

철도차량 안전 관리 절차

2023.05.31

레일솔루션연구소

시스템엔지니어링팀 (오지은 책임)

- I. 철도차량 안전 요구 사항
- II. 현대로템 안전 관리 절차
- III. 안전 활동 및 실례
- IV. 해외 운영사 안전 관리 체계
- V. 문제점 및 개선점

I. 철도 차량 안전 요구 사항

1. 국내

- (1) 적용 법규: 철도 안전법 철도차량 기술기준
- (2) 적용 안전관리 산업 규격
 - 1) 코레일: 산업 규격 요구사항 없음 (자체 안전 요구 조건 명시)
 - 2) 지자체 (서울교통공사): IEC 62425 (EN 50129)

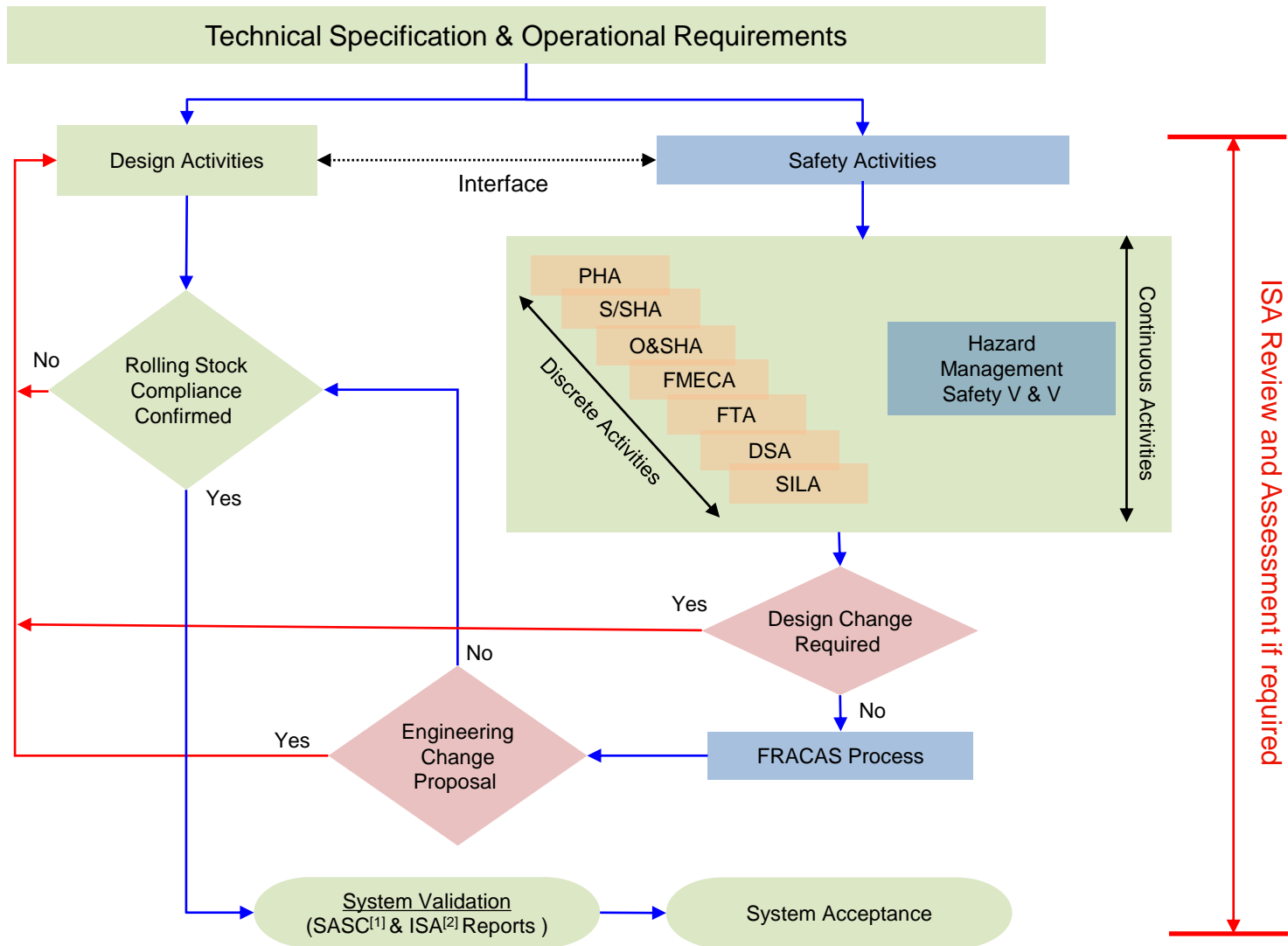
2. 해외

- (1) 적용 법규: 해당 국가에 따른 법규 적용
 - 1) 미국: 49 CFR 238 및 Safety certification program
 - 2) 홍콩 MTRC: 없음 (대신 시행청에서 고용한 E&M level ISA 평가 받음)
 - 3) 아일랜드: Notified National Technical Rules
- (2) 적용 규격
 - 1) 미국: MIL-STD-882
 - 2) 홍콩 MTRC: EN 50126 기반 자체 안전 요구 조건 명시
 - 3) 유럽: EN 50126/EN 50128/EN 50129

* 차이점:

- 국내: 차량 제작사가 직접 형식 시험 승인 신청 (철도 안전법)
위험도 분석 방법 산업 규격과 상이 및 상호 수용 불가 (Cross-Acceptance)
- 해외: 운영사에서 직접 정부 기관 승인 신청 (제작사 지원 역할)
위험도 분석 산업규격과 동일 및 상호 수용 가능

II. 현대로템 안전관리 절차



EN 50126/ MIL-STD-882에 따른 현대로템 표준 안전 관리 절차

III. 안전 활동 및 실례

1. Risk Matrix (해외)

			CONSEQUENCE						
			7	6	5	4	3	2	1
			Trivial	Negligible	Marginal	Serious	Critical	Catastrophic	Disastrous
Staff/Contractor Safety	Fatality						<5	5 or more	
	Major Injury					<5	5 or more		
	Minor Injury	with ≥ 3 days sick leave			<5	5 or more			
		with < 3 days sick leave		<5	5 or more				
Passenger/Public Safety	Fatality						<5	5-50	51-500
	Major Injury					<5	5-50	51-500	501 - 5000
	Minor Injury				<5	5-50	51-500	501 - 5000	>5000
Service	System Disruption				<20 min	1 hour	1 day	1 week	1 month
	Line Disruption			20-60min	few hours	1 day	1 week	1 month	few months
	Station Disruption		<20min	few hours	1 day	1 week	1 month	few months	1 year
FREQUENCY	A	Few times per week or more	≥ 100 /year	R3	R1	R1	R1	R1	R1
	B	Few times per month	≥ 10 - <100 /year	R4	R2	R1	R1	R1	R1
	C	Few times per year	≥ 1 - <10 /year	R4	R2	R2	R1	R1	R1
	D	Few times in 10 years	≥ 0.1 - <1 /year	R4	R3	R2	R1	R1	R1
	E	Once since operation	≥ 1E-2 - <1E-1 /year	R4	R3	R3	R2	R1	R1
	F	Unlikely to occur	≥ 1E-3 - <1E-2 /year	R4	R4	R3	R3	R2	R1
	G	Very unlikely to occur	≥ 1E-4 - <1E-3 /year	R4	R4	R4	R3	R3	R2
	H	Remote	≥ 1E-5 - <1E-4 /year	R4	R4	R4	R4	R3	R3
	I	Improbable	≥ 1E-6 - <1E-5 /year	R4	R4	R4	R4	R4	R3
	J	Incredible	< 1E-6 /year	R4	R4	R4	R4	R4	R3

