지 할당결과의 차이가 존재함을 확인하였다. 이는 위험요인의 심각도에 기반한 안전 무결성 수준 할당 결과가 위험도 그래프를 이용한 안전 무결성 수준 할당 결과 보다 상대적으로 초기 위험요인의 위험도 평가 시 위험요인으로 인한 결과를 보수적(Worst Case)으로 평가하며, 해당 위험요인 발생 시 결과적인 사고를 회피할 수 있는 외부적인 대책(Barrier) 및 사고발생을 유발하는 사건(Trigger event)에 대한 고려가 별도로 이루어지지 않았기 때문으로 판단할 수 있었다.

결론적으로, 특정시스템에 대한 안전 무결성 수준 할당 시 적용되는 방법론 및 위험요인 분석 결과에 따라 안전 무결성 수준 할당결과가 달라질 수 있으며, 보수적인 안전 무결성 수준 할당 결과는 안전성 측면에서만 고려할 경우 적용이 간단하고 적합한 방법이긴 하나, 반면에 현실적으로 적용이 가능하지 않거나 시스템 개발에 소요되는 노력이나 비용적인 측면에서 불필요하고 부적절한 목표가 설정될 수 있을 것으로 판단된다.

References

1) IEC61508, Functional Safety of Electrical / Electronic /Programmable Electronic Safety-related Systems, Part 5, IEC, pp. 10-44, 2010.
2) IEC62278, Railway Applications - Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), IEC, pp. 49-53 2002.
3) IEC62425, Communication, Signalling and Processing Systems - Safety Related Electronic Systems for Signalling IEC, pp. 33-46, 2007.
4) E. Marzal and E. Scharpf, “"Safety Integrity Selection”", The Instrumentation, System and Automation Society, pp. 5-28, 161- 203 , 2002.
5) IEC61511, Functional safety - Safety Instrumented Systems for the Process Industry Sector, Part 3, IEC, pp. 15-45, 2004.
6) Engineering Safety Management (The Yellow Book), Fundamental and Guidance, Railtrack, Vol. 1 & 2, pp. 198-206, 2007.