III. 안전 활동 및 실례

1. Risk Matrix (국내)

등 급		사소한	경미한	주요한	매우 주요한	중대한	매우 중대한	심각한	매우 심각한	치명적인	재난 발생 가능한
		C10	C9	C8	C7	C6	C5	C4	C3	C2	C1
매주 발생하는	F1	B	B	B	A	A	A	A	A	A	A
격주로 발생하는	F2	B	B	B	B	A	A	A	A	A	A
격월로 발생하는	F3	B	B	B	B	B	A	A	A	A	A
분기/반기에 발생하는	F4	C	B	B	B	B	B	A	A	A	A
연 1회 내외	F5	C	C	B	B	B	B	B	A	A	A
2~4년에 1회 내외	F6	C	C	C	B	B	B	B	B	A	A
5~7년에 1회 내외	F7	C	C	C	C	B	B	B	B	B	A
10년에 1회 내외	F8	C	C	C	C	C	B	B	B	B	B
15년에 1회 내외	F9	C	C	C	C	C	C	B	B	B	B
매우 희박한	F10	C	C	C	C	C	C	C	B	B	B

위험도를 3가지 (A,B,C)로 관리

III. 안전 활동 및 실례

1. Risk Matrix (국내): 빈도수

서비스 지연 심각도 엄격하게 관리

구분	등급	C10	C9	C8	C7	C6	C5	C4	C3	C2	C1
		사소한	경미한	주요한	매우주요한	중대한	매우중대한	심각한	매우심각한	치명적인	재난발생가능한
결과	서비스지연 (심각도)	5분 미만	5분 이상~ 10분 미만	10분 이상~ 20분 미만	20분 이상~ 40분 미만	40분 이상~ 1시간 미만	1시간 이상~ 2시간 미만	2시간 이상~ 4시간 미만	4시간 이상~ 8시간 미만	8시간 이상~ 1일 미만	1일 이상
	사망 (명)	0	0	0	0	0	0	1~2	3~4	5~9	10이상
	중상 (명)	0	0	0	0	1~4	5~9	10이상	-	-	-
	경상 (명)	0	0	0	1~5미만	10미만	30미만	30이상	-	-	-

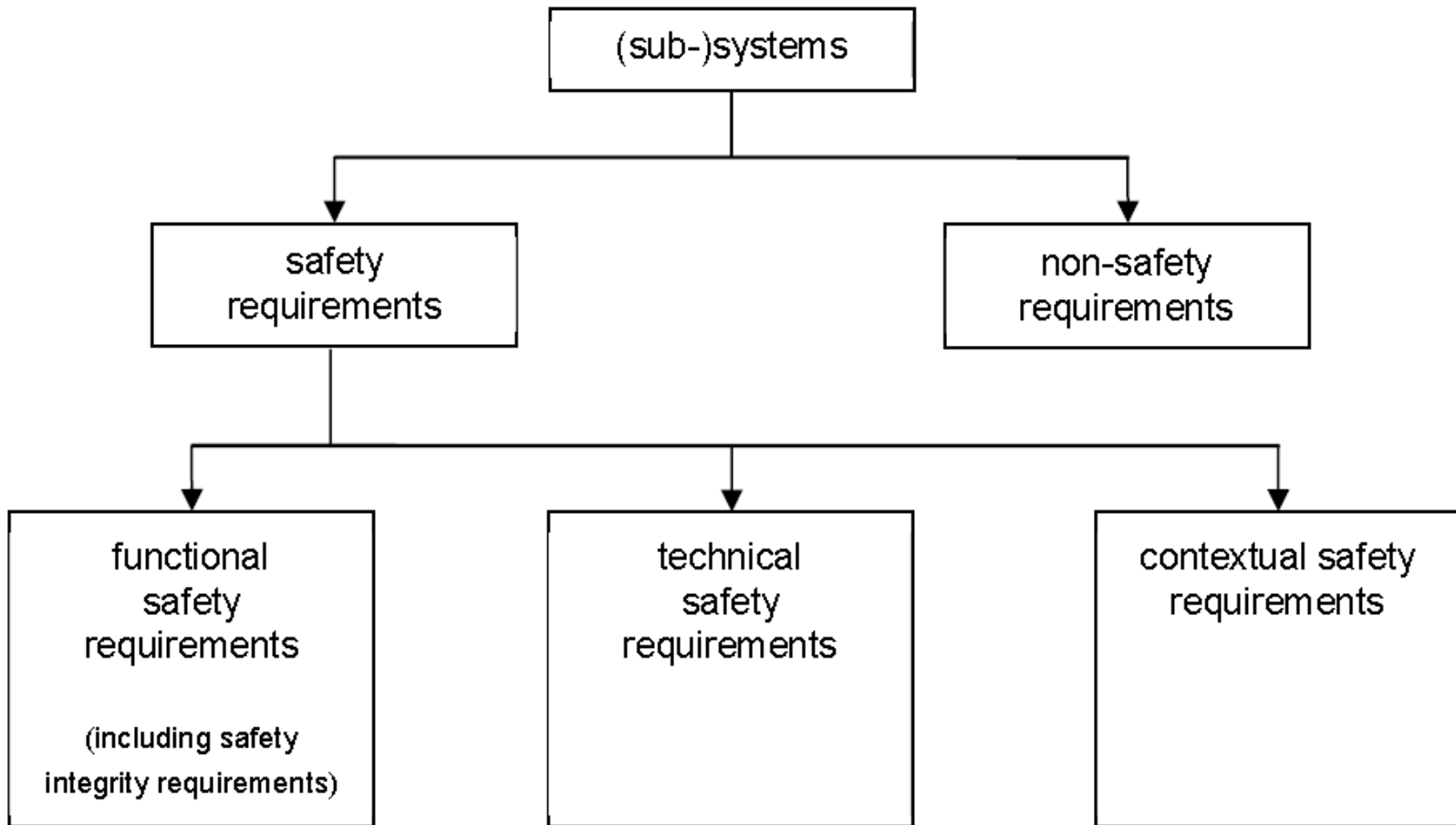
III. 안전 활동 및 실례

1. Risk Matrix (국내) : 심각도

발 생 빈 도	위험원 조건	Ranking (등급)		발생 간격	연간 발생건수
	운행 중 동일 장치의 동일 부품에서 발생한 고장으로 열차지연이나 운행중지 등 차량교체가 발생한 경우, 인명피해 및 중대한 재산상의 손실 우려가 있는 위험요인 및 사고	F1	매주 발생하는	1주 내외	>50(이상)
		F2	격주로 발생하는	2주~4주 미만	49.99~14.50
		F3	격월로 발생하는	1개월 이상~3개월 미만	14.49~5.00
		F4	분기/반기에 발생하는	3개월 이상~9개월 미만	4.99~1.65
		F5	연 1회 내외	9개월 이상~1.5년 미만	1.64~0.66
		F6	2~4년에 1회 내외	1.5년 이상~4년 미만	0.65~0.25
		F7	5~7년에 1회 내외	4년 이상~8년 미만	0.24~0.125
		F8	10년에 1회 내외	8년 이상~13년 미만	0.124~0.08
		F9	15년에 1회 내외	13년 이상~20년 미만	0.079~0.05
		F10	매우 희박한	20년 이상~40년 미만(폐차)	<0.05(미만)

III. 안전 활동 및 실례

2. Safety Requirement 식별



PHA/ 각종 위험 분석을 통해 Safety Requirement 식별

III. 안전 활동 및 실례

3. System (Subsystem) Hazard Analysis

- 장치 고장으로 인해 발생할 수 있는 위험을 식별하는 방법

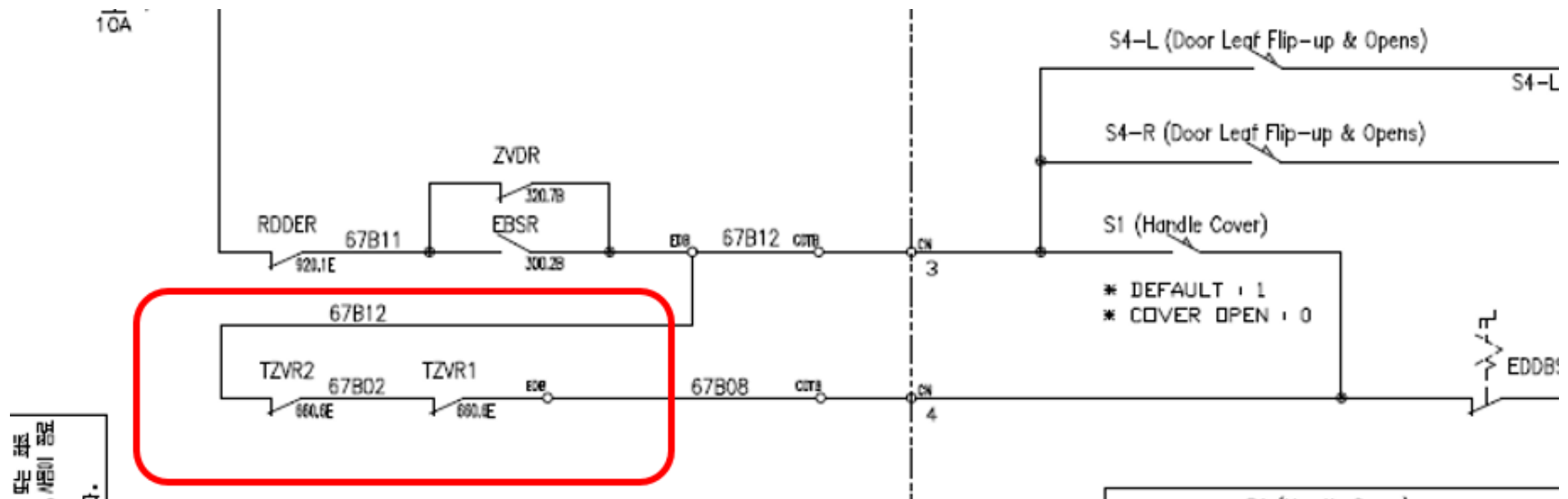


화재 발생시, 역간에서 Train이 정차할경우 Side Door를 통해 Detrainment Device를 펼쳐서 승객이 Track side로 탈출 가능 (장치 고장으로 잘못 작동 시 Side skirt 및 Safety Chain이 있어 작동 불가 설계)

III. 안전 활동 및 실례

4. Interface Hazard Analysis

- 타 System/Subsystem간의 interface로 인해 발생할 수 있는 위험을 식별하는 방법

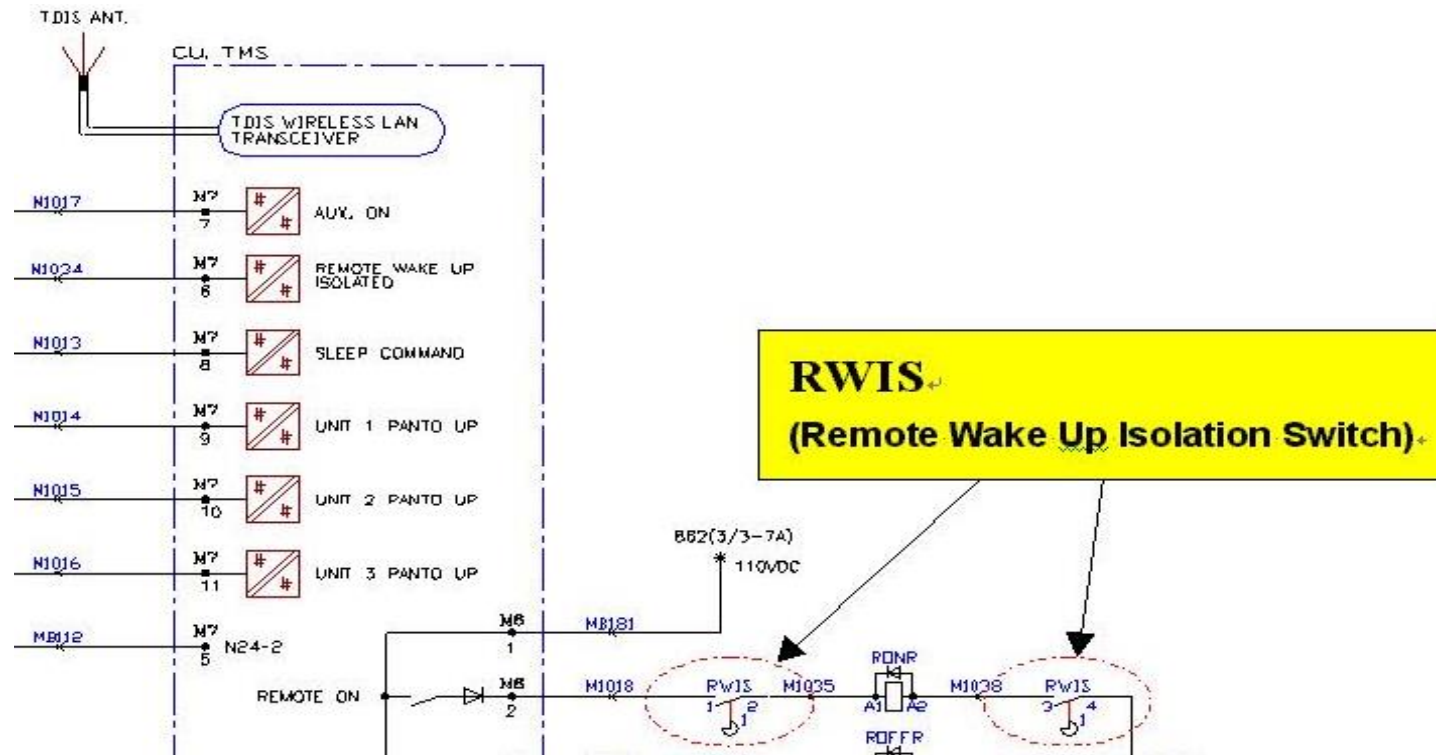


차상 신호에서 ZVR 신호를 받을 경우 전두부 비상문 열림 가능 (무인 운전 차량)

III. 안전 활동 및 실례

5. Operating and Support Hazard Analysis

- Human Error/ Train Operator 나 Maintenance Staff가 업무 수행 중에 발생할 수 있는 위험을 식별하는 방법



기지에서 자동으로 TMS를 통해 Energize/De-energize 가능한데, 만약 정비를 수행시, Depot Control Center에서 Remote로 Energize시키면 Pantograph 상승으로, maintainer가 감전사 당할 수 있음 → 정비 전 RWIS를 off하면 remote wake up 기능 안됨

III. 안전 활동 및 실례

8. SCIL

- Safety Critical Item 선정 후 유지보수 집중 관리 (대부분 기계 장치)

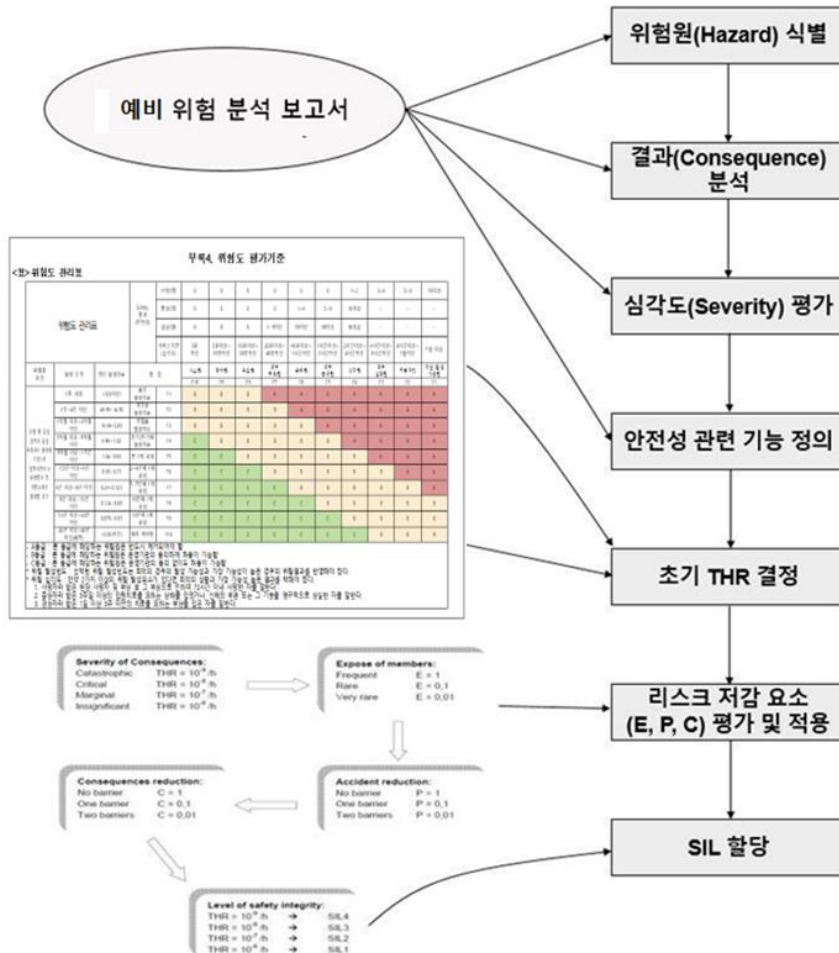
		CONSEQUENCE					
		Negligible	Marginal	Serious	Critical	Catastrophic	Disastrous
	Fatality	Nil	Nil	Nil	<5	5-50	51-500
	Major Injury	Nil	Nil	<5	5-50	51-500	501-5000
	Minor Injury	Nil	<5	5-50	51-500	501-5000	>5000
No. of Independent Failures	Single	NSC	NSC	SC	SC	SC	SC
	Double	NSC	NSC	NSC	SC	SC	SC
	Triple	NSC	NSC	NSC	NSC	SC	SC
	Quadruple (or More)	NSC	NSC	NSC	NSC	NSC	NSC

Assembly / Component	Description		No of Failures Required to cause adverse consequence	Consequence Severity	Result (SC/NSC)
Wheel	Function:	Support wheel and provide mounting face for brake discs	(Circle as appropriate)	(Circle as appropriate)	(Circle as appropriate)
	Parallel System:	N/A			
	Protection system & its safety function:	N/A	Single	Serious	
	Description of Failure Scenario:	Wheel fractures	Double	Critical	SC
	Additional Independent Failure(s):	N/A	Triple	Catastrophic	
	Consequence:	Possible derailment in worst case	Quadruple	Disastrous	NSC
	Applicable maintenance task:	1. Corrective Maintenance (CM): Replace Wheel 2. Preventive Maintenance (PM): Visual Inspection should be carried out (3C-132200-01)			

III. 안전 활동 및 실례

9. SIL(Safety Integrity Level Analysis)

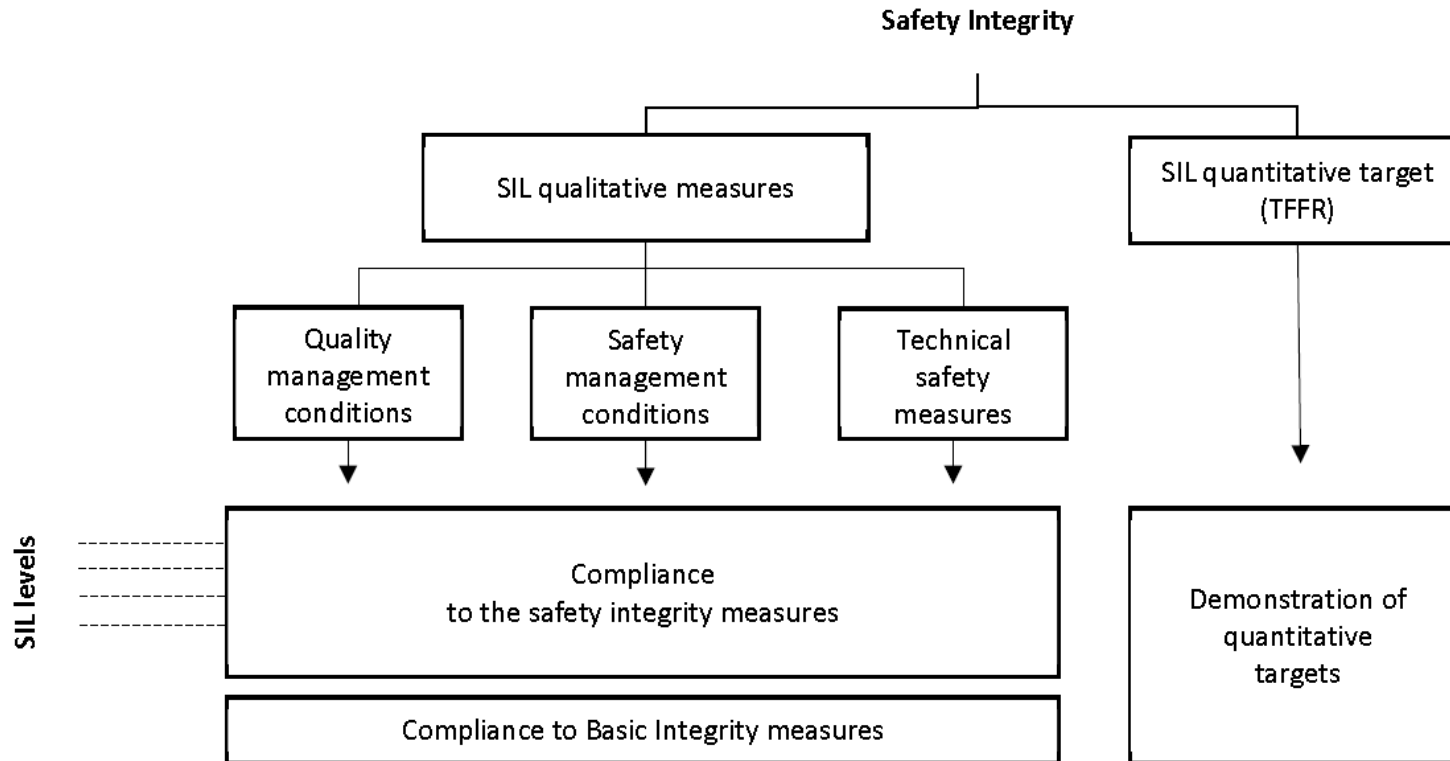
1) SIL 할당 절차



장치명	안전 기능		관련 위험	SIL	SSIL
	SF ID	안전 기능 설명	PHA ID		
출입문 장치	SF11	장애물 감지 기능(모터 전류 모니터링)	PHA-DR19	2	2
			PHA-DR20	0	
	SF12	장애물 감지 기능(장애물 감지 센서)	PHA-DR19	2	2
			PHA-DR20	0	
	SF13	안전한 출입문 열림 기능(모터 제어)	PHA-DR17	2	2
	SF14	안전한 출입문 열림 기능(도어 잠금 제어)	PHA-DR17	2	2
	SF15	안전한 입출력 제어	PHA-DR17	2	2


III. 안전 활동 및 실례

2) SIL 대책 방안



III. 안전 활동 및 실례

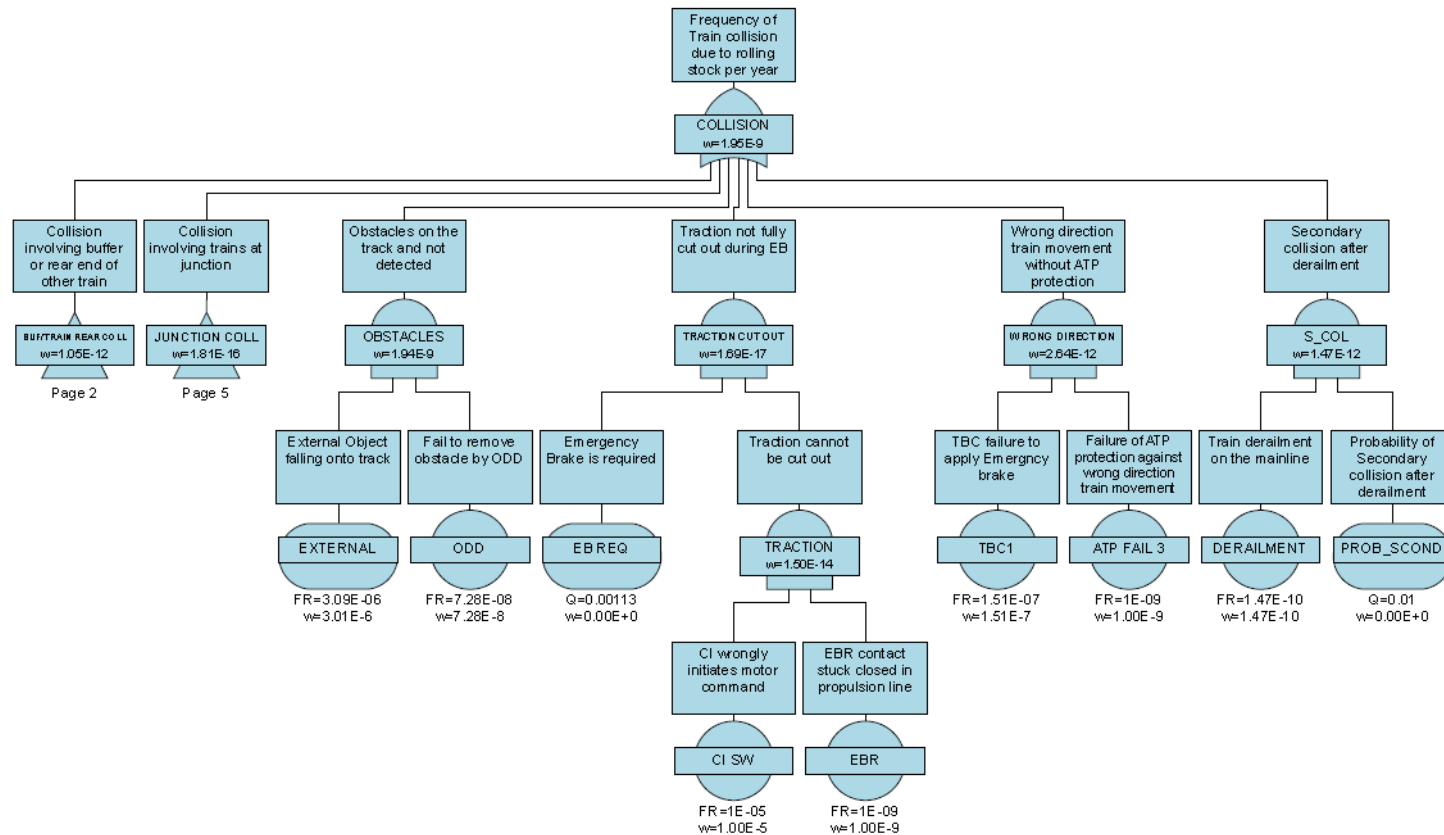
3) SIL 등급에 따른 수행 업무 (예: EN 50128)

TECHNIQUE/MEASURE	Ref	 Basic Integrity	SIL 1	SIL 2	SIL 3	SIL 4
1. Defensive Programming	D.14	-	HR	HR	HR	HR
2. Fault Detection & Diagnosis	D.26	-	R	R	HR	HR
3. Error Correcting Codes	D.19	-	-	-	-	-
4. Error Detecting Codes	D.19	-	R	R	HR	HR
5. Failure Assertion Programming	D.24	-	R	R	HR	HR
6. Safety Bag Techniques	D.47	-	R	R	R	R
7. Diverse Programming	D.16	-	R	R	HR	HR
8. Recovery Block	D.44	-	R	R	R	R
9. Backward Recovery	D.5	-	NR	NR	NR	NR
10. Forward Recovery	D.30	-	NR	NR	NR	NR
11. Retry Fault Recovery Mechanisms	D.46	-	R	R	R	R
12. Memorising Executed Cases	D.36	-	R	R	HR	HR
13. Artificial Intelligence – Fault Correction	D.1	-	NR	NR	NR	NR
14. Dynamic Reconfiguration of software	D.17	-	NR	NR	NR	NR
15. Software Error Effect Analysis	D.25	-	R	R	HR	HR
16. Graceful Degradation	D.31	-	R	R	HR	HR
17. Information Hiding	D.33	-	-	-	-	-
18. Information Encapsulation	D.33	R	HR	HR	HR	HR
19. Fully Defined Interface	D.38	HR	HR	HR	M	M
20. Formal Methods	D.28	-	R	R	HR	HR
21. Modelling	Table A.17	R	R	R	HR	HR
22. Structured Methodology	D.52	R	HR	HR	HR	HR
23. Modelling supported by computer aided design Table and specification tools	A.17	R	R	R	HR	HR

III. 안전 활동 종류 및 실례

10. Fault Tree Analysis (바람직하지 않는 사건에 논리적 구조 및 빈도수 계산)

Top Event 1: Train Collision on mainline



III. 안전 활동 및 실례

11. Safety demonstration (Safety Case)

1) 정의

- Generic product

component/product capable of performing certain functions, with a specific performance level, **in the environmental and operational conditions stated in the reference specifications.**

- Generic application

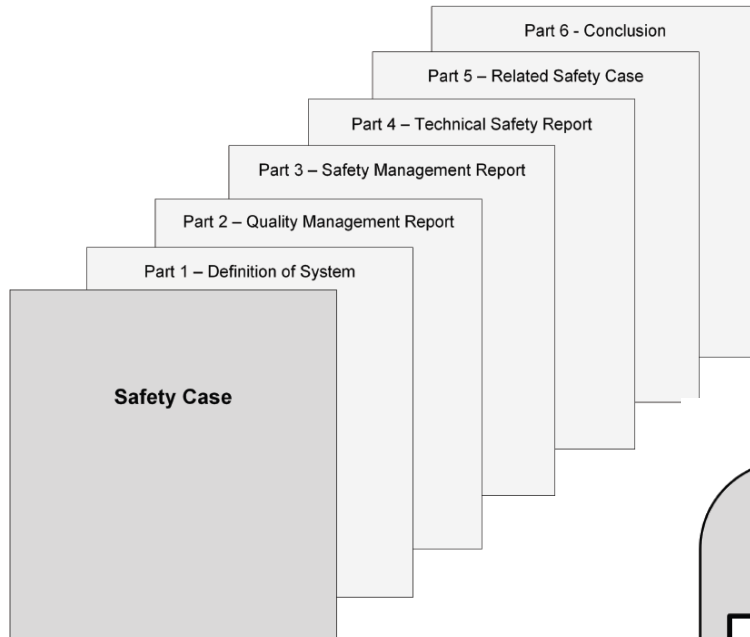
system with specific functions that are related to "a category of applications" associated with **a general environmental and operational context**, which is developed on the basis of criteria of standardization and parameterization of its elements, so as to render it serviceable for various tangible applications.

- Specific application

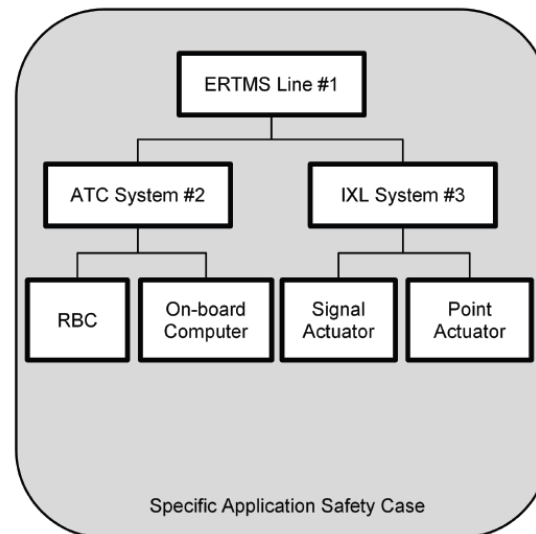
a specific application is used for only **one particular installation**

III. 안전 활동 및 실례

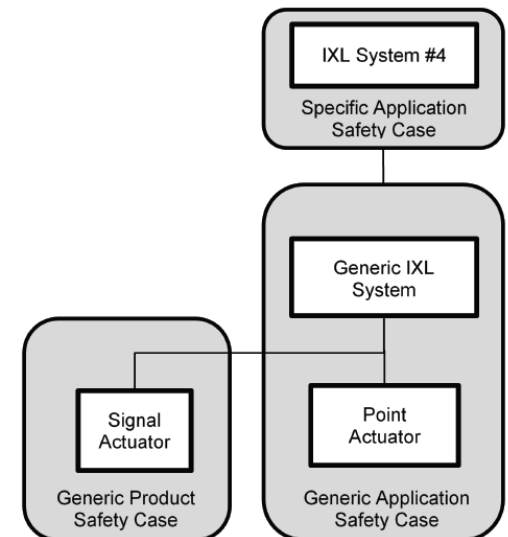
2) Safety Case 종류



Example 1

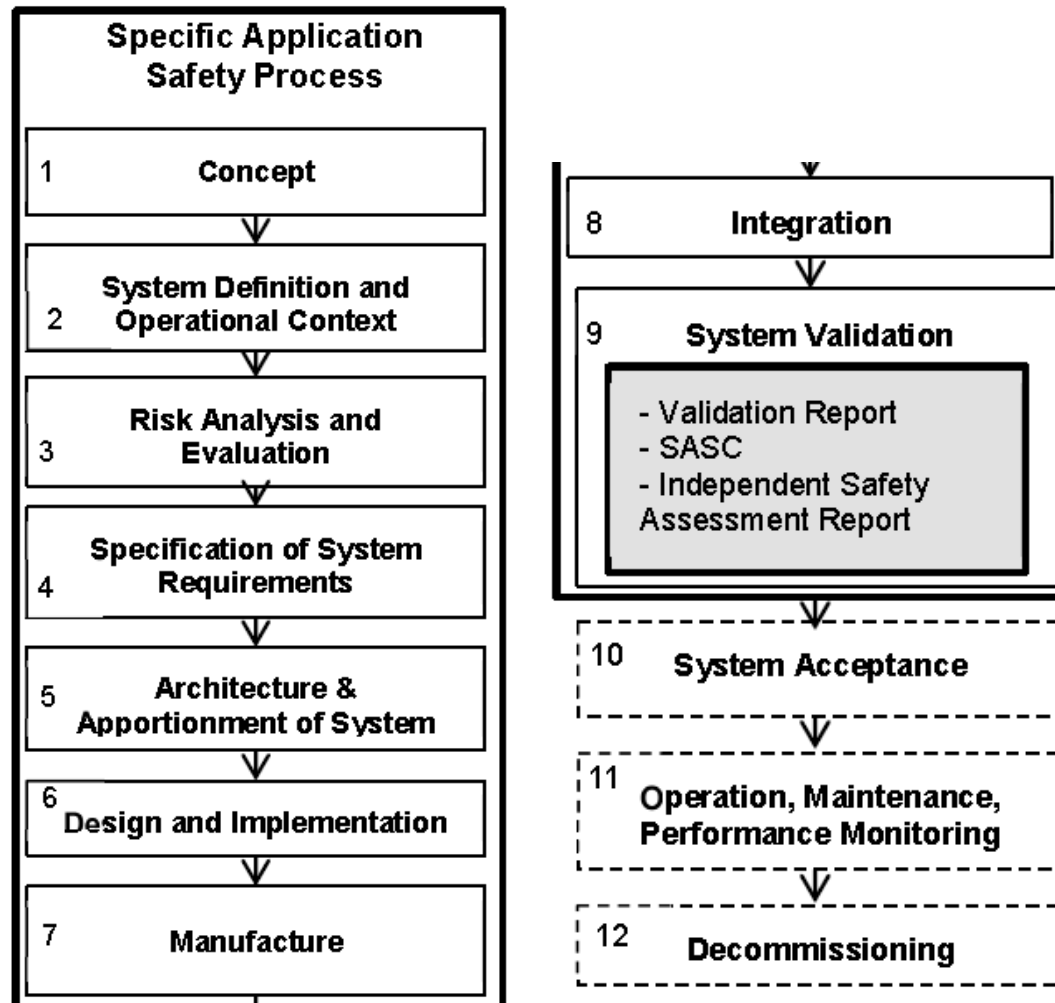


Example 2



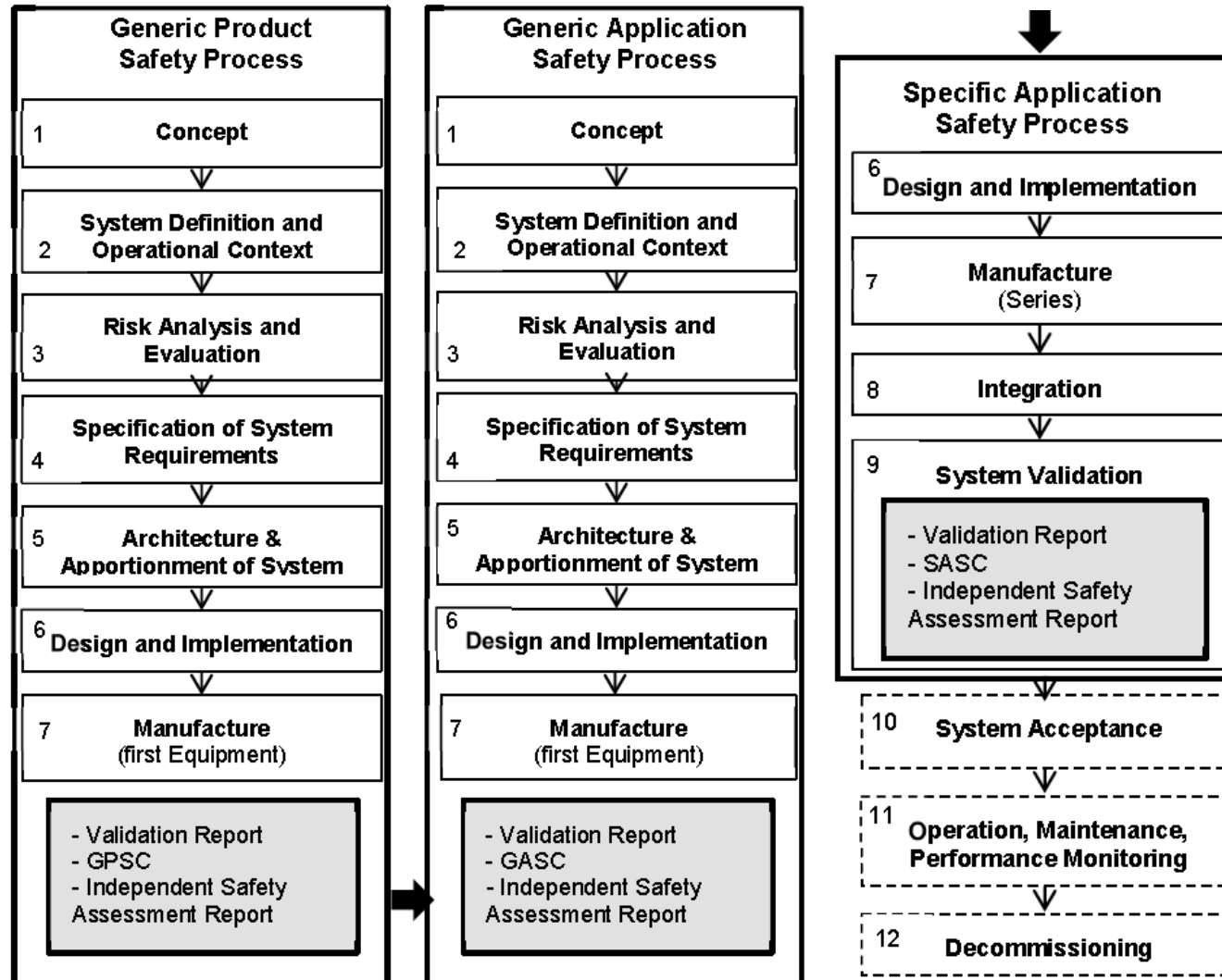
III. 안전 활동 및 실례

3) Safety Acceptance 절차 (SA)



III. 안전 활동 및 실례

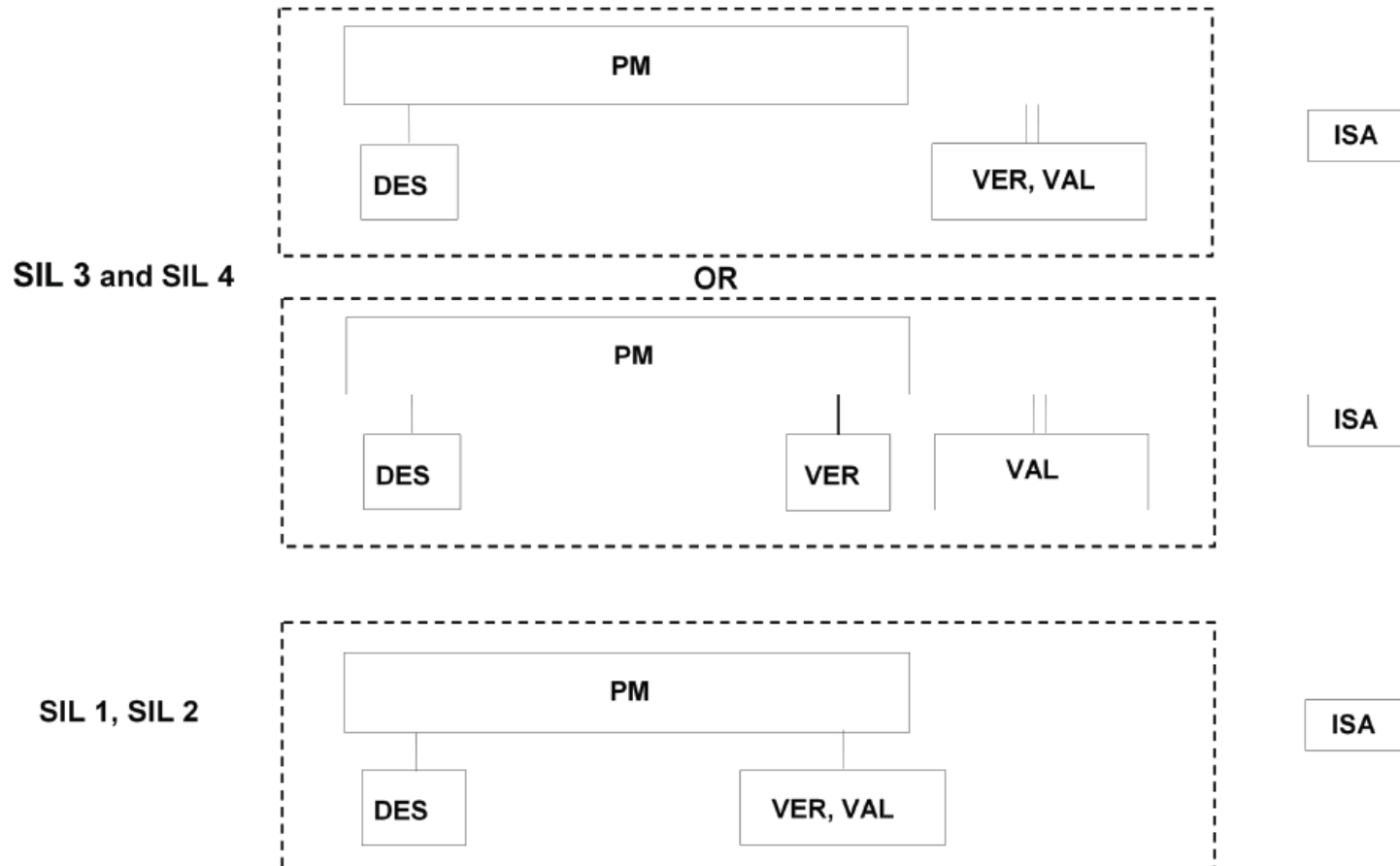
4) Safety Acceptance 절차 (GP+GA+SA)



III. 안전 활동 및 실례

12. Independent Safety Assessment

1) SIL 등급에 따른 조직/ ISA 요구사항



III. 안전 활동 및 실례

2) ISA 자격 요구사항

1. be competent in the domain/technologies where independent assessment is carried out
2. **have acceptance/licence** from a recognised safety authority (ISO/IEC 17020/025/065)
3. have / strive to continually gain sufficient levels of experience in the safety principles and the application of the principles within the application domain
4. be competent to check that a suitable method or combination of methods in a given context have been applied
5. be **competent** in understanding the relevant safety, human resource, technical and quality management processes in **fulfilling the requirements of the EN 50126**
6. be competent in independent assessment approaches/methodologies
7. have analytical thinking ability and good observation skills
8. be capable of combining different sources and types of evidence and synthesise an overall view about fitness for purpose or constraints and limitations on application
9. have an understanding of the overall system including its application environment
10. understand the requirements of EN 50126

III. 안전 활동 및 실례

3) ISA 인증서



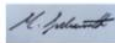
Ricardo
Certification

Independent Safety Assessment Certificate

Certificate Number: RC/ISA/762507/L/2021/217/01

System Under Assessment	Jinjeop Line EMU 50 cars
Description	The specific application of the Jinjeop Line EMU 50 cars. The detailed system configuration is identified in Section 7.1 of the Assessment Report (*).
Applicant Name & Address	Hyundai Rotem Company Cheoldobulmildgwan-ro 37, Ulsang-si, Gyeonggi-do, Republic of Korea
Assessment Requirements	<ul style="list-style-type: none">• IEC 62278:2002 Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)• IEC 62279:2015 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems• IEC 62425:2007 Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling The ISA has assessed the EMUs to determine whether the safety management of the EMUs is compliant with the safety principles of the above standards.
Configuration Definition	The certificate reflects the Baseline Rev. A of Jinjeop Line EMU 50 cars and the system configuration detailed in Section 7.1 of the assessment report.
Assessment Statement	It is confirmed that the Jinjeop Line EMU 50 cars, as defined in the Safety Case and Section 7.1 of the Assessment Report (*), has been demonstrated as safe for commercial operation. The EMU system has been independently assessed and their respective safety arguments are considered satisfactory for the scope of commercial operation. Its design, manufacturing & installation, test & commissioning conforms to the safety management principles of the IEC 62278:2002, IEC 62279:2015 and IEC 62425:2007 and the project has shown that the risk from commercial operation is regarded as being As Low As Reasonably Practicable (ALARP).
Restrictions to Approval	See the attached Annex to this certificate.
Annex of Certificate	Page 2 of this certificate.
Assessment Report	762507RHJ211210 Jinjeop Line EMU 50 Cars Safety Assessment Report, Issue 01, 10 th December 2021. Note: This certificate should be read in conjunction with the above Assessment Report (*) that is an integral part of this certificate.
Validity	Issue Date: 10 th December 2021 Issue No.: 1 This certificate is valid for the defined commercial operation from its issue date until such a time as changes or modifications are made to the configuration referenced above.

Signature:



E-sig: 21/MCD/241

Mark Dodsworth

Ricardo Certification Signatory

On behalf of Ricardo Certification Limited

Shoreham Technical Centre, Old Shoreham Road, Shoreham-by-sea, West Sussex, BN43 5FG, UK

Ricardo Certification (Reg. no 9481761) is a limited company registered in England and Wales. Registered office: Shoreham Technical Centre, Old Shoreham Road, Shoreham-by-sea, West Sussex, BN43 5FG, UK (A5 no. 9208).

Ricardo Certification Limited, its subsidiaries and holding companies (in each case as defined in section 1159 of the Companies Act 2006) and any subsidiaries or holding companies of such companies, as well as their respective affiliates, officers, employees and agents are, individually and collectively, referred to in this paragraph as the "Ricardo Group". The Ricardo Group assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Ricardo Group entity for the provision of information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.



Certificate

ID-Number: ACR/B 11/207

CENELEC Railway Standards

Certification Body TÜV Rheinland InterTraffic GmbH

Owner of Certificate ViaQuatro
Rua Heitor dos Prazeres 320
Vila Sonia - 05522 000 - São Paulo - SP, Brazil

Type designation / Product tested OPM Level - Train Control System and Rolling Stock Doors and Emergency Brake safety functions of Metro São Paulo Line 4 Subphase 1.3 - Carousel Mode (Item under Assessment - IUA)

Manufacturer Siemens-Rotem Metro São Paulo L4 Consortium

Bases of Assessment ¹⁾ EN 50126:1996, EN 50128:2001, EN 50129:2003

Assessment Report / Date ²⁾ ACR/B 11/207, 01-09-2011

Assessment Result ³⁾ The OPM Safety Case and underlying documentation (refer to chapter 4.1 of report ACR/B 11/207) are suitable for passenger revenue service of Subphase 1.3 of the São Paulo Line 4 in automatic mode (MTO) for carousel operation. It has been checked, whether the assessed subsystems comply with the requirements given in chapter 2 of report ACR/B 11/207. All safety related deficiencies have been closed. We have no objections to start passenger operation of Subphase 1.3 of the São Paulo Line 4 automatic mode (MTO) for carousel operation under consideration of the conditions and constraints referenced in chapter 4.6 of report ACR/B 11/207, especially the rules for operation to be established by the operator. For Details please refer to chapters 4.1, 4.2, 4.3, 4.4.1, 4.4.2, 4.4.3, 4.4.4 and 4.4.5 of report ACR/B 11/207.

Validity Valid for the configuration of the Train Control System and Rolling Stock Doors and Emergency Brake safety functions of Metro São Paulo Line 4 Subphase 1.3 - Carousel Mode, as described in the OPM Safety Case, RA DPR/SPL4/116.0742.11/CB/CR 01, Ed/Rev: 02/00 of 22-08-2011.

¹⁾ Further Codes and standards to be applied are contained in the assessment report.

²⁾ This assessment report is an integral part of the certificate.

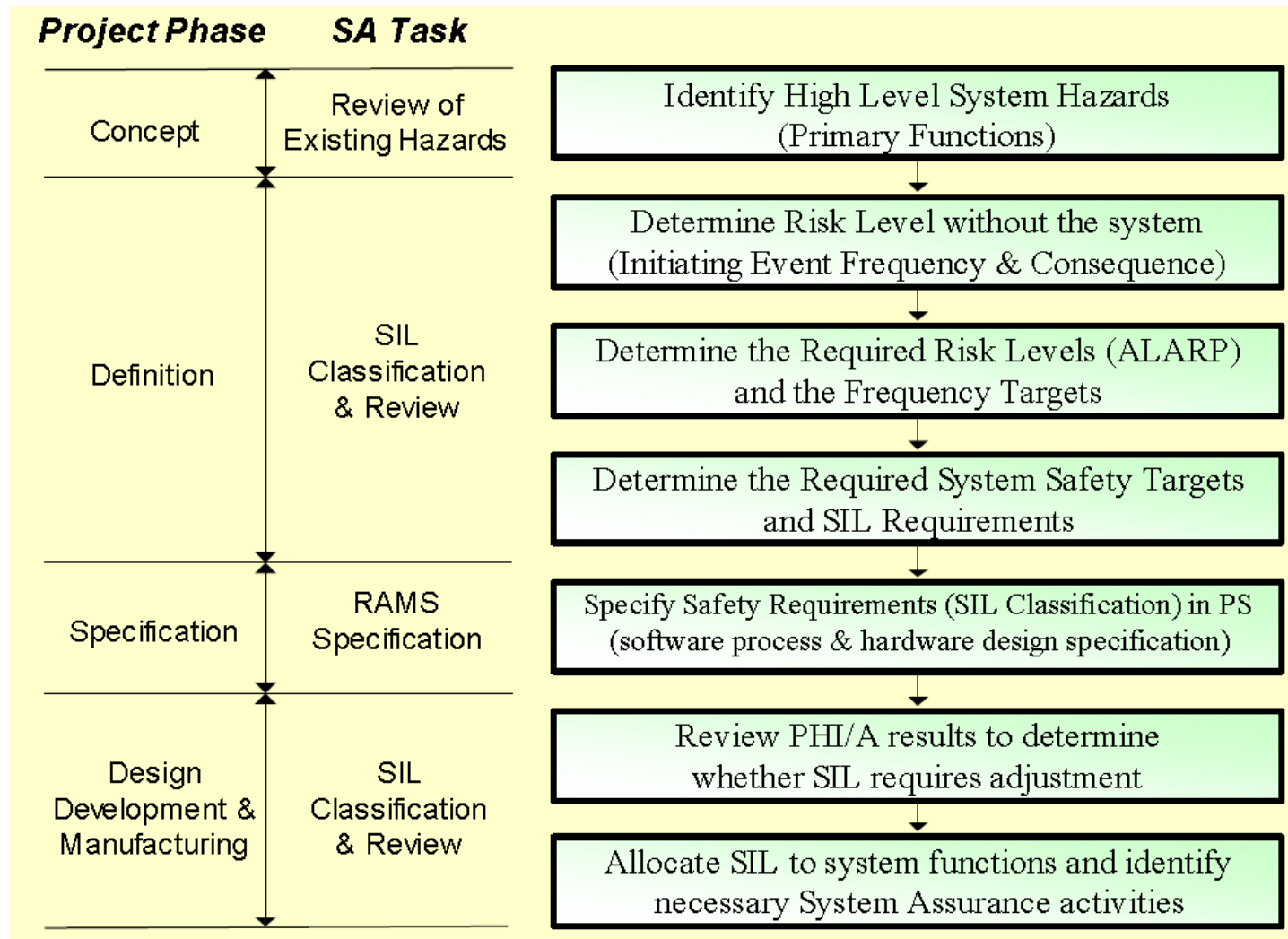
³⁾ This assessment report is an integral part of the certificate.

Cologne, 01-09-2011

TÜV Rheinland InterTraffic GmbH
Am Grauen Stein • 51105 Köln
www.tuv.intertraffic.de


Certification Office
(Florian Steiner)

IV. 해외 운영사 안전 관리 체계



운영사에서 SIL 할당 및 장치 요구 사항 명시 (SIL 등급에 따라 설계 상이)

V. 문제점 및 개선점

1. 철도 차량 기술기준

1) 문제점: 장치 사양은 상세 위험 분석시 결정 불가

3.2.4.7 화재 진압 설비

- 5) 예비위험도분석 및 상세위험도분석 결과 필요하다고 인정되는 철도차량에는 자동으로 화재를 진압하고 이를 운전실에서도 작동시킬 수 있는 자동 화재진압설비가 설치되어야 한다.

4.2.5 장애물 제거기

- 1) 운전실이 설치된 철도차량의 안전운행을 위하여 궤도위에 있는 임의의 장애물을 제거하기 위한 장애물제거기가 설치되어야 한다. 다만 위험도분석 등을 통해 소형장애물 충돌 위험도가 허용 가능한 수준인 경우 장애물 제거기를 설치하지 않을 수 있다.

4.2.15 운전실 및 비상탈출구

- 5) 운전실은 기관사·승무원이 비상시에도 용이하게 탈출할 수 있는 구조로 설계되어야 한다. 이 경우 예비위험도 및 상세위험도 분석 결과 필요하다고 인정되는 경우 별도의 비상탈출구가 설치되어야 한다.

2) 개선점

- 철도 차량 기술기준 수정 : 상세 위험도 분석 삭제
- 운영사 운영환경/ 사고 데이터 근거로 제작 예비 위험도 분석 결과에 따라 제작 사양서에 명시

V. 문제점 및 개선점

2. Cross Acceptance (상호 수용) 불가

1) 문제점: ISO/IEC 17020 자격 가진 유럽 업체 발행 ISA report 수용 불가로 ISO/IEC 17065 인정기관 발행에 따른 추가 시간 및 비용 소요

2) 개선점
전세계적으로 공인된 유럽 업체에 대해 ISO /IEC 17020 자격 가진 유럽 업체 발행 ISA report 수용
될 수 있도록 절차 개선

3. 기존 노선 신호 장치 철도 안전법 적용 난이

1) 문제점: 기존 노선 납품한 해외 신호 업체 철도 안전법 적용 수용 불가 주장

2) 개선점: 영업운전으로 안전성 입증된 신호 장치에 대해 운영사에서 차량 발주 전 동일 신호 장치 적용 추진시 철도 안전법 미적용 예외규정 마련 필요